A New Model for Computer Network Security Risk Analysis

**By
Sophie Martel**

**A thesis submitted to the
Department of Systems and Computer Engineering
Carleton University
Ottawa, Ontario**

**In partial fulfilment of the requirements for the degree of
Master of Engineering
Telecommunication Technology Management
May 2002**

©Copyright 2002 by Sophie Martel , Ottawa, Ontario.

National Library
of Canada

Acquisitions and
Bibliographic Services

395 Wellington Street
Ottawa ON K1A 0N4
Canada

Bibliothèque nationale
du Canada

Acquisitions et
services bibliographiques

395, rue Wellington
Ottawa ON K1A 0N4
Canada

Your file Votre référence

Our file Notre référence

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-79770-8

Canada

The undersigned recommend to the
Faculty of Graduate Studies and Research
Acceptance of the thesis:

A New Model for Computer Network Security Risk Analysis

Submitted by
Sophie Martel
in partial fulfillment of the requirements
for the degree of
M.Eng. in Telecommunication Technology Management

Professor L. Briand, Thesis Supervisor

Chair, Department of Systems and Computer Engineering

Carleton University

© June 2002

Abstract

Conventional security risk-analysis methodologies focus mainly on the identification of new security services and mechanisms. In our day, the problem with Information System (IS) security is not that secure technologies or products are not present, but rather that ISs are not implemented and used effectively. Consequently, a new approach needs to be researched

The proposed model consists of a process by which a Global Risk Value (GRV) is dynamically determined for a specific “asset/exposure” pair as the environment changes. This GRV can then be used to generate a prioritized security-related action list to fix implementation flaws. A prototype was built and three cases were analysed to test the model. From the analysis, it is concluded that the technique is promising and may help overcome some of the present barriers to effective risk management created by the dynamic aspect of the new information technology environment.

Acknowledgements

I would like to thank my thesis advisor Dr. Lionel Briand. I would also like to thank Dr. Alain Martel, from Laval University and Capt. Luc Dandurand, from the Canadian Forces Red Team, for their valuable advice. As well, I would like to thank Dr. Adel Guitouni, from DREV, for his support with the Expert Choice Software. Special thanks must also go to Stephan Gregory, Victor Singl, Donald Clark, Darren Dentremont and WO Garry Rideout for providing the expertise required to validate the research. Although their names cannot be listed here, many others have contributed in various ways, either directly or indirectly and I thank them for their support.

Table of contents

Abstract.....	iii
Acknowledgements.....	iv
Table of contents.....	v
List of Tables	viii
List of Figures	xi
List of Appendices.....	xiii

PART 1- INTRODUCTION

Chapter 1 – Introduction.....	2
1.1 Introduction.....	2
1.2 Issues and problems to be addressed	3
1.3 Vocabulary.....	4
1.4 Thesis structure	5

PART 2 – BACKGROUND

Chapter 2 – Risk analysis methodologies.....	11
2.1 Introduction.....	11
2.2 Conventional risk analysis	11
2.2.1 First generation risk analysis	12
2.2.2 Second generation risk analysis	12
2.3 Today's environment versus existing methodologies.....	14
2.4 Conclusion	18
Chapter 3 – Network security technologies.....	19
3.1 Introduction.....	19
3.2 Exposures.....	19
3.3 Security auditing tools	21
3.4 Incident detection.....	24
3.4.1 Attack and incident	24

3.4.2	Intrusion detection systems.....	25
3.5	Countermeasures.....	28
3.6	Conclusion	30

PART 3 – A NEW METHOD FOR SECURITY RISK ANALYSIS

Chapter 4 – Risk Control Network Service (RCNS) – The concept and the model.. 32

4.1	Introduction.....	32
4.2	RCNS model concept.....	35
4.3	RCNS structure	37
4.4	Introduction to the risk model.....	39
4.4.1	Risk formula.....	39
4.4.2	Using the risk model	41
4.5	Risk model implementation	42
4.6	Conclusion	44

Chapter 5 Estimation of the damage value parameter in the risk value formula..... 45

5.1	Introduction.....	45
5.2	Multi-attribute Decision Making (MADM).....	46
5.2.1	General overview	46
5.2.2	Nontraditional Capital Investment Criteria (NCIC)	47
5.3	Building the risk model.....	54
5.3.1	Damage value procedure.....	54
5.3.2	Calculation based on NCIC	55
5.3.3	Damage value structured analysis.....	72
5.4	Conclusion	79

Chapter 6 Estimation of the probability parameter in the risk value formula 81

6.1	Introduction.....	81
6.2	Comparison of prediction systems.....	81
6.2.1	Rule-based systems	81
6.2.2	Feed-forward neural networks	83
6.2.3	Bayesian networks	83
6.3	Supporting tool.....	87
6.4	Building the Bayesian network.....	87
6.4.1	Building our Bayesian network (BN)	88
6.4.2	Evidence on the information and motivation variables	94
6.4.3	Conditional threat probabilities.....	98
6.4.4	Conditional attack probability.....	106

6.5	Damage value structured analysis.....	108
6.6	Conclusion	112
PART 4- EMPIRICAL APPROACH		
Chapter 7	– RCNS prototype.....	114
7.1	Introduction.....	114
7.2	Prototype process implementation.....	114
7.3	Eliciting expert judgement.....	117
7.3.1	Selecting and motivating the experts	117
7.3.2	Eliciting techniques and potential bias	119
7.4	Conclusion	127
Chapter 8	- Model validation and performance assessment.....	128
8.1	Introduction.....	128
8.2	Experimental methodology	128
8.2.1	Case Study	128
8.2.2	Basis for ranking comparison	130
8.3	Empirical validation.....	132
8.4	Sensitivity analysis.....	141
8.4.1	Harm value parameter m_{sik} sensitivity analysis	142
8.4.2	Probabilistic parameter sensitivity analysis	150
8.5	Conclusion	156
PART 5 – CONCLUSION		
Chapter 9	– Conclusion	159
9.1	Introduction.....	159
9.2	Lessons learnt.....	161
9.3	Value of RCNS	162
9.3.1	Pros	162
9.3.2	Cons	163
9.4	Future research.....	165
References		167
Acronym		173
Lexicon		175

List of Tables

Table 2.1. Criteria to evaluate security risk analysis requirements	15
Table 2.2. IT generation comparisons.....	16
Table 3.1. Attacks/incidents.....	25
Table 5.1. Sensitivity rating definitions with respect to confidentiality	58
Table 5.2. Sensitivity rating definitions with respect to integrity	58
Table 5.3. Sensitivity rating definitions with respect to availability	58
Table 5.4. Sensitivity rating definitions with respect to the service function.....	60
Table 5.5. Standard list of attributes and sensitivity level for Figure 5.3	61
Table 5.6. Small network domain scenario covering attributes for SWE (k =1).....	64
Table 5.7. Small network domain scenario cost attributes for SWE (k =1)	65
Table 6.1: Motivation variable states.....	97
Table 6.2. Scale of comparison.....	99
Table 6.3. The PCM of the probabilities conditioned on the states of the ID variable...	101
Table 6.4. Estimation of P(Threat ID)	101
Table 6.5. The PCM of the probabilities conditioned on the states of the complexity variable.....	102
Table 6.6. Estimation of P(Threat Complexity).....	102
Table 6.7. The PCM of the probabilities conditioned on the states of the motivation variable.....	103

Table 6.8. Estimation of $P(\text{Threat} \text{Motivation})$	103
Table 6.9. The PCM of the probabilities conditioned on the states of the complexity variable.....	104
Table 6.10. Estimation of $P(\text{Threat} \text{ET})$	104
Table 6.11. $P(\text{Threat} \text{ID}, \text{C}, \text{M}, \text{ET})$	105
Table 6.12. The PCM of the probabilities conditioned on the states of the complexity variable.....	107
Table 6.13. Estimation of $P(A T)$	107
Table 8.1. ranking consensus (reference ranking)	133
Table 8.2. Case 1 - Comparison from expert 1 judgement with the consensus ranking.	134
Table 8.3. Case 1 - Comparison from expert 2 judgement with the consensus ranking.	134
Table 8.4. Case 1 - Comparison from expert 3 judgement with the consensus ranking.	135
Table 8.5. Case 2 - Comparison from expert 1 judgement with the consensus ranking.	135
Table 8.6. Case 2 - Comparison from expert 2 judgement with the consensus ranking.	135
Table 8.7. Case 2 - Comparison from expert 3 judgement with the consensus ranking.	135
Table 8.8. Case 3 - Comparison from expert 1 judgement with the consensus ranking.	136
Table 8.9. Case 3 - Comparison from expert 2 judgement with the consensus ranking.	136
Table 8.10. Case 3 - Comparison from expert 3 judgement with the consensus ranking	136
Table 8.11. Case 1 - Comparison from the RCNS prototype with the consensus ranking	137
Table 8.12. Case 2 - Comparison from the RCNS prototype with the consensus ranking	137

Table 8.13. Case 3 - Comparison from the RCNS prototype with the consensus ranking	137
Table 8.14. Summary of experimental data	138
Table 8.15. Case 1 - Comparison of the Cybercop ranking with the consensus ranking	140
Table 8.16. Case 2 - Comparison of the Cybercop ranking with the consensus ranking	141
Table 8.17. Case 3 - Comparison of the Cybercop ranking with the consensus ranking	141
Table 8.18. Bridge attributes limit Interval	142
Table 8.19. Essential pairwise comparison judgements	144
Table 8.20. Experiment 1	145
Table 8.21. Experiment 2	146
Table 8.22. Experiment 3	146
Table 8.23. Case 1 sensitivity analyses on $P(T ID)$ PCM	151
Table 8.24. Case 3 sensitivity analyses on $P(T ID)$ PCM	152
Table 8.25. Case 1 sensitivity analyses on $P(T ET)$ PCM	152
Table 8.26. Case 3 sensitivity analyses on $P(T ET)$ PCM	153
Table 8.27. Case 1 sensitivity analyses on $P(A T)$ PCM	154
Table 8.28. Case 3 sensitivity analyses on $P(A T)$ PCM	155

List of Figures

Figure 1.1. Thesis structure.....	6
Figure 3.1. Multiple complex threats.....	27
Figure 4.1. Information system (IS).....	33
Figure 4.2. UML class diagram representing the RCNS concept.....	34
Figure 4.3. RCNS model concept	36
Figure 4.4. RCNS structure.....	38
Figure 4.5. RCNS model architecture.....	42
Figure 5.1. NCIC attributes PCM for alternative k.....	52
Figure 5.2. Attributes tree-structure template	56
Figure 5.3. Small network domain scenario	61
Figure 5.4. Evaluation of SWE services harm for the scenario in Figure 5.3	69
Figure 5.5. Damage value data flow diagram	73
Figure 6.1. Directed acyclic graph.....	88
Figure 6.2. BN representing the sphere of influence of a vulnerable process component	93
Figure 6.3. Change in ID state over time	95
Figure 6.4. Change in M state over time.....	97
Figure 6.5. Change in ET state over time	98
Figure 6.6. Probabilistic parameter data flow diagram.....	108
Figure 7.1. RCNS processes implementation	115

Figure 7.2. Anticipated biases in our elicitation method	124
Figure 8.1. Case 3: Experiment 1 - accuracy against simulated pairwise comparison error	147
Figure 8.2. Case 3: Experiment 2 - accuracy against simulated pairwise comparison error	148
Figure 8.3. Case 3: Experiment 3 - accuracy against simulated pairwise comparison error	148
Figure 8.4. Case 3: Experiment 2 - accuracy against simulated pairwise comparison error with a cut off inconsistency ratio of 0.09.....	149
Figure 8.5. Case 3: Experiment 2 - accuracy against simulated pairwise comparison error with a cut off inconsistency ratio of 0.02.....	150

List of Appendices

Appendix A - The Analytical Hierarchy process.....	180
Appendix B – Elicitation of expert judgement to determine $P(\text{Threat} \text{Complexity})$	189
Appendix C – Elicitation of expert judgement to determine $P(\text{Threat} \text{Motivation})$	192
Appendix D: Case Study - Experts Analysis	194
Appendix F - Experimental Data	218

PART 1 - INTRODUCTION

Chapter 1 – Introduction

1.1 Introduction

Networks have become a fundamental part of today's communication and information systems. Attacks directed against them could disable a larger number of services they provide. The impacts of such attacks vary depending on the area concerned. A large network attack in the financial sector can result in wide-ranging economic losses. An intrusion in a military command and control system can result in failed operations and the loss of life. Small corporations can literally go out of business because of well-organized attacks, if their productivity relies heavily on their information systems. Some of the dangers outlined by early advocates of information warfare are starting to emerge as real concerns due to the penetration of computer networks in our society. Security mechanisms to protect against network attacks are therefore receiving considerably more attention than in the past in the academic, government and industrial sectors. Today, the problem is not that secure technologies or products do not exist, but rather that they are not implemented and used effectively. In order to more effectively and appropriately use existing countermeasures, risk analysis needs to be performed.

1.2 Issues and problems to be addressed

As the advantages of being connected to the Internet multiply, so do the risks. Various ingenious techniques have been devised to infiltrate networks connected to the Internet, and still other exposures are being uncovered and exploited each day. In order to take calculated risks, these risks need to be analyzed using an appropriate risk analysis methodology. Today, despite the fact that information technology has evolved a lot, the methodologies used for analyzing the risks to these technologies have stayed the same. The conventional risk-analysis methodologies focus mainly on the identification of new security services and mechanisms. In our day, the problem with Information System (IS) security is not that secure technologies or products do not exist, but rather that ISs are not implemented and used effectively. In fact, due to the distinctiveness of the new environment the network operators are overwhelmed with network security flaws to fix. They have too many things to do. Therefore, they need a way to prioritize their work to deal with the risk involved with the issues. It has become clear that current risk-analysis methodologies could only be applied with difficulty to the new environment and that a new risk-analysis approach is required [LAB 99] [WRI 99] [FLE 95]. This document defines a risk model on which a new network service, referred as “Risk Control Network Service”(RCNS), could be developed. The RCNS is presented as a possible way in which risk analysis could be performed by adapting to the dynamic computer network situation. The innovative risk analysis model allows the aggregation of a wide range of

information concerning the network environment into Global Risk Values that can be used to prioritize the implementation of countermeasures.

1.3 Vocabulary

Many different definitions have been formulated for technical terms that are used in this text. However, for the purposes of the present document, the following definitions are used in the context of the research to be undertaken:

- Threat: Circumstances that have the potential to cause loss or harm [PFL 96] .
- Exposure: Weakness in the organisation that would create a condition, which would allow the threat to cause an impact to an organisation by triggering a loss [PEL 01] . The opportunity for the attack [PFL 01] . Flaw allowing unauthorized access or use [AMO 94].
- Asset: Platform (equipment used for input, storage, processing, transfers...) and Interface equipment (router, firewall).
- Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities, or processes [ARC 93] . Confidentiality is sometimes called secrecy or privacy [PFL 96] .
- Integrity: The assurance, under all conditions, that a system will reflect the logical correctness and reliability of the operating system; the logical completeness of the hardware and software that implement the protection

mechanisms; and the consistency of the data structures and accuracy of the stored data [ARC 93] .

- Availability: The goal of ensuring that information and information processing resources both remain readily accessible to the authorised users [ARC 93] .
- Countermeasure: Protection to block threats or close exposures.
- Risk analysis: Process, involving Security threats and exposures identification in order to better understand the security requirements of the environment in question.

1.4 Thesis structure

We start our investigation into network security by a study of existing risk analysis methodologies. We then identify some problems. Afterward, we examine the existing network security technologies that can be used to gather some information about the environment. Having gained the necessary background information, we proceed to conceptualize a possible solution to the said issues and problems. We then define the risk model behind this solution. We conclude with a practical implementation of the latter model and we present the results of a few case studies. The organization of our work is presented in Figure 1.1.

Figure 1.1. Thesis structure

The arrows in Figure 1.1 indicate the relationship between the various chapters. This thesis consists of five parts, each part in turn consisting of one or a number of chapters. Part 2 presents the problem and serves as background information, without which the reader would not be able to understand the proposed model. Chapter 2 of part 2 provides an overview of the existing risk-analysis methods. This is followed by an evaluation of these methods. From this chapter, it becomes evident that today's existing method could not easily be used to dynamically prioritize the implementation of countermeasures and that a new approach to risk analysis is sorely needed. The next chapter, chapter 3, is devoted to a brief presentation of some network security technologies. The latter overview is deemed important as it is aimed at facilitating the reader's understanding of how these technologies can be used to dynamically provide information about computer network environments to the model.

Part 3 starts off with a description of the proposed model. This is followed by a detailed explanation of how the risk formula parameters are estimated and the theories behind this. Chapter 4 is entitled "RCNS – the concept and the model". It presents the reader with an overview of the "RCNS" concepts and introduces the risk value formula that is the heart of the model. The formula is based on the expected loss which is defined as the damages value of the assets at risk multiplied by how exposed they are [PFL 01] [PFL 96] [PEL 01] [NOR 00]. The next two chapters are devoted to discussions on each of the parameters of risk. In this way, chapter 5 provides a detailed explanation of how the damage value parameter can be subjectively estimated in practice. The estimation of this

parameter is a multidimensional problem that justifies the use of a Multi-Criteria Decision Making (MADM) methods. Having looked at different MADM method, we decided to base our damage value equation on the Nontraditional Capital Investment Criteria (NCIC) principles. The NCIC method provides an easy to use MADM method, which allows including consideration of multiple, non-monetary attributes of alternatives. The advantage of this method with respect to our problem is that it represents the final score in monetary terms. Chapter 6 provides a detailed explanation of how the probabilistic parameter can be subjectively estimated in practice. Having looked at different prediction systems, we decided to use Bayesian networks to dynamically evaluate the probabilistic part of our model. The first advantage of doing so is that the Bayesian networks represents the structure of the arguments in an intuitive, graphical format. The second advantage is that using probability calculus and Bayes theorem, if the evidence change, it is possible to update the values of all the probabilities in the Bayesian networks. The beauty of both Bayesian networks and NCIC is that they are able to accommodate subjective and objective data. The chapters 4, 5 and 6 constitute the main contribution of the thesis, as they contain details of an alternative approach to risk analysis.

Part 4 defines the empirical approach used to evaluate the risk model. First, to prove that the concept was tenable, a prototype needed to be developed. The intent of chapter 7 is to describe how the modeling methodology presented in earlier chapters was implemented using tools such as Hugin Lite [HUG 02] , Expert Choice [EXP 00] and

Microsoft Excel. Chapter 8 validates the proposed risk model, by analyzing the risk value scores, produced by the prototype for the exposures presented in the three case studies described in appendix D. The chapter first presents the experimental methodology. Then, the outputs of the prototype are analyzed. Finally, a sensitivity analysis is performed on the knowledgebase data used in the prototype.

The thesis culminates in part 5, which is comprised of chapter 9. In this last chapter, we weigh up the pros and cons of the proposed model, we review our research effort and we identify possible future research directions. There it is concluded that the technique is promising and may help overcome some of the present barriers to effective risk management created by the dynamic aspect of the new information technology environment.

PART 2 - BACKGROUND

Chapter 2 – Risk analysis methodologies

2.1 Introduction

By examining the computer security literature over the last 25 years we realized that the methods and practices employed for information system risk analysis have changed considerably. It is possible to look at their evolution in terms of generations of information technologies (IT) [LAB 99] . The purpose of this chapter is to demonstrate that a risk-analysis methodology used for one IT generation cannot necessarily be used for another. In other words, we want to demonstrate that as the IT environment evolves, so should the risk-analysis approaches and that today's existing method could not be used to provide the data analysis required in the new environment. Fletcher and Labuschagne, in their respective papers, assert that risk analysis methodologies have gone through two generations and need to enter a third [FLE 95]. From this chapter, it becomes evident that a new approach to risk analysis is sorely needed. At the end of this chapter we define the requirements for a third generation risk analysis model that allows a dynamic prioritization of the implementation of countermeasures.

2.2 Conventional risk analysis

The purpose of this section is to present the risk-analysis methodologies used for the first and the second IT generation.

2.2.1 First generation risk analysis

The first generation approaches to risk analysis grew up in the first IT generation in the time of centralized mainframes. Given the assets that comprised a system, these approaches assumed an unchanging threat environment. They measured a facility's information security by assessing what measures were in place to reduce the risk value on an asset. In many cases, the methodologies used were nothing more than a collection of checklists. Some of the basic tools used for risk analyses in this generation were @RISK, ALRAM and RiscPAC [LAB 99].

2.2.2 Second generation risk analysis

In the second IT generation, as LANs proliferated and as the computing environments became more distributed, the first generation risk analysis methodologies were rendered obsolete. In fact, in that new environment, it became clear that combinations of threats were more serious and realistic than individual threats. In addition, the organizations started to realize that there was a need to focus not only on protecting equipment, but also on protecting the very data and information involved. The second-generation thinking formalized six concepts in risk analysis: (1) assets, (2) exposures, (3) threats, (4) impacts, (5) likelihood, and (6) countermeasures. Groups of asset (domains) were established to determine the total effect of the combination of threats on a group, as well as the exposures associated with that group. Risk-analysis approaches now involve more sophisticated mathematical equations based on priorities and weights. These approaches use both quantitative and qualitative techniques. The majority of risk-analysis

approaches are making use of automated tools, due to the extensive amount of data to deal with and the complexity of the calculation required. Tools codify expert knowledge about relationships between these six concepts. To assess a given system, the analyst applies the tool's encapsulated expert knowledge against a catalog of system assets to obtain a list of issues that need to be addressed. Thus, second generation systems began to allow the analyst to tailor assessments on a system-by-system basis. COBRA Risk Consultant is an example of an excellent second-generation tool still used for risk analysis. It provides an ISO 17799¹ [ISO 01] compliant risk analysis service, compatible with most recognised methodologies (qualitative and quantitative). It is a questionnaire based PC system using 'expert' system principles and an extensive knowledgebase. In the recent past, new security management tools have appeared on the market. These tools do not perform risk analysis but help to manage the risk. An example is Tivoli Secure Way Risk Manager (TSRM) [TIV 01] . TSRM is an enterprise-wide risk management solution enabling organizations to correlate security information from security auditing tools (see section 3.2), intrusion detectors (see section 3.1), firewalls (see section 3.3) and other security checkpoints. The integrated security management capability enables system administrators to monitor and assess the network security posture in real-time across an organization's multiple security checkpoints.

¹ ISO17799, is a detailed security standard. It is organized into ten major sections, each covering a different topic or area: Business Continuity Planning, System Access Control, System Development and Maintenance, Physical and Environmental Security, Compliance, Personnel Security, Security Organisation, Computer & Network Management, Asset Classification and Control, Security Policy

2.3 Today's environment versus existing methodologies

The last step in IT evolution happened when public networks became backbones for inter-organisational communication (such as via intranets) as well as for organisation-to-organisation communication (such as via extranets). The latest happened because of the requirement for global connectivity: everyone needs to talk to everyone. Today, messages travel across numerous networks with different sensitivity levels before arriving at their final destination. It is now almost impossible to determine which assets are involved during any given communication session. In addition, new types of attacks and exposures are being uncovered on a daily basis. Identifying threats is now really difficult because attacks often are undetected. Given this new environment, second generation risk analysis methodologies have evolved into a highly complex field that can only be tackled by experts. Besides, the time it takes to perform these methodologies seems to extend, rather than to decrease. Also, the conventional risk-analysis methodologies focus mainly on the identification of new security services and mechanisms. In our day, the problem with Information System (IS) security is not that secure technologies or products do not exist, but rather that ISs are not implemented and used effectively [LAB 99] . Conventional risk-analysis methodologies cannot be used to dynamically prioritize the implementation of countermeasures. Even if this would be possible, the gap between the need for security and the supply of security professionals is growing, and it is becoming more and more difficult, if not impossible, to perform meaningful risk analysis. In essence, there is neither enough time nor ample human

resources to perform conventional risk analyses in the new, distributed environments. Using the criteria defined in Table 2.1, the various IT generations were compared in Table 2.2 to pinpoint the distinctiveness of the third IT generation. Understanding the philosophy behind the conventional risk analysis methodologies and highlighting the distinctiveness of the third IT generation environment, it was possible to identify third generation risk analysis requirements.

Table 2.1. Criteria to evaluate security risk analysis requirements

Criteria	Definition
1. Service evaluation	Does the damage according to C/I/A change for different services provided by a network domain?
2. Threat assessment	Is it possible to know and understand all threats at the level where they could be accurately assessed?
3. Exposure assessment	Is it possible to know the assets' inherent exposures?
4. Probability estimates	Is it possible to estimate the probability for all identified threats?
5. Physical environment	Is the environment static in a way that it does not change on a regular basis?
6. Time	Is the environment static enough to be described and modeled in detail and still obtain valid results?
7. Human intervention	Is the cost of human intervention incurred in identifying and modeling the environment appropriate considering the period of time for which the results would remain valid?
8. Human expertise	Are there enough security experts available in this environment to meet the security requirements of all the organizations concerned?
9. Combination of threats	Are combinations of threats more serious and realistic than individual threats
10. Services dependencies	Are some services supporting others
11. Global Connectivity	Does everyone need to talk to everyone?

Table 2.2. IT generation comparisons

Evaluation Criteria	IT generations		
	First	Second	Third
1. Service evaluation	P	P	Y
2. Threat assessment	Y	P	P
3. Exposure assessment	Y	Y	Y
4. Probability estimates	P	P	P
5. Physical environment	Y	P	N
6. Time	Y	Y	N
7. Human Intervention	Y	Y	N
8. Human expertise	Y	P	P
9. Combinations of threats	P	Y	Y
10. Services dependencies	N	P	Y
11. Global connectivity	N	N	Y

Y= Yes N= No P= Partially

Table 2.2 indicates that the third-generation information technology environment requires a paradigm shift in terms of risk-analysis methodologies in order to effectively address the third generation distinctiveness. In fact, six of the eleven questions defined in Table 2.1 provide different answers, in Table 2.2, for the third IT generation than for the first and second. The foundations of the distinctiveness are raised by the following issues:

- The requirement for global connectivity implies the connection of services of different sensitivity levels (criteria 1 and 11)
- The third generation IT environment is of dynamic nature (criteria 5,6, 7 and 11)
 - Exposures are being discovered daily
 - Systems are altered daily
- There are dependencies between services in the same network domain (criteria 10, 11)

As previously mentioned, in our day, the problem with IS security is not that secure technologies or products do not exist, but rather that ISs are not implemented and used effectively. In fact, due to the distinctiveness of the new IT environment, the network operators are overwhelmed with network security flaws to fix. The list of security issues to be resolved changes dynamically because of the ever-changing nature of the communication networks and because new types of attacks and exposures are being uncovered daily. Also, the network operator “to do list” (security related) is so long that even if they have the security expertise required to take action, they don’t know where to start (being overwhelmed by the work to be done). It is difficult to envisage the use of the conventional risk analysis methods to help address the new expectations placed on the network operators. In fact, when the environment changes daily, one should wonder if these kinds of tools have the capability to deal with a dynamic environment (without getting automated input from the environment) and still obtain valid results. Even if this would make sense, it is doubtful that the cost of the human intervention incurred in identifying and modeling the environment every time it changed would be appropriate, considering the period of time for which the results would remain valid. By consequence, what is required is a decision support tool that processes the information from the environment (i.e.: network service value, exposure scanners, intrusion detection, firewall), and present dynamically a list of what is the next best thing to do to improve the security posture of the network. In the recent past, security management tools like Tivoli Secure Way Risk Manager (TSRM) have taken a step in that direction [TIV 01]. However, the purpose of these tools is mainly to correlate security

information from various security checkpoints. It is not to perform a detailed risk analysis evaluating the expected losses. In other words, the security management tools do not consider the fact that assets host different services of different value. Clearly, a Domain Name Server (DNS) is more valuable than a Clerk Personal Computer (PC). In addition, some assets might host services dealing with top-secret information and others only unclassified information. In consequence, when coming up with a prioritized list, the respective damage value should be considered.

2.4 Conclusion

To sum up, a new innovative model to lay out the basis for a new risk management tool is required to support the third generation IT environment. The model needs to employ an approach, according to which risk scenarios can be identified and related action items prioritized. The model needs to permit dynamic risk analysis. Dynamic risk analysis is based on performing automated risk assessments when the environment changes as opposed to performing risk assessment occasionally. Part 3 of the text provides more information about the model. The next chapter is devoted to a brief presentation of some network security technologies useful to provide information about the environment at risk.

Chapter 3 – Network Security technologies

3.1 Introduction

The purpose of this chapter is to briefly present various network security technologies.

The latter overview is deemed important, as it is aimed at facilitating the reader's understanding of how these technologies can be used to dynamically provide information about the computer network environment to the model. Most technologies represent and process exposures in one form or another. By consequence, this chapter first better defines the term “exposure” and then reviews the technologies.

3.2 Exposures

First, it is important to understand that threats and exposures are not the same. However, they are intrinsically related. In fact, exposures are defined as weaknesses of a network that create the conditions that allow a threat to trigger a loss [PEL 01] . The term exposure is used to describe and name all publicly known flaws about computer systems that could allow somebody to violate a reasonable security policy for that system [CVE 01] . In the literature, these facts are sometimes also referred to as vulnerability.

However, a review of the literature has revealed that the use of the term vulnerability is ambiguous. In fact, there are at least two common uses of the term “vulnerability”. This

is best illustrated via a simple example. Lets consider the finger² service. Since the finger service reveals user information, there are security policies that disallow finger from being run on some systems. Thus finger may be regarded as vulnerability according to this usage of the word. A narrower view holds that some security-related flaws are not 'true' vulnerabilities. With respect to the finger service, it may be argued that since finger behaves as it was designed to behave, it should not be considered as a vulnerability. The new non-ambiguous term currently used in the IT security world to refer to all weaknesses is the term exposure. In consequence, this is the term used in this text.

These days, enterprise computer networks use a variety of tools to assess their security posture, including security auditing tools (see 3.2.2) and intrusion detection system (see 3.2.3) from a wide variety of vendors. These tools can all provide information about the environment and they all represent and process exposures in one form or another. To be able to aggregate environmental data from the variety of technologies, a common exposure dictionary is required. In fact, without agreement on how to list and name the exposures, the integration task is more difficult due to the number of mappings needed.

The dictionary is required to:

- Enumerate and discriminate all known exposures.
- Assign a unique name to each exposure.

² A standard protocol specified in RFC-742. A program implementing this protocol lists who is currently logged in on another host. In short, finger is a computer command that displays information about people using a particular computer, such as their names and their identification number.

The MITRE³ Corporation offers a not yet official dictionary. The approach is called the Common Vulnerabilities and Exposures (CVE) initiative. Many technologies are presently CVE compliant. By agreeing to limit the use of CVE to the role of a logical bridge, MITRE avoids competing with existing and future commercial efforts [CVE 01]. This research assumes that a standard such as the one proposed by MITRE is used to allow the aggregation of the environmental data.

3.3 Security auditing tools

Security auditing tools (SAT) audit a network to find exposures. The analysis of a heterogeneous enterprise computer network for exposures is an overwhelming task. There are a number of tools to help an administrator evaluate a network for exposures. They are most often referred to as a scanner or as security-auditing tools. One could ask: Can these tools discover all known exposures? The answer to this question is “no”. Humphries et al [HUM 00] divide exposures into five different categories:

- Physical/Environmental;
- Network/Connectivity;
- Platform/Operating System;
- Application/Service;
- Human Policy.

³ MITRE, working in partnership with the US government, is an independent, nonprofit corporation working in the public interest

This definition of exposure implicitly assumes that there could be policy and physical security exposures. However, automated tools deal mostly with scanning for exposures associated with network connections, operating systems and applications/services.

Although it is recognized that physical and policy exposures could have significant effect on a system's overall security, they do not lend themselves to easy assessment using automated techniques. Therefore our model will not consider these exposures.

Nevertheless, this is not considered to be a problem since physical and policy exposures are more static in nature and hence, do not need to be dealt with dynamically.

Although there are a number of new approaches to assessing networks for exposures currently under development [HUM 00] the majority of available tools fall into the broad categories of host-based or network-based exposure assessment systems. These two types of tools have a number of fundamental differences and lend themselves to very different deployments in an organization. A host-based exposure assessment system (HES) runs on a specific host and is able to test the host for exposures unique to the operating system, resident applications, local services available, hardware configuration and local user profiles. The checks can be matched to the exact circumstances of the machine extremely well and, if configured properly, should produce very telling results. There are a number of HES's available including Titan, COPS (Computer Oracle and Password System), Tiger and a few commercial products available from the major computer security vendors. A network-based exposure assessment system (NES) is run from a central machine or suite of machines against a remote host across a network. The

intention is to see the target machine as a potential hacker would see the machine, and to assess the machine against a number of known exploits. There is no executable code placed on the target machine. Collection of exposure information across the network is quick and, again, if properly configured, the tool can be very effective. There are a number of NES's available including SATAN (Security Administrator Tool for Analyzing Networks), SARA (Security Auditor's Research Assistant), Nessus and Cybercop.

Each of the typical security auditing tools contains a number of strengths and weaknesses [CRO 01] . Organizations that want to take security auditing to the highest level would likely want to impose some mixture of network and host-based exposure assessment systems. This is not an ideal solution because of the additional complexity of using, training on and monitoring two tools for what really is a single purpose. In general, an NES has the strength of being centralized and scalable, while an HES has the advantage of being more powerful in its ability to determine all the exposures present on a host. The ideal tool would probably be one that can be centrally controlled and administered, while still having the strength of putting executable scans on each host. Note that most SAT attempt to arbitrarily rank the exposures scanned. In fact, they usually first rank exposures in terms of predetermined qualitative risk factors (high, medium, low). Once this is done, exposure identification numbers usually rank the exposures. Chapter 8 demonstrates that even if this is better than nothing, this is not adequate to be able to manage the risk efficiently.

3.4 Incident detection

The previous chapter explained that security weaknesses (exposures) in information systems are detectable by SAT. SAT indicates flaws that have the potential to lead to attack as well as incidents (successful attack(s)). There are also tools available on the market that monitor events occurring in a computer system and analyze them for signs of attack and incidents. These tools are called intrusion detection systems (IDSs). The outputs from IDSs provide information about the environment. The first part of this section defines the terms “incident” and “attacks” to make sure that the jargon is well understood. The second part of this chapter provides a brief overview of what IDSs are.

3.4.1 Attack and incident

An *attack* is a single unauthorized access attempt, or unauthorized use attempt, regardless of success. An *incident*, on the other hand, can involve more than one successful attacks that can be related by the goal of the end result. This concept is illustrated by the examples in Table 3.1. In the first example, many attacks lead to one incident. However, in the second example, one attack leads to one incident: a denial-of-service shutdown of the system.

Table 3.1. Attacks/incidents

	Attacks Examples	Incident
Example 1	<ul style="list-style-type: none"> • Copies password file, • Gains access to user account, • Then gains access to root privileges 	Copy files, software
Example 2	<ul style="list-style-type: none"> • Sends e-mail to flood system 	Denial-of-service

An attack can be performed to gain unauthorized access, and/or, given an authorized access, to use that access in an unauthorized manner. An attack can harm one or many services hosted by an asset on a network domain.

3.4.2 Intrusion detection systems

Intrusion detection is the process of monitoring the events occurring in a computer system or network, and analyzing them for signs of security problems. [GUR 00]

Analogous systems in other areas are burglar alarms and video-monitoring systems found in stores and banks. The bulk of intrusion detection research and development has occurred since 1980. However, this research has produced a wide range of proposed solution strategies for accomplishing intrusion detection goals. Until 1990, IDSs were largely host-based, confining their examination of activity to operating system audit trails or other host-centric information sources. In the simplest terms, IDSs consist of three functional components:

- An information source that provides a stream of events records
- An analysis engine that finds signs of intrusions

- A response component that generates reactions based on the outcome of the analysis engine

The automated detection and immediate reporting of these events are required to respond to information attacks against networks and computers. In intrusion detection, most analysis approaches involve misuse detection, anomaly detection, or some mix of the two. Misuse detection engines look for something that can be defined as bad. They filter event streams, searching for activity patterns that match a known attack or other violation of security policy. Anomaly detection engines look for something rare or unusual. They analyze system event streams using statistical techniques to find patterns of activity that appear to be abnormal. The leading technical approach to present day intrusion detection is multi-host network-based, which combines host based intrusion detection with network traffic monitoring [MUK 94] [SNA 91]. Current commercial IDS such as ISS RealSecure and Computer Misuse Detection System (CMDS) have distributed architectures using rules-based misuse detection, statistical-anomaly detection, or both. A significant challenge remains for IDSs designers to combine data and information from several heterogeneous distributed agents (and managers) into a rational method that can be used to assess the security of cyberspace. Multi-sensor data fusion technology is a significant possibility toward the development of extremely reliable IDS that identify, track, and assess cyberspace situations with multiple complex threats (See Figure 3.1).

Figure 3.1. Multiple complex threats

Today's network-based IDSs are not going to work unless there are sensors in place.

These sensors can be located a different place on the network to monitor internal or external traffic. Using these tools, it is essential to recognize that the sensors may not be able to observe all events. In fact, the following things can be observed:

- Events on a different network: Unauthorized "backdoor" connections into a network are very common.
- The IDS Sensor is not functioning.
- Events in the protocol that the IDS cannot decode are not observable.
- Events that occur above the sensor's maximum bandwidth-handling capability cannot be observed.
- The sensors are not placed correctly.

3.5 Countermeasures

Since attack use exposures and some exposures can be protected using countermeasures it is appropriate to review them quickly. Following is a list of common countermeasures:

- Firewalls
- Authentication devices
- Cryptography
- Virtual Private Networks
- Tunnelling (IPSec, SSL, etc.)
- Secure Links
- Public Key Infrastructure
- Digital Signature
- Cryptographic checksums
- Virus Scanners
- Backups
- Software Patches/ upgrades

Even though the countermeasures were listed, it is not important for the reader to understand the specifics of every one of them. In fact, the only thing that needs to be known is that when an exposure is countered it minimises or discards the risk. This is true for every type of countermeasure except for the firewall technologies. In fact, the firewalls are different from the other countermeasures because they have been created to

protect the network domain perimeter as opposed to specific assets. In other words, the firewalls are installed to protect the network domain from an external threat agent attempting to break in. Firewalls do not protect from internal threat. Usually, the firewalls secure the network domain point where the network connects to the Internet. In practice there may be several interfaces, but every additional one greatly increases the difficulty of securing the network domain. A firewall can be configured from a security management tool. A firewall is typically a combination of hardware and software used to make access control decisions about traffic on a network in order to enforce a policy at the point connecting the network to other networks. There are two basic types of firewalls. Application-level gateways, also known as proxies, reconstruct application data and use that additional information to allow or disallow traffic. Packet filters operate on raw packets to make access decisions. There are two types of packet-filtering firewalls. Stateless firewalls, such as router access control lists, simply consult rule tables and make decisions about packets in real time. State full firewalls maintain state and base decisions on the contents of the packets as well as on the information about other packets and connections. The boundary between packet filters and proxies is slightly blurred. There are state full packet filters that exhibit some of the properties of proxies. There are also proxies that do little more than reconstructing the original packets. For the purpose of this text the reader does not need to know a lot more about firewalls. The two key points to keep in mind are as follows: First, firewalls protect from external threat only. Second, firewalls cannot protect from any types of attack. For instance, if there is a packet-filtering firewall in place, and if a web Server is placed inside the network

perimeter, then, an exploitation of the web server could be used to launch an attack on the internal network.

3.6 Conclusion

The purpose of this chapter is to facilitate the reader's understanding of how technologies can be used to dynamically provide information about the computer network environment. The most obvious one is probably the SAT. SAT audits a network to find Network/Connectivity, Platform/Operating System and Application/Service exposures. The term exposure is used to describe and name all publicly known flaws about computer systems that could allow somebody to violate a reasonable security policy for that system.

The second category of technology reviewed is the IDS. The IDS processes and monitors the events occurring in a computer system or network, analyzing them for signs of security problems. Incident detection analysts use information from the IDSs to establish if an incident occurred on the network domain and the exposure(s) that were used to cause the incident. If there was an incident on a network exploiting a given type of exposure, the subject exposure type is more likely to represent a threat if nothing has been put in place to prevent the same type of incident.

Finally, from the network and the firewall configuration, it is possible to know if there is an external threat to the network or not.

PART 3 – A New Method For Security Risk Analysis

Chapter 4 – Risk Control Network Service (RCNS) – The Concept and the Model

4.1 Introduction

As the advantages of global connectivity multiply, so do the risks. Various ingenious techniques have been devised to infiltrate networks, and still other exposures are being uncovered and exploited each day. Today, despite the fact that the information technology environment has evolved a lot, the methodologies used to manage the risks have stayed the same. From chapter 2, it has become clear that the current risk-analysis methodologies are not sufficient and that an innovative risk-analysis approach is required. The requirement for the new approach is principally raised by the call for global connectivity and by the dynamic nature of the third generation environment. In fact, the conventional risk-analysis methodologies focus mainly on the identification of new security services and mechanisms. However, in our day, the problem with Information System (IS) security is not that secure technologies or products do not exist, but rather that ISs are not implemented and used effectively [LAB 99] . In fact, due to the distinctiveness of the new environment the network operators are overwhelmed by network security flaws to fix. In consequence, what they require is a decision support tool that processes the information from the environment (i.e.: network service value, exposure scanners, intrusion detection, firewall), and presents dynamically a list of what is the next best thing to do to improve the security posture of the network. So, this new

approach needed to be researched. For the purpose of this research, a system is considered to be composed of domains, assets and services. This is illustrated in Figure 4.1.

Figure 4.1. Information system (IS)

A domain, as illustrated in Figure 4.1, is a definable boundary within which a set of services is executed. We introduce the concept of domains to model large, complex

information systems managed by different groups. The equipment for which each group is responsible is part of that group's domain. Sometimes the organization chart determines the delineation. Domains consist of assets, which are defined as platform (ex: equipment used for input, storage, processing, transfers...) and interface equipment (ex: router, firewall). Finally, services are provided by assets. A service is defined as function provided to the domain's users or to the system itself.

In order to generate a prioritized actions list, risk analysis needs to be performed. It has become manifest from chapter 2 that the conventional risk-analysis methods cannot be used in relation with the new proposed concept. Consequently, an innovative method is required. One such possible approach is based on the assessment of risk of an attack associated with an exposure found by a given Security-Auditing Tool (SAT) on a given domain. This is illustrated in the UML class diagram [AMB 01] of Figure 4.2 .

Figure 4.2. UML class diagram representing the RCNS concept

Figure 4.2 also illustrates that an attack can affect zero to many services characterized by a list of attributes (confidentiality, integrity, availability, cost to regenerate, number of users, function). From the risk values, it is then easy to derive an action list for the network operators. That way, the exposures (flaws) implying the highest risk value would be considered first. The present chapter describes the proposed approach in more detail. The method is referred to as the “Risk Control Network Service”(RCNS) as inspired by Captain Luc Dandurand. Captain Dandurand originally imagined the RCNS as a possible way in which to manage risk by dynamically analyzing a wide range of information and prioritizing actions based on an innovative risk model. The purpose of this thesis is not to research all the aspects required to put the RCNS in place. Our objective is to define the risk model behind the service. In this chapter the RCNS model concept is first introduced. Then, a possible RCNS structure is presented to put things into context. Finally, the risk model formula is presented.

4.2 RCNS model concept

This section quickly explains the concept behind the researched RCNS model. As previously mentioned, the RCNS is seen as a method that provides a rapid and efficient means of evaluating the risk associated with every scanned exposure on a domain. The risk is evaluated for every exposure-asset pair. In fact, an attack using the same type of exposure on two different assets can affect different services. Consequently, the resulting

risk is not the same. The RCNS helps to manage the risk inherent to a domain, by distributing the knowledge of what security related flaws (exposure/asset pair), need to be fixed first. The flaw involving the highest risk needing to be fixed first. In other words, the RCNS provides a prioritized list of things to fix, security wise, for system administrators. The concept of the model is graphically summarized in Figure 4.3.

Figure 4.3. RCNS model concept

Figure 4.3 demonstrates that to cope with the dynamic nature of the new environment, the risk associated with every detected exposure is recomputed every time the data describing

the environment is altered. In other words, the level of risk is managed by modifying the prioritized action list when the environments change. We consider that the environment changes:

- When a new exposure is scanned on the network domain,
- When an incident is reported by an incident detection analyst on the network domain,
- When the importance of the services attributes defined in Figure 4.2 are altered,
- When the network domain firewalls are reconfigured or added,
- When the network domain configuration is modified.

This is explained in more detail in chapters 5 and 6.

4.3 RCNS structure

This section quickly presents our views about the RCNS structure. Figure 4.4 clearly demonstrates how we picture the RCNS as a possessor of three constituents: Consoles, Servers, and Asset Agents. To keep things simple, Figure 4.4 is composed of only one console and one server. Obviously, there could be more. This structure is inspired from discussions with Captain Dandurand. No such concept is discussed in the security literature. The purpose of this research is not to develop this structure. However, it is presented here to put our risk model into context.

Figure 4.4. RCNS structure

We imagine the role of the RCNS's three constituents as follows. The console is the graphical interface used by the system operator as well as the experts to interact with the RCNS. The server is used to store system-wide data. It also performs the computations related to our risk model (see section 4.4 and chapters 5 and 6). Besides, it implements the communication between the server and the asset agent, between the server and the configuration management tool and between the server and the security management tool. Finally it implements a network-based exposure assessment system (see chapter 3). asset agents run on each platform equipment assets on the network (interface equipment such as routers and switches cannot easily run external code). The system operator uses the

asset agent to get the data required to determine and set the value of the service attributes (see Figure 4.2) belonging to the asset. The service attributes are set when the asset is initially installed on the network. The attributes of the interface equipment services have to be entered manually in the database. The asset agents also run a host-based exposure assessment system (see chapter 3) to scan the assets for exposures according to the signature files sent from the server. The communications between asset agents and servers would require the usual security services of confidentiality (controlled access), availability, and integrity to prevent malicious exploitation of the system. The specific requirements within each of these security services, as well as the redundancy in the server components, are not presented since they are not deemed necessary to put our model into context. In short, the RCNS should not introduce additional exposures in the network, and should be able to operate in any environment.

4.4 Introduction to the risk model

This section briefly presents the formula and the procedure according to which our risk model computes the risk value for every detected exposure. The different parts of the risk formula and the theory behind them are described in detail in chapters 5 and 6.

4.4.1 Risk formula

The formula is based on the expected loss, which is defined as the damage value of the services at risk multiplied by how exposed they are [PFL 01] [PFL 96] [PEL 01] [NOR 00]. The damage value is estimated in monetary terms. The probability parameter

represents subjective probabilities. In fact, getting objective probability is not deemed necessary to develop a tenable ranking concept; what really needs to be known is that the probability of a successful attack is higher for an asset-exposure pair than for another but not as high as another one. The theory behind the estimation of both parameters is covered in chapters 5 and 6 respectively. We have previously introduced our approach as being based on the assessment of risk associated with every scanned exposure listed by a security-auditing tool. This implies that the risk is computed for every exposure in relation with the particular features of the exposure. Chapters 5 and 6 explain in details how these features are taken into account. For now, we only introduce our risk formula. This formula can then be used to calculate the risk associated with a given exposure. To calculate the risk value, the estimated damage value parameter is multiplied by the estimated probability parameter, given the characteristics of the exposure being analyzed. To clarify this concept, the following notation is introduced:

D = set of assets of the network domain ($i \in D$)

S = set of services of the network domain ($s \in S$)

S_i = set of services belonging to asset i ($s_i \subset S$)

K = set of relevant exposure types for the network domain ($k \in K$)

S_{ik} = Set of services affected by a successful exposure k attack on asset i ($s_{ik} \subseteq S$)

P_{ik} = relative probability of a successful attack of type k on asset i

V_{ik} = Total damage value caused to the domain services S_{ik} in monetary terms, by a successful exposure k attack on asset i

The global risk values for a given domain are assessed with the expression.

$$\text{GRV}_{ik} = P_{ik} V_{ik} \quad i \in D, k \in K \quad (1)$$

Note that this definition implies that the services affected by an attack k on asset i are not limited to those belonging to S_i . In fact, different exposures allow different types of attacks that can result in a different service $s_{ik} \subseteq S$ being compromised: one attack may culminate in compromising only s_i , whereas another attack may result in compromising other S_{ik} services. In addition, on every domain D there are dependencies between services S . Consequently, the damage of a parent service might lead to the child service being disturbed. For example, if the availability of the Domain Name Services (DNS) is compromised, this might culminate in a denial of service (DoS) for the domain Web Server.

4.4.2 Using the risk model

Recall that the risk is evaluated for every exposure k every time the data about the environment are altered. This is done using the following procedure. Every time there is a change in the domain environment, do:

- Estimate P_{ik} , $\forall i \in D, k \in K$

- Estimate V_{ik} , $\forall i \in D, k \in K$
- Compute GRV_{ik} , $\forall i, k$ with (1)
- Sort the asset/exposure pairs (i,k) in decreasing GRV_{ik} value order

4.5 Risk model implementation

This section briefly presents how we imagine the risk model implementation. This is done to demonstrate the feasibility of using the approach. The RCNS model uses two main spheres. For the purpose of the present thesis, the term “sphere” is defined as “a logical collection of components”. Figure 4.5 illustrates the said two spheres.

Figure 4.5. RCNS model architecture

The external resource spheres represent the resources required by the organization implementing the approach. It is fair to assume that organizations requiring a system such as the RCNS already have these resources in place. In fact, if they don't they should get them to make sure that their network domain is well managed and secure. Anyone in the organization can be considered an organizational expert if he or she has deep knowledge and strong practical experience in the organization business operations supported. In addition, the organizational expertise is only required once when the RCNS is implemented.

The RCNS sphere, in turn, consists of four components (groups of components for asset agents), namely the knowledgebase, the database, the inference engine and the assets agents. The functions of the asset agents were defined in section 4.3. The three other components are defined as follows:

- Knowledgebase: contains the information and the processes useful for problem solving.
- Database: includes a set of facts.
- Inference engine: carries out the rezoning whereby the system reaches a solution. It links the process and the information given in the knowledgebase with the facts in the database.

All communication sessions between the different components of the two spheres are effected through the inference engine. Based on the information and the process

stipulated in the knowledgebase and on the facts contained in the database, a risk value is determined for each i,k pair every time the environment changes. The inference engine then sorts the risk value in decreasing order. The knowledgebase and the database are kept separate, owing to the type of information contained in each base. The database contains factual information that is information that is specific. New information needs to be added as the environment changes. However, this information is easy to obtain. The knowledgebase, on the other hand, contains more subjective information, which is more difficult to get. Nevertheless, the information requiring a good deal of groundwork is only requested once before the model can first be implemented. The processes inherent to the calculation of V_{ik} and P_{ik} are built in the knowledge base, they do not need to be modified and are ready to be used by the inference engine. So, once the RCNS is implemented, the operator's responsibility is only to keep the database up to date. Part of this could be done through software patches.

4.6 Conclusion

It should now be clear to the reader that our research aim is to define the RCNS model and the processes to build such a model. It is not to research all the aspects required to put the RCNS in place. We spent the last part of this chapter presenting the formula on which our risk model is based (equation (1)) and the risk model architecture. Chapter 5 and 6 explain how the P_{ik} and V_{ik} parameters can be subjectively estimated in practice and the theories behind this.

Chapter 5 Estimation of the damage value parameter in the risk value formula

5.1 Introduction

It makes sense to assume that the risk derives from the damage value incurred in monetary terms [PFL 01] [PFL 96] [PEL 01] [NOR 00]. Estimating V_{ik} defines two problems: First, the designation of the service attributes⁴ (see Figure 4.2) defining the service value and then the estimation of the respective values for each attribute. Chapter 4 provided a foretaste regarding the attributes of concern (see section 4.2). To be included in an economic analysis, positive and negative attributes of the alternatives⁵ need to be denominated in dollar terms as monetary costs. However, the service attributes listed in Figure 4.2 are not readily expressed in monetary terms. Consequently, there is no simple way to combine these attributes into a single measure of financial worth. Because the non-financial characteristics are especially important, we need to use concepts and methods that provide the capacity to account for the attributes of a general nature (confidentiality, integrity, availability, number of users and function). Multi-attribute Decision Making (MADM) methods consider non-financial attributes (qualitative and quantitative) in addition to common financial worth measures when evaluating alternatives. The first part of this chapter justifies our choice of MADM

⁴ Attributes represent the different dimensions from which an alternative can be viewed [TRI 00]

⁵ In the context of this paper alternatives are related to the different services that can be affected by an attack of type k (see figure 4.2). In consequence, the set of alternatives is assumed to be finite ranging from several to hundreds.

method. The second part of this chapter provides detailed information on how V_{ik} is estimated using the chosen MADM method.

5.2 Multi-attribute Decision Making (MADM)

5.2.1 General overview

The assessment of V_{ik} is a multi-dimensional problem, which justifies the use of a MADM method. MADM is one of the most well known branches of decision-making. MADM methods concentrate on problems with discrete decision spaces where the set of decision alternatives has been predetermined. There are many MADM methods but there are not many that can provide the final scores in monetary value. In fact, the most popular methods (according to Chen and Hwang [CHE 91]) all provide unitless “desirability scores”. Our research for a method applicable to our problem, lead us to the Non-traditional Capital Investment Criteria (NCIC) method. Boucher and MacStravic developed this method [BOU 91]. The methodology takes advantage of some of the techniques of a well-known MADM method: the Analytical Hierarchy Process (AHP) as primarily developed by Saaty [SAA 80] . NCIC was created to overcome some of the criticisms about the AHP, which have appeared in the literature [BOU 91][BOU 97] , and to tie multi-attribute evaluation of alternatives more closely to traditional present worth analysis⁶. To accomplish this latter objective, NCIC provides final scores in dollar value, rather than producing unitless “desirability scores”. Consequently, the method

⁶ Present worth is the equivalent value at time zero (the present) of a set of cash flows[PW 02].

represents the most attractive approach for this research. The NCIC method is described in detail in the following sub-section.

5.2.2 Nontraditional Capital Investment Criteria (NCIC)

The procedure for applying NCIC is similar in some respects to AHP (AHP is explained in appendix A) and consists of four steps [BOU 96]:

1. Identify the evaluation attributes and the alternatives,
2. Make pairwise comparisons to determine the relative importance of attribute for each alternative,
3. Evaluate judgmental inconsistency from the pairwise comparison processes,
4. Compute the worth of each alternative based on the value of the traditional and non-traditional attributes.⁷

This section first introduces the set of underlying assumptions and features of NCIC. The procedures and computational techniques are explained in greater detail in the next section.

5.2.2.1 Underlying assumptions and features of NCIC

NCIC reflects both a set of underlying assumptions and a set of procedural and computational techniques used to practically implement the method. The basic logic of NCIC is based on the following assumptions:

⁷ The Non-traditional attributes are the attributes of non monetary nature

- **Alternative scores:** NCIC develops numerical scores, which characterize the total implied value of each alternative v_s (for each of the alternatives, $s = 1, \dots, n$).
- **Variable attribute weights:** The relative importance of attributes is not assumed to remain the same across alternatives. Instead, the importance of attributes changes upon each alternative. Consequently, NCIC uses changing weights to characterize the relative importance of the attributes or sub attributes.
- **Contributions to value:** Each attribute j contributes an increment of value v_{sj} , which can be either positive or negative, to the total value of the alternative v_s .
- **Additive:** The separate increments of value are additive. In other words, the total implied value of an alternative v_s is defined as the sum of the value increments associated with its performance relative to each attributes.

NCIC uses the following procedures:

- **Pairwise comparisons:** NCIC converts the problem of specifying the increments of value for each alternative v_s into the problem of making a series of attributes pairwise comparisons. For each pair of attributes (“ j ” and “ u ”) compared, the decision maker responds to the question “How much more valuable is this alternative’s relative to attribute j than to attribute u ?”. NCIC summarizes the results of pairwise comparisons in a Pairwise Comparison Matrix (PCM) (see appendix A, Figure A.1).

- **Principal eigenvector method:** NCIC uses the principal eigenvector method [SOS 02][SAA 80] to convert the PCM into a vector of weights. Boucher and MacStravic recommend the use of the consistency check suggested by Saaty for use with AHP (see appendix A) to check for consistency among the pairwise comparisons in the PCM.
- **Hierarchy:** The NCIC method allows describing a multi-attribute decision problem hierarchically in a tree-structure, dividing attributes into sets of sub attributes. NCIC allows the hierarchies of attributes to be different for different alternatives. Consequently, if there is an attribute, which is associated with only one of the alternatives, then it is included only in the tree-structures defined for that alternative.
- **Implied increments of value:** NCIC includes calculations, which convert the vectors of covering attributes weights into implied increments of value v_s . In principle, v_s can be expressed in the units of measurement associated with any one of the measurable attributes. However, NCIC uses a monetary attribute as the bridge attribute, so that the increments of value are all expressed in monetary terms.

The following sub-sections describe in greater detail how NCIC uses the procedures and computational methods that were just introduced.

5.2.2.2 Specifying a baseline alternative

At the beginning of a MADM analysis with NCIC, a baseline alternative needs to be specified, against which all other alternatives are judged. In other words, for each alternative, decision makers assess the increments of value added (or subtracted) by each of the differences in performance between the alternative and the baseline. Boucher and MacStravic [BOU 91] recommend that the baseline alternative represent the “statusquo”.

5.2.2.3 Use of hierarchy in NCIC

Appendix A presents the rationale for structuring attributes and sub attributes with AHP. This rationale holds for complex MADM problems using NCIC just as for AHP. There are, however, two practical differences in the use of hierarchy between the two methods. First, NCIC acknowledges that one or more attributes may be significant for only certain alternatives. NCIC allows constructing a separate attribute tree-structure for each alternative when needed. The tree-structures for each alternative contain only those attributes that detract from the baseline alternative. Second, NCIC requires that each tree-structure contain the bridge attribute.

5.2.2.4 Pairwise comparisons

Recall that NCIC converts the problem of specifying the increments of value for each alternative v_s into the problem of making a series of pairwise comparisons. In NCIC, the separate sets of pairwise comparisons are made among the pertinent attributes for each alternative. The increments of value attributed are compared to each of the separate

ways in which an alternative differs from the baseline alternative. The individual value increments are additive. Therefore, if an attribute is composed of several sub attributes, then the incremental value of an attribute is equal to the sum of the incremental values associated with each of its sub attributes. For this reason, only the covering attributes⁸ (leaves attributes) of a tree-structure need to be included in the pairwise comparisons. When the number of covering attributes for a given alternative exceeds, say, 10 or so, the total number of paired comparisons can be reduced by grouping the covering attributes into two or more sets. Then, a separate PCM is developed for each set of covering attributes. A tree-structure template generally suggests appropriate sets of attributes.. The final synthesis of the results obtained from separate PCMs requires some overlap of attribute between the sets. This is done by including the “bridge attribute” in each set of covering attributes formed.

5.2.2.4.1 Computing incremental values

The PCMs in NCIC contain the decision maker’s judgments comparison, for a given alternative. The values of differences from the baseline alternative are compared with respect to pairs of attributes. In other words, alternative s diverges from the baseline alternative with respect to attributes j and u . Each of these differences adds (or subtracts) an increment of value (v_{sj} and v_{su}) to alternative s . Instead of asking the decision maker to estimate these value increments directly, NCIC asks the decision maker to compare the value increments associated with pairs of attributes. For example, the elements of the

⁸ The covering attributes are referred to as the leaves attributes in the graph theory. They are at the bottom of each branch of the tree-structure .

PCM for alternative s are estimate of the ratios of the incremental contribution of attribute j (v_j) and attribute u (v_u). This is illustrated in Figure 5.1

Figure 5.1. NCIC attributes PCM for alternative k

$$[v_j / v_u] = \begin{bmatrix} 1 & v_1 / v_2 & v_1 / v_3 & \dots & v_1 / v_m \\ v_2 / v_1 & 1 & v_2 / v_3 & \dots & v_2 / v_m \\ v_3 / v_1 & v_3 / v_2 & 1 & \dots & v_3 / v_m \\ \dots & \dots & \dots & 1 & \dots \\ v_m / v_1 & v_m / v_2 & v_m / v_3 & \dots & 1 \end{bmatrix}$$

Boucher and MacStravic recommended using Saaty's 1-9 numerical scale (see appendix A, Table A.1) to fill up the PCM in Figure 5.1. The diagonal elements are all equal to 1, because each value is exactly as important as itself ($j = u$). The elements below the diagonal are equal to the reciprocals of the corresponding elements above the diagonal. In consequence, only half of the matrix needs to be filled in by the decision maker. If the judgments were perfectly consistent, then the columns of the PCM would all be scalar multiples of each other, and any column could be chosen to represent the relative values. However, decision makers do not generally provide perfectly consistent judgments for the PCM. Instead of choosing any single one, it is best to somehow combine them all and find a compromise among them. NCIC (like AHP) uses the principal eigenvector method to derive a vector from the entire matrix, which serves as such a compromise. Also like AHP, NCIC utilizes an eigenvalue-based check of the consistency among the pairwise comparisons (see appendix A). In general, the inconsistency ratio needs to be

less than 0.1 or so to be considered reasonably consistent. The eigenvector and the inconsistency ratio can be obtained using an appropriate software.

Based on Figure 5.1, if we divide the PCM principal eigenvector $\underline{e}$ by $\underline{e}$'s first element (e_1), we obtain a vector, which serves as an approximation of the ratio's incremental values, as presented in equation (2).

$$\underline{e}(1/e_1) \cong [1 \quad v_2/v_1 \quad v_3/v_1 \quad \dots \quad v_n/v_1] \quad (2)$$

Now, recall that NCIC calls for including a monetary bridge attribute into each set of attributes. Let this attribute be attribute 1 in Figure 5.1. The bridge attribute is the one attribute for which the monetary value of its increment (v_1) needs to be explicitly known prior to the NCIC analysis. Then, by multiplying the eigenvector by the known (monetary) incremental value, we obtain the estimate of the incremental values for every attribute. In fact, the contribution for, let's say, attribute j can be computed with the relation:

$$v_j = (e_j/e_1) v_1 \quad (3)$$

The increments of values for a given alternative s are then summed to obtain the estimate of the total value (v_s) for the alternative. The total value for each alternative can then be converted to present value if required.

5.3 Building the risk model

The purpose of this section is to provide more information on how the damage value parameter V_{ik} is estimated. The first part of this section presents the procedure used to develop a damage value formula and defines the notion of service “harm value” which is essential to estimate the damage value. The last part of this section uses an example to demonstrate how NCIC is used to evaluate the service “harm value” and finally V_{ik} .

5.3.1 Damage value procedure

It is very difficult to estimate the amount of damage caused by an attack [AVI 01] .

However, to be able to rank the exposures, we only need ballpark figures. From chapter 4, recall that different exposures of type k allow different types of attacks that can result in different services S_{ik} being compromised. Also, for a domain D there are essential dependencies between services S that lead to additional services S_{ik} being affected. For example, if an exposure allowed a Denial of Service (DoS) attack on a DNS server, this most likely also implies a DoS attack on the domain web server. This example also demonstrates that the services affected by an attack k on asset i are not limited to those belonging to S_i . For the purpose of this research, we define V_{ik} as the sum of the “harm

values” associated with the services S_{ik} that can be affected by an attack performed by using an exposure k on a given asset i . To clarify this concept, the following notation is introduced:

m_{sik} = harm value caused to a service $s \in S_{ik}$ in monetary terms by a successful exposure k attack on asset i .

Thus V_{ik} can be computed using the following procedure

- Identify all services $s \in S$ that could be affected by an attack performed by using exposure k on asset I (S_{ik}).
- Evaluate the “harm value” m_{sik} associated with every service $s \in S_{ik}$
- Sum up the “harm values” associated with every compromised service $s \in S_{ik}$ to get the damage value:

$$V_{ik} = \sum_{s \in S_{ik}} m_{sik} \quad (4)$$

5.3.2 Calculation based on NCIC

As previously mentioned, m_{sik} needs to be calculated for the various services $s \in S_{ik}$ that could be affected by an exposure k on asset i . Evaluating the harm values associated with every service defines two problems: first, the designation of the attributes involved in the evaluation and second, the estimation and the amalgamation of the respective values. This section first represents the tree-structure template that is used to determine the attributes applicable to given alternatives (see Figure 5.2). Recall that NCIC allows

the hierarchy for each alternative to contain only those attributes that detract from the baseline alternative. In this condition, if there is an important attribute, which is associated with only one of the alternatives, then it is included only in the tree-structure defined for that alternative.

Figure 5.2. Attributes tree-structure template

In chapter 4 a service was defined as: “a function provided by the network domain to the domain’s users or to the system itself”. So, there are two basic types of services. A service can be a “user” service or a “system” service. The user services are the ones that are used directly by the users. The system services are only there to support the user services. As Figure 5.2 illustrates, the highest level of our hierarchy is broken down into two groups: the “loss value” group, and the “service importance” group. Note that only the “loss value” group of attributes characterizes the system services. This is because the

business operations (function) and the users are only disturbed if the user services are affected. This means that if a system service is compromised, the business operations and the users are troubled only if the users services that rely on this specific system service are affected. The procedure used to calculate V_{ik} , forces the consideration of the dependency between the user and system services while identifying the affected services. By consequence, only the users services need to include the service importance group of attributes to compute m_{sik} . To better define the sub-attributes included in the two groups, the following notation is introduced:

S_u = Set of user services of the network domain ($S_u \subset S$)

The loss value group of attributes consist of every attribute that, if affected, implies a direct loss of some sort. The most obvious attribute specific to every service $s \in S$ is the direct cost to regenerate the service. The sensitivity level of this attribute is evaluated in monetary terms. Three non-financial attributes are also specific to every service $s \in S$. In fact, an attack compromising the Confidentiality, Integrity and/or Availability (C/I/A) of a service can also imply a considerable loss. The “Information Technology Security Architecture Handbook” [CIS 94] sensitivity descriptions, are used to define the sensitivity level of every $s \in S$ with respect to the C/I/A. The sensitivity levels qualitative scales are represented in Tables 5.1 to 5.3 for each of the C/I/A attributes, respectively.

Table 5.1. Sensitivity rating definitions with respect to confidentiality

Confidentiality Rating	Type of Information
No Sensitivity	The information can be seen by anybody
Low Sensitivity	The information should only be disclosed if needed (Need-to know)
Medium Sensitivity	Unauthorized disclosure could be prejudicial to the organization interest
High Sensitivity	Disclosure could endanger the organization under study
Very High Sensitivity	Disclosure could result in exceptionally grave danger to the organization

Table 5.2. Sensitivity rating definitions with respect to integrity

Integrity Rating	Consequences of inaccurate or incomplete data to user's capability
No Sensitivity	No consequence
Low Sensitivity	Minor reduction
Medium Sensitivity	Moderate reduction
High Sensitivity	Major reduction
Very High Sensitivity	Complete stop

Table 5.3. Sensitivity rating definitions with respect to availability

Availability Rating	Acceptable down time for the user
No Sensitivity	
Low Sensitivity	Less than 48 hours
Medium Sensitivity	Less than 8 hours
High Sensitivity	Less than 4 hours
Very High Sensitivity	Restoration must be immediate (Less than 5 minutes)

The “harm value” attributes framework hierarchy presented in Figure 5.2 also includes the services’ importance group of attributes. These attributes specify the relative

importance of the services $s \in S_u$ with respect to one another. The first attribute refers to the number of service's users. The second attribute (function) is related to the importance of the services $s \in S_u$ with regard to the business operation. Although the number of users attribute is "countable", it is characterized by a fixed number of intervals so that it can be treated in the same way as the other attributes. The number of intervals is limited. The restriction is imposed by the fact that the NCIC makes a series of pairwise comparisons using a 1 to 9 linear scale (see appendix A, Table A.1). The services $s \in S_u$ are also categorized according to their importance with respect to the business operations. That way, at an equal risk level, the most important service would be considered first. For multi-function services, the most critical function determines the classification categorization of the service. The classification categorization of the service functions is in terms of the effect on the business operations success. The definition of the operation success varies depending on the area concerned. In the financial sector, success is related to financial gain. In a military command and control environment, success can be associated with saving lives. For another corporation, success might rely on the level of productivity. Table 5.4 outlines our generic approach for prioritizing a large inventory of services $s \in S_u$. We categorize the services according to general operations criticality. These categories could be expanded and/or altered to better fit a given organization. We define operation critical user's services as follows: All services $s \in S_u$ whose loss would preclude the safe and successful execution of the business critical functions.

Table 5.4. Sensitivity rating definitions with respect to the service function

Function Rating	
Not Required	These services do not support the task or mission in question.
Nice-To-Have	These services support the given task or function, but are not critical to its safe and successful completion.
Necessary	These services are identical to the essential services except that a known work-around or backup exists.
Essential	Services, which meet the definition of operation criticality above for the task or function in question. As well, there is no identified manual work-around or backup system that could support this function should the particular service fail.

Note that to implement the model it is not necessary to specify the sensitivity level of every service attribute $s \in S_{ik}$ every time that the damage value V_{ik} has to be calculated.

A standard list of attributes and sensitivity levels can be prepared when the risk analysis system is implemented for every service $s \in S$ and subsequently modified as needed. An example of such a list for the small network domain scenario illustrated in Figure 5.3 is given in Table 5.5. The services s provided by the network domain in Figure 5.3 are enumerated and are listed in the first column of Table 5.5. The second and third column of Table 5.5 lists the attributes for every service and their sensitivity levels according to the template presented in Figure 5.2.

Figure 5.3. Small network domain scenario **Table 5.5. Standard list of attributes and sensitivity level for Figure 5.3**

Services	Attributes	Sensitivity Level
System Services		
Routing Service (s=13)	Cost to regenerate	100\$
	Confidentiality	Low
	Integrity	Very High
	Availability	Very High
Firewall Service (s=14)	Cost to regenerate	100\$
	Confidentiality	Low
	Integrity	Very High
	Availability	Very High
Switching Service (Hub) (s=12)	Cost to regenerate	80\$
	Confidentiality	Low
	Integrity	High
	Availability	High

WorkStation1 Operating Service (WIN NT WS) (s=11)	Cost to regenerate	50\$
	Confidentiality	Low
	Integrity	Low
	Availability	Low
WorkStation2 Operating Service (WIN 2000 WS) (s=7)	Cost to regenerate	50\$
	Confidentiality	Low
	Integrity	Low
	Availability	Low
Server 1 Operating Service (s=4)	Cost to regenerate	75\$
	Confidentiality	Low
	Integrity	Med
	Availability	Med
Server 2 Operating Service (s=2)	Cost to regenerate	200\$
	Confidentiality	Low
	Integrity	Med
	Availability	Med
Domain Name Service (DNS) (s=1)	Cost to regenerate	1000\$
	Confidentiality	Med
	Integrity	High
	Availability	Med
User Services		
Outlook (s=10 & s=6)	Cost to regenerate	250\$
	Confidentiality	Low
	Integrity	Low
	Availability	Low
	Number of users	2
	Function	Necessary
Office Automation Service (s=8)	Cost to regenerate	100\$
	Confidentiality	Low
	Integrity	Low
	Availability	Low
	Number of users	2
	Function	Necessary

Web Browser Service (s=9 & s=5)	Cost to regenerate	50\$
	Confidentiality	Low
	Integrity	Low
	Availability	Med
	Number of users	2
	Function	Necessary
Web Server Service (s=3)	Cost to regenerate	200\$
	Confidentiality	Low
	Integrity	Med
	Availability	Low
	Number of users	Unlimited
	Function	Necessary
Internet (s=15)	Cost to regenerate	50\$
	Confidentiality	Low
	Integrity	Low
	Availability	Med
	Number of users	2
	Function	Necessary

Note that for a given exposure $k \in K$, all the attributes in Table 5.5 are not necessarily relevant. In what follows, we assume that the cost attribute is always there, but it may be null. The other attributes are considered as qualitative and the impact of a successful attack on these attributes has a different intensity depending on the affected services in S . As Table 5.5 illustrates, the sensitivity levels in Figure 5.2 characterize the intensity. The multi-criteria analysis method NCIC is then used to obtain monetary attribute values. When using NCIC, the covering attributes used are always composed of a base attribute qualified by a sensitivity level. A possible covering attribute would be “Availability-low”, for example. To implement this we define:

A_{sk} = set of covering attributes (i.e base attribute/sensitivity level pairs) applicable to service s under exposure k .

The next sub-section illustrates the concept via a simple example.

5.3.2.1 Evaluating a given exposure V_{ik}

Using the description of the attributes presented in the previous section, it is possible to evaluate the potential damage associated with an exposure. The concept of the undertaken evaluation is best illustrated via a simple example. Next V_{ik} is determined for i = server 2 ($i=2$) and k = "Syslog write enable (SWE)"($k=1$) according to the scenario illustrated in Figure 5.3. The SWE exposure allows writing information to the Syslog. This means that an attacker could write enough erroneous data to the Syslog file to fill the log files and cause a hard disk failure. Tables 5.6 and 5.7 summarize the data required to calculate V_{21} .

Table 5.6. Small network domain scenario covering attributes for SWE ($k=1$)

Services	Covering Attributes		
	Base attributes	Sensitivity Level	
System Services			
Domain Name Service (DNS) ($s=1$)	Availability	Med	} A_{11}
Server 2 Operating Service ($s=2$)	Integrity	Med	} A_{21}
	Availability	Med	
User Services			
Web Server Service ($s=3$)	Availability	Low	} A_{31}
	Number of users	Unlimited	
	Function	Necessary	

Table 5.7. Small network domain scenario cost attributes for SWE ($k=1$)

Services	Cost to regenerate
DNS	\$1000
Server 2 Operating Service	\$200
Web Server	\$0

The procedure in section 5.3.1 first tells us to identify all services in S that could be affected by an attack performed by using exposure k on asset i . The SWE exposure on server 2 can compromise three services as described in Tables 5.6 and 5.7. The SWE exposure demonstrates how the model deals with the interdependencies between the services. A successful attack using the SWE exposure on server 2 compromises the availability of Server2's DNS. This automatically leads to a Denial of Service of server1's Web Server.

The second step in the procedure presented in section 5.3.1 tells us to evaluate the "harm value" m_{s21} associated with every service (user and system) $s \in S_{21}$ in monetary terms. For the scenario presented in Figure 5.3, the costs to regenerate all services $s \in S_{21}$ were provided in Table 5.7. The other attributes are qualitative so the multi-criteria analysis method NCIC is used to obtain monetary attribute values. Recall that, when using the NCIC method, the covering attributes used are always composed of a base attribute qualified by a sensitivity level.

At the start of a MADM analysis with NCIC, the decision maker must specify a baseline alternative against which all other alternatives are judged. In our case, the Baseline

alternative is the “status quo”, that is the case where an attack is not successful. The NCIC’s method also requires determining a monetary attribute to be able to convert the vectors of covering attributes into implied increments of value. In fact, NCIC needs to use this attribute to express all increments of value in monetary terms. For each alternative, the increments of value are obtained by making a series of pairwise comparisons ($A_{sk} \times A_{sk}$). For each pair of attributes (“j” and “u”) being compared, the decision maker responds to the question: “How much more waste is incurred relative to attribute j than relative to attribute u?” Recall that the pairwise comparisons are made versus the baseline alternative. The challenge with that is that for some alternatives, like for the SWE, the delta between the status quo and the alternative for the “cost to regenerate” attribute is null (ex: the Web Server in Table 5.7). At first this does not seem like an issue because the NCIC method allows for some attributes not to be present. However, the “cost to regenerate” attribute is the only monetary attribute and the NCIC method needs a monetary attribute to convert the vectors of covering attributes into implied increments of value. Our solution to this problem is to define a new monetary attribute and to use it as the bridge only. The incremental waste value associated with this new attribute is fixed in advance. As it is demonstrated in chapter 8 this attribute can take a range of values. This makes sense because often data in MADM problems are imprecise and changeable. However, the sensitivity analysis performed in chapter 8 demonstrates that the use of the Saaty’s scale (appendix A, Table A.1) bounds the range of monetary value that the bridges attribute can take. To clarify this we define:

v_{amax} = the maximum incremental waste value that can be incurred by a relevant attribute

v_{amin} = the minimum incremental waste value that can be incurred by a relevant attribute

v_{BA} = the predefined incremental waste value associated with the bridge attribute in monetary terms

Then, the range of value that can be taken by v_{BA} is restricted as follows:

$$\frac{v_{amax}}{9} \leq v_{BA} \leq v_{amin} * 9 \quad (5)$$

To recapitulate, for a given service $s \in S_{ik}$ and an exposure k the NCIC method analysis is constructed by evaluating the increments of value ratio with respect to the baseline alternative for the corresponding $(A_{sk} \times A_{sk})$ PCM. This exercise needs to be performed by organizational experts in collaboration with the RCNS expert using the Saaty's value scale (see appendix A, Table A.1). Using an appropriate software the eigenvalues e_a , $a \in A_{sk}$, can then be obtained. Next, (3) can be used to compute the monetary value of each attribute, that is

$$v_{saik} = \left(\frac{e_{sa}}{e_{BA}} \right) v_{BA}, a \in A_{sk}, s \in S_{ik} \quad (6)$$

Finally, the harm value in monetary terms of all the attributes used for service s is obtained with:

$$m_{sik} = c_{sik} + \sum_{a \in A_{sk}} v_{saik} \quad (7)$$

Where c_{sik} = direct cost to regenerate service s after a successful attack of type k on asset

i. Figure 5.4 illustrates how m_{s21} is calculated for the services affected by the SWE exposure on server 2 ($s \in S_{21}$) of Figure 5.3. Five steps are used for every affected service to clearly demonstrate the process. A bridge attribute $v_{BA} = \$2500$ was used to carry one with the example. Table 5.6 and 5.7 provide the information required to perform the calculation.

Figure 5.4. Evaluation of SWE services harm for the scenario in Figure 5.3**DOMAIN NAME SERVICE (s=1)****Step 1: Identify the Harm value attributes** **Step 2: Create covering attributes PCM**

	Bridge Attribute \$2500 (BA)	Availability -Med(A)
Bridge Attribute (BA)	1	v_{BA}/v_A
Availability -Med (A)	Not required	1

Step 3: Calculate the eigenvector for the PCM created in step 2

e for this matrix is of the form $[e_{1BA}, e_{1A}]$ with $\sum e_{sa} = 1$

Step 4: Calculation of the increment of value

Weights	Multiplied by	v_{BA}	equals	Respective increment of value (\$)
e_{1A}/e_{1BA}	*	2500\$	$\cong$	$v_A/v_{BA} * 2500$ (Availability Med)$

Step 5: Calculation of m_{sik}

$$m_{121} = \$1000 + (e_{1A}/e_{1BA} * 2500\$)$$

SERVER 2-OPERATING SYSTEM (OS) (s=2)

Step 1: Identify the Harm value attributes

Step 2: Create covering attributes PCM

	Bridge Attribute \$2500 (BA)	Integrity - Med (I)	Availability - Med(A)
Bridge Attribute (BA)	1	v_{BA}/v_I	v_{BA}/v_A
Integrity - Med (I)	Not required	1	v_I/v_A
Availability -Med	Not required	Not required	1

Step 3: Calculate the eigenvector for the PCM created in step 2

e for this matrix is of the form $[e_{2BA}, e_{2I}, e_{2A}]$ with $\sum e_{sa} = 1$

Step 4: Calculation of the increment of value

Weights	Multiplied by	v_{BA}	equals	Respective increment of value (\$)
e_{2I}/e_{2BA}	*	2500\$	$\cong$	$v_I/v_{BA} * 2500\$$ (Integrity)
e_{2A}/e_{2BA}	*	2500\$	$\cong$	$v_A/v_{BA} * 2500\$$ (Availability)

Step 5: Calculation of m_{sik}

$$m_{221} = \$200 + (e_{2I}/e_{2BA} * 2500\$) + (e_{2A}/e_{2BA} * 2500\$)$$

WEB SERVER (s=3)

Step 1: Identify the Harm value attributes **Step 2: Create covering attributes PCM**

	Bridge Attribute \$2500 (BA)	Availability - Low (A)	Nbr of Users Unlimited (NU)	Function – Nec (F)
Bridge Attribute (BA)	1	v_{BA}/v_A	v_{BA}/v_{NU}	v_{BA}/v_F
Availability Low	Not required	1	v_I/v_A	v_I/v_F
Number of Users U	Not required	Not required	1	v_{NU}/v_F
Function - Nes	Not required	Not required	Not required	1

Step 3: Calculate the eigenvector for the PCM created in step 2

$\underline{e}$ for this matrix is of the form $[e_{3BA}, e_{3A}, e_{3NU}, e_{3F}]$ with $\sum e_{sa} = 1$

Step 4: Calculation of the increment of value

Weights	Multiplied by	v_{BA}	equals	Respective increment of value (\$)
e_{3A} / e_{3BA}	*	2500\$	$\cong$	$v_{3A} / v_{3BA} * 2500\$$ (Availability)
e_{3NU} / e_{3BA}	*	2500\$	$\cong$	$v_{3NU} / v_{3BA} * 2500\$$ (Number of users)
e_{3F} / e_{3BA}	*	2500\$	$\cong$	$v_{3F} / v_{3BA} * 2500\$$ (Function)

Step 5: Calculation of m_{sik}

$$m_{321} = (e_{3A} / e_{3BA} * 2500\$) + (e_{3NU} / e_{3BA} * 2500\$) + (e_{3F} / e_{3BA} * 2500\$)$$

The third step in the procedure presented in section 5.3.1 tells us to calculate the damage value V_{ik} using (4). For the scenario presented in Figure 5.3 and from the harm values calculated in Figure 5.4:

$$V_{21} = m_{121} + m_{221} + m_{321} = \$1000 + (e_{1A} / e_{1BA} * 2500\$) + \$200 + (e_{2I} / e_{2BA} * 2500\$) + (e_{2A} / e_{2BA} * 2500\$) + (e_{3A} / e_{3BA} * 2500\$) + (e_{3NU} / e_{3BA} * 2500\$) + (e_{3F} / e_{3BA} * 2500\$)$$

5.3.3 Damage value structured analysis

This section presents the steps of the damage value assessment with the help of a data flow diagram (DFD) [SMA 02] Data flow diagramming is defined as a means of representing a system with a graphical network of symbols showing data flows, data stores, data processes, and data sources/destination [KOZ 97]. This is presented to clarify the process of V_{ik} assessment to try to avoid misunderstanding. Figure 5.5 graphically illustrates how the damage value is obtained for an i,k pair. Figure 5.5 first presents the

context diagram. Then, a level 1 DFD is included for the evaluation of m_{sik} (process number 9) since this process is more complex.

Figure 5.5. Damage value data flow diagram

Process 9 Level one DFD

The context diagram in Figure 5.5 illustrates ten processes. Let's look at them in turn.

Process 1: Get the list of attributes

Recall that to implement the model it is not necessary to specify the sensitivity level of every service attribute $s \in S_{ik}$ every time that the damage value V_{ik} has to be calculated. A standard list of attributes and sensitivity levels is prepared when the RCNS is first implemented for every service $s \in S$ and subsequently modified as needed in the database (see Figure 4.4). When the asset agents are set, the organizational expert can use them to get the data required to determine and set the value of the service attributes belonging to the asset. An example of such a list for the small network domain scenario

illustrated in Figure 5.3 is given in Table 5.5. Process 1 represents the work required by the organizational expert to build such a list.

Process 2: Get expert judgements

Recall that to evaluate m_{sik} NCIC uses separate sets of pairwise comparisons for each $s \in S_{ik}$. Indeed, NCIC allows the covering attributes A_{sk} to be different for different services s under exposure k (see section 5.2.2.3). The organizational expert provides the pairwise comparison judgments. To be able to automate the process, it is suggested to use a baseline PCM matrix to perform this process. An example of a baseline PCM is presented in appendix E. Still, only the set of covering attributes (i.e base attribute/sensitivity levels pairs) applicable to service s under exposure k are used to calculate m_{sik} , but the pairwise comparison ratio entered in the PCM is taken from the baseline PCM. To try to lower the inconsistency inherent to the use of this baseline matrix only inconsistency ratios lower than 0.02 (as opposed to 0.1) are accepted. The sensitivity analysis in chapter 8 justifies our cut-off choice. The Bridge attribute used to build the baseline PCM needs to be selected according to (5). A trial and error process needs to be used to build the baseline PCMs that allow consistent results for every sub-PCM. This process requires a good deal of work from the expert but needs to be performed only once, when the RCNS is implemented. Then, the baseline PCM is kept in the RCNS knowledgebase (see Figure 4.4).

Process 3: Get exposure data

Recall that the RCNS calculate V_{ik} for a given asset and a given exposure. So, by definition, the impact of the exposure under analysis needs to be known. This information is kept in the RCNS database and is produced by network security experts when the RCNS tool is first built. The exposure database then needs to be updated through software patches by the RCNS operator. Process number 3 represents the work required to produce the exposure database.

Process 4: Get service dependency data

To be able to figure out all $s \in S_{ik}$, the Inference Engine needs to know what service is dependent on which other one. Most network domains these days use similar services that have comparable dependencies. Consequently, a service dependency template can be used and kept in the database to help implement the RCNS in an operational environment. Process 4 represents the work required by network security experts to produce such a template.

Process 5: review data.

The service dependency template might need to be customized to better fit a given organization when the RCNS is first implemented. Process 5 represents the work required by the organizational expert to modify the service dependency template.

Process 6: Identify $s \in S_{ik}$

Process 6 represents the work required by the inference engine to analyse the impact of an exposure of type k on asset i by looking at the network configuration and at the services dependency template to identify $s \in S_{ik}$.

Process 7: Identify the covering attributes

Process 7 represents the work required by the inference engine to analyse the impact of an exposure of type k and by looking at the standard list of attributes and sensitivity levels to identify the covering attributes $\forall s \in S_{ik}$. An example of such a list for the small network domain scenario illustrated in Figure 5.3 is given in Table 5.6.

Process 8: Identify the costs to regenerate attributes

Process 8 represents the work required by the inference engine to analyse the impact of an exposure of type k and by looking at the standard list of attributes and sensitivity levels to identify the value of the cost to regenerate attribute $\forall s \in S_{ik}$. An example of such a list for the small network domain scenario illustrated in Figure 5.3 is given in Table 5.7.

Process 9: Evaluate $m_{sik} \forall s \in S_{ik}$

Process 9 represents the work required by the inference engine to evaluate the “harm value” m_{sik} associated with every service (user and system) $s \in S_{ik}$ in monetary terms

using (7) in conjunction with the baseline PCM and the lists of attributes (from process 7 and 8). For the scenario presented in Figure 5.3, the $m_{sik} \forall s \in S_{ik}$ are given in Figure 5.4, step 5.

Process 10: Evaluate V_{ik}

Process 10 represents the work required by the inference engine to evaluate the “damage value” V_{ik} in monetary terms using (4) and recording the value obtained in the RCNS knowledgebase.

The Level one DFD for process 9 illustrates four processes. Let’s look at them in turn.

Process 9.1: Create covering attributes PCM

Process 9.1 represents the work required by the inference engine to take the information out of the baseline PCM and the list of covering attributes to create the covering attribute PCM. An example of such matrixes for the small network domain scenario illustrated in Figure 5.3 is given in step 2 of Figure 5.4.

Process 9.2: Calculate the PCM eigenvector

Process 9.2 represents the work required by the inference engine to take the PCM created in process 9.1 and produce the resulting eigenvector. An example of such vectors for the small network domain scenario illustrated in Figure 5.3 is given in step 3 of Figure 5.4.

Process 9.3: Calculate covering attributes increment of value

Process 9.3 represents the work required by the inference engine to calculate the covering attributes' respective increment of value using (6). An example of such calculation for the small network domain scenario illustrated in Figure 5.3 is given in step 4 of Figure 5.4.

Process 9.4: Calculate m_{sik}

Process 9.4 represents the work required by the inference engine to evaluate the “harm value” m_{sik} associated with every service (user and system) $s \in S_{ik}$ in monetary terms using (7) in conjunction with the list of cost to regenerate attributes. For the scenario presented in Figure 5.3, the $m_{sik} \forall s \in S_{ik}$ are given in Figure 5.4, step 5.

5.4 Conclusion

This chapter explained how V_{ik} can be subjectively estimated in practice and the theories behind this. The assessment of the V_{ik} is a multi-dimensional problem, which justifies the use of a MADM method. We proposed the following procedure to evaluate V_{ik} associated with a given exposure k on asset i .

- Identify all services $s \in S$ that could be affected by an attack performed by using exposure k on asset i .

- Evaluate the “harm value” m_{sik} associated with every service (user and system) s

$\in S_{ik}$:

$$m_{sik} = c_{sik} + \sum_{a \in A_{sk}} v_{saik}$$

- Sum up the “harm values” associated with every compromised service $s \in S_{ik}$ to get the damage value:

$$V_{ik} = \sum_{s \in S_{ik}} m_{sik}$$

The NCIC MADM method was selected to evaluate the “harm value” m_{sik} , for $s \in S_{ik}$ as it is specially designed to make explicit the implied monetary value, which is assigned to non-financial attributes. For a given service $s \in S_{ik}$ and an exposure k the NCIC analysis is constructed by evaluating the increments of value ratio with respect to the baseline alternative for the corresponding $(A_{sk} \times A_{sk})$ PCM. Organizational experts should perform this exercise. The next chapter explain how the P_{ik} can be subjectively estimated in practice and the theory underlying it.

Chapter 6 Estimation of the probability parameter in the Risk value formula

6.1 Introduction

It is widely accepted that the risk derives from the probabilistic estimate of a successful attack [PFL 01] [PFL 96] [PEL 01] [NOR 00]. In this chapter, a method to estimate P_{ik} , considering different factors increasing the chances of a successful attack, is proposed. This chapter begins by providing a brief overview of different prediction systems. We then compare the different prediction systems in order to determine the most appropriate to estimate P_{ik} in (1). We then provide a detailed description of the subjective estimation procedure. We do so by providing explanations on how P_{ik} is developed, using the prediction system that we think is the most appropriate to solve our problem.

6.2 Comparison of prediction systems

This section provides a brief overview of three potential prediction systems that could be used to subjectively estimate the probabilistic parameter in (1). This section also explains why Bayesian Networks were selected.

6.2.1 Rule-based systems

Any rule consists of two parts: the “IF” part called the antecedent and the “THEN” part called the consequence. In general, a rule can have multiple antecedents joined by the

keywords “AND”, “OR” or a combination of both [NEG 02]. A rule-based system consists of a collection of rules. These rules reflect essential relationships and behaviour. When specific information comes in the rules, the rules are used to draw conclusions and to point out appropriate actions. This is called inference. The inference is a kind of chain reaction. Rules can be used backward and forward (IF A THEN B/ IF B THEN A) depending on how a domain expert solves a problem. When the information is subject to uncertainty, a certainty measure is added to the antecedent as well as the consequence in the rules. In its simplest form, this looks like:

IF condition (with certainty x) THEN action (with certainty $f(x)$)

where uncertainty is defined as the lack of exact knowledge that would enable reaching a perfectly reliable conclusion [STE 87] . There are many schemes for treating probabilities in rule-based systems. Common to all of these schemes is that the probability is treated locally. That is, the treatment is connected directly to the incoming rules and the uncertainty of their elements. There are different algebras for combinations of uncertainty, depending on the scheme. In many cases, they come to incorrect conclusions [CLE 97] [VOO 02]. This is because the combination of probability is strongly dependent on the entire situation and although the individual production rules tend to be relatively simple and self-documented, their logical interaction within the large set of rule is opaque. Rule-based systems make it difficult to observe how individual

rules serve the overall strategy. This problem is related to the lack of hierarchy knowledge representation in the rule-based expert systems [NEG 02].

6.2.2 Feed-forward neural networks

A neural network can be defined as a model of reasoning based on the human brain [NEG 02]. An artificial neural network consists of a number of highly interconnected layers of processors called neurons. At the top there is a layer of input-neurone, at the bottom a layer of output-neurons and in between, usually 1-2 hidden layers. Every neurone in a layer is normally connected to every neurone in the layer just below. The neurones are connected by weighted links. Neural networks perform pattern recognition. So, except for the amount of layers and the amount of neurones in each layer, the weights and the thresholds establish the behaviour of the network. Weights and thresholds are established in order for the network to work as well as possible. A neural network learns through repeated adjustment of these weights. There is nothing that prevents the use of neural networks for handling probabilities. If relations are uncertain, a neural network is able to give the most probable conclusion, given some information.

6.2.3 Bayesian networks

Bayesian Networks are models for representing uncertainty in our knowledge. Bayesian Networks use probability theory to manage uncertainty by explicitly representing the conditional dependencies between the different knowledge components. This provides an intuitive graphical visualization of the knowledge including the interactions among the

various sources of uncertainty. The graph consists of nodes and arcs. The nodes represent variables, which can be discrete or continuous. The arcs represent causal relationships between variables.

Bayesian Networks are becoming an important area for research and application in the entire field of Artificial Intelligence [NIE 98] . The advantage of describing a probabilistic argument via a Bayesian Network is that the Bayesian Network represents the structure of the argument in an intuitive, graphical format. The main use of Bayesian Networks is in situations that require statistical inference⁹. Using probability calculus and Bayes theorem¹⁰ it is possible to update the values of all the other probabilities in the Bayesian Network. Bayesian analysis can be used for both 'forward' and 'backward' inference.

Although Bayesian probability has been around for a long time it is only in the last few years that efficient algorithms (and tools to implement them) have been developed to enable propagation in networks with a reasonable number of variables. Bayesian propagation computations, even for a small problem are very complex and cannot be calculated manually. With tools (such as Hugin [HUG 02]) it is possible to perform fast propagation in large Bayesian Networks (with hundreds of nodes and millions of state

⁹ In addition to statements about the probabilities of events, the user has some evidence, that is, some events that have actually been observed, and wishes to infer the probabilities of other events, which have not as yet been observed

¹⁰ Bayes' theorem: $P(A | B)P(B) = P(B | A)P(A)$

combinations). The recent explosion of interest in Bayesian Networks is due to the developments of new tools, which mean that for the first time realistic size problems can be solved. These recent developments make Bayesian Networks the best method for reasoning about uncertainty [SER 02]. To date Bayesian Networks have proven useful in applications such as medical diagnosis and diagnosis of mechanical failures. Their most publicly recognized use has been by Microsoft. They underlie the help wizards in Microsoft Office and also underlie the interactive printer fault diagnostic system on the Microsoft web site.

6.2.3.1 Comparing rule-based systems and Bayesian networks

The updating method of Bayesian networks, as opposed to the methods of rule-based systems, uses a global perspective, and if the information and the model are correct, the method calculates the new probabilities correctly. An important difference between rule-based systems and systems based on Bayesian networks is that rule-based systems try to model the expert's way of reasoning, while Bayesian networks try to model causal effect. With rule-based systems the individual production rules tend to be relatively simple and self-documented but the interaction between the large set of rules is opaque. Consequently, rule-based systems make it difficult to observe how individual rules serve the overall strategy. This problem is related to the lack of hierarchy knowledge representation in the rule-based expert systems. By opposition, Bayesian networks explicitly represent the dependencies between the different knowledge components.

Since our objective is to estimate P_{ik} , considering different factors increasing the chances of a successful attack, our problem is a problem of causal effects (dependencies). In consequence, Bayesian networks prediction systems are considered more appropriate for this research.

6.2.3.2 Comparing neural networks and Bayesian networks

The principle distinction between the two types of networks is that all the nodes of a Bayesian network represent concepts that are well defined. The meaning of a node and its probability tables can be the subject of an external discussion, regardless of their function in the network. This does not make any sense when speaking of neural networks. This means that the construction of a Bayesian network requires detailed knowledge. It is often criticized that in order to construct a Bayesian network you have to “know” too many probabilities [NEG 02]. On the other hand, there is not a considerable difference between this number and the number of weights and thresholds that have to be “known” in order to build a neural network, and the latter can only be learned by training. It is an enormous weakness of neural networks that it is not possible to utilize the knowledge that might be available in advance. Probabilities, in contrast, can be assessed using a combination of theoretical insight, empiric studies, training and various more or less subjective estimates. Finally, in the construction of a neural network the route of inference is fixed. It is decided in advance, about which relations

information is gathered, and which relations the system is expected to calculate. Bayesian networks are much more flexible in that respect.

6.3 Supporting tool

Bayesian Networks can be constructed and tested in a development environment such as Hugin products. Hugin experts' products enable construction of intelligent systems using Bayesian Networks. Their technology has already been used to create intelligent solutions for risk management. Their demo version, Hugin Lite, has an easy-to-learn user interface that enables building of models quickly. The next section of this chapter explains how the probabilistic parameter in (1) is subjectively estimated using a Bayesian network.

6.4 Building the Bayesian network

The purpose of this section is to develop the Bayesian network (BN) necessary to evaluate the probabilistic parameter of our risk value formula (1). It is understood that occasionally, security auditing tools (see chapter 3) may report false positive exposures¹¹ when countermeasures are implemented. However, security management tools such as Tivoli Secure Way Risk Manager (TSRM) [TIV 01] can be used to eliminate almost

¹¹ Exposure that cannot be exploited

every false positive. Consequently, for the purpose of this research, it is assumed that the exposures of type k under analysis are not a false positive.

6.4.1 Building our Bayesian network (BN)

A BN is used to model a sphere of influence containing uncertainty in some manner. As previously mentioned, a BN is a directed acyclic graph (DAG) where each node represents a variable. Figure 6.1 illustrates a directed acyclic graph representing three variables (A, B, C).

Figure 6.1. Directed acyclic graph

The graph is the qualitative representation. Each node contains the states of the random variable it represents and a conditional probability table (CPT). The CPT of a node contains probabilities of the node being in a specific state given the states of its parents. The CPT is the quantitative representation. In this sub-section the BN is presented qualitatively; the next section explains how the quantitative data is obtained.

For this research, the sphere of influence is an exposure k on an asset $i \in D$. Recall that threats and exposures are intrinsically related. In fact, exposure was defined as a weakness of a network that creates the condition, which allows a threat to cause damage

[PEL 01] . On the other hand, a threat has previously been defined as a situation that has the potential to cause an attack. Four pieces of evidence indicate the probability or improbability of a threat event. First, to raise a threat, people need motivation. Second, if the exploitation of the exposure is simple, the threat is more likely. Third, if the incident detection analysts can establish that an incident occurred on a domain exploiting the exposure under analysis, the subject exposure is more likely to represent a threat. Finally, assuming that there is a firewall in place, if the firewall is not configured to stop external attacks of type k , then the threat is more significant. The situation can be modeled with a BN. To simplify the notation, the index i and k are not always used in this section but the discussion permanently assumes that we are dealing with a given asset i and exposure k and that a change in the domain environment has just occurred. To formulate the BN, three types of variables need to be defined: Information variables, Mediating variables and Hypothesis variables. The variables are defined as follow.

1. Information variables: These are variables, which can be observed. In our case, they provide evidence regarding the environment. Two information variables are used in our model:

- Incident detection (ID) with two possible states:
 - Yes (y) if according to the incident detection analyst, an incident occurred in the past by means of an exposure k on asset i , $i \in D$.

- No (n) otherwise.
- External threat (ET): with two possible states:
 - Yes (y) if according to the network security expert, the firewall can block an external attack of type k on asset i.
 - No (n) otherwise.

These variables provide subjective evidence coming from the specifications of the incident detection analyst for Incident detection and from the security management tool for External threat.

2. Mediating variables: These are introduced to facilitate the acquisition of conditional probabilities by having a more refined model of the sphere of influence. Two mediating variables are used in our model.

- Complexity (C): with three possible states:
 - High (h) if the exploitation of this exposure k requires code, which is difficult to write and may require access to specific types of computer systems. Using this exposure may require specific knowledge of the exposure and the system on which it is present.
 - Medium (m) if a special-purpose software tool is required to exploit the exposure k; this tool is probably quite easy to use

and understand by a neophyte hacker, but exploitation of this problem may be out of the reach of individuals who are not familiar with the security community or the hacker underground.

- Low (l) if an attack of type k can be executed by an unskilled attacker without any special tools (perhaps by using standard Unix utilities, or by using their web browser). The problem may be obvious even to someone who is not familiar with the issues involved in computer security.
- Motivation (M) : with three possible states:
 - High (h) if there is a lot of motivation to attack the services s threatened, $s \in S_{ik}$
 - Medium (m) if there is some motivation to attack the services s threatened, $s \in S_{ik}$
 - Low (l) if there is little or no motivation to attack the services s threatened, $s \in S_{ik}$

These variables provide subjective evidence coming from the specifications of the security-auditing tool for complexity and from indirect managerial assessment for motivation.

3. Hypothesis variables: Variables with the state that is asked for. They are impossible to observe. Two hypothesis variables are used in our model.

- Threat (T): with two possible states:
 - Yes (y) if the pair asset i/exposure k represents a menace to the services $s, s \in S_{ik}$.
 - No (n) otherwise.
- Attack (A): with two possible states:
 - Yes (y) if the pair asset i/exposure k represents a successful attack affecting the services $s, s \in S_{ik}$.
 - No (n) otherwise.

The BN constructed with these variables is shown in Figure 6.2. The figure also includes the possible state of each variable and it indicates the data required to obtain the relative probability of a successful attack ($P_{ik} = P(A=y)$) with the BN.

Figure 6.2. BN representing the sphere of influence of a vulnerable process component

The BN in Figure 6.2 shows that there is a causal dependency, from Incident detection (ID) to Threat(T), from Motivation(M) to T, from Complexity (C) to T and from External threat(ET) to T. Finally, there is a causal dependency from T to Attack (A). The arrows represent this. When there is a causal dependency from one node A to another node B, it is expected that when A is in a certain state it has an impact on the state of B.

In the following sections, the approaches proposed to obtain all the data elements identified in Figure 6.2 are explained

6.4.2 Evidence on the information and motivation variables

In Figure 6.2, we have the graphical representation of the BN. The figure can quickly be drawn in a development environment such as Hugin. Yet, this is only what is called the qualitative representation of the BN. To build the model it is also essential to specify the quantitative representation for every CPT. By definition, the CPT shows the probability of a node being in a specific state depending on the states of its parent nodes. However, since ID, M, C and EX do not have any parent nodes, they are not conditioned by anything. The purpose of this section is to explain how the states of these variables are assigned for a given exposure k on an asset i . Once the states are known they can be entered as evidence in the CPT of the model.

6.4.2.1 Incident detection (ID)

Let's recall that the incident detection analysts can establish if an incident occurred on the network domain D and the exposure(s) K_{ik} , $K_{ik} \subset K$ that were the cause of that incident (see chapter 3.3). As a consequence, the state of ID changes dynamically in real time. This means that as soon as an exposure k , $k \in K_{ik}$, is reported to be the cause of an incident on the network domain D , the state for the ID variables changes to "yes". This is illustrated in Figure 6.2

Figure 6.3. Change in ID state over time

Figure 6.2 illustrates that once the state has changed to “yes” it cannot turn back to “no” unless the incident detection analyst indicates that a countermeasure has been put in place to make sure that a similar incident cannot be reproduced. This is because computer criminals are really patient and once they know about an exposure, it is not possible to figure out when they are going to use it. In addition, it makes sense to believe that a network is more exposed when people know about the exposures.

6.4.2.2 Complexity

The state for a given exposure k is set by a network security expert when the exposure is entered in the security auditing tool database. There is nothing that prevents the database from being modified. However, this is unlikely unless the wrong state was first entered. Consequently, it is assumed that the complexity state allocated to a given exposure k does not change through time.

6.4.2.3 Motivation

The Webster's New Collegiate Dictionary defines motivation as a motivating force or influence. In reality, the influence is a motive. The motive can be presented by many different factors. Pfleeger [PFL 01] provides a list of factors that affect whether a threat agent has reason to attack. However, most of the factors are generic to an organization. In other words, they are shared by every service of a network domain. This means that even if these factors would change P_{ik} they would not affect the final ranking of the asset/exposure pair. So, they are unneeded according to the ultimate goal of this research. Only one factor changes from one asset/exposure pair attack to another. This factor is related to the damage value imposed on the services compromised. In fact, the attacker may be looking for recognition for the attack or satisfaction for the accomplishment. Informal "bragging rights" within the hacker community confer more credit for attack that creates more damage [PFL 01]. Consequently, the motivation variable can be defined in terms of the damage value of the services at risk which in reality is V_{ik} . From there, assuming that the motivation is directly proportional to the damage value, V_{ik} can be used to designate the state of the motivation variable. A step functions is used to assign the level of motivation. The purpose of the step function is to translate the aggregate data into the appropriate rating intensity (high medium low). To implement this, the following notation is defined:

V_{DK} : The highest potential total damage value caused to a set of service $S_{ik} \subset S$ in monetary terms calculated with (4) (see section 5.3.1).

M_{ik} : The motivating influence (incentive, drive) associated with a successful exposure k attack on asset i .

From there, the following equation is used to compute the motivation level

$$M_{ik} = \frac{V_{ik}}{V_{DK}} \quad (8)$$

V_{DK} in (8) is used to normalize the damage value V_{ik} to allow the use of a step function.

To generate the step function, a lower and higher data bound for M_{ik} is defined for each possible state of M . This is presented in Table 8. 3.

Table 6.1: Motivation variable states

State	Lower bound	Higher bound
High	0.66	1
Medium	0.33	0.66
Low	0	0.33

The state of M changes dynamically. This means that when a new V_{DK} is obtained every M_{ik} for $i \in D$ and $k \in K$ needs to be recalculated, and the motivation states need to be modified accordingly. This is illustrated in Figure 6.3.

Figure 6.4. Change in M state over time

6.4.2.4 ET

The state for a given i, k pair is set with the security management tool. If there are no firewalls in place, the state of ET is automatically “yes”. The state of ET changes dynamically in real time if there is a change in the firewall configuration that modifies the network management tool interpretation of ET. In other words, every time a firewall is added or reconfigured, the state of the ET is revised $\forall i \in D, k \in K$ by the security management tool and modified if required. This is illustrated in Figure 6.4.

Figure 6.5. Change in ET state over time

6.4.3 Conditional threat probabilities

The Threat node also needs to be quantitatively defined in a CPT. When a variable like T has several parents in a BN it is necessary to specify $P(T|C^*)$ for each configuration C^* of the parents [JEN 96] to be able to estimate the entries in the CPT. In order to acquire the relevant conditional probabilities, we had to rely on elicitation techniques. In fact, although information for structuring the network is abundant in the literature [PFL 01] [PFL 96] [NOR 00] the literature does not provide sufficient information to quantify the probabilistic relationships among the domain variables. Furthermore, no data was

available for the automatic estimation of the probabilities of interest. Although the AHP MADM method (see appendix A) is devised for the purpose of preference elicitation, it lends itself naturally to the task of probability elicitation [HAH 99] [HUG 93] [MON 00] [YAG 79]. Consequently, the AHP method discussed in appendix A is used to provide reasonable estimates of $P(T|ID)$, $P(T|C)$, $P(T|M)$ and $P(T|ET)$. To utilize AHP in this context, we adapt the original terminology for utilities and preferences to the probabilistic setting. In particular, we replace the term attribute with the term stochastic event, and the term importance with the term likelihood. With these modifications, the new method can be described as follows: First, a scale of comparison is established, based on which it is possible to compare pairwise the events of interest. The scale proposed is an adaptation of the Saaty's scale; it is presented in Table 6.2.

Table 6.2. Scale of comparison

Judgement	Numerical Equivalents
Extremely more likely	9
• Between very strongly and extremely more likely	8
Very Strongly more likely	7
• Between strongly and very strongly more likely	6
Strongly more likely	5
• Between moderately and strongly more likely	4
Moderately more likely	3
• Between equally and moderately likely	2
Equally likely	1

Once the scale is defined, it is possible to compare pairwise the possible states under consideration according to the given scale. Since every event is compared with every other event, the resulting assessments can be arranged in a square matrix that we refer to as the likelihood matrix. From appendix A we know that Pairwise Comparison Matrix (PCM) eigenvectors have nonnegative elements that sum to one. Consequently, when the elements are mutually exclusive and exhaustive, the values can be directly adopted as the probabilities of the corresponding state [MON 00] . The rationale behind using this approach is that the elicitation of the pairwise comparisons is easier and better accepted by the expert than the direct elicitation of the probabilities of interest. The remaining of this section provides more details about how the $P(T|C^*)$ for each configuration C^* of T is estimated to finally obtain $P(T|ID, C, M, ET)$.

6.4.3.1 Estimation of $P(T|ID)$

$P(T|ID)$ is estimated using AHP. A sensitivity analysis on the possible entries in Table 6.3 was performed. The results are presented in chapter 8. Table 6.3 presents the likelihood matrix used to compare the likelihood of $T=y$ conditioned on the different states that can be taken by the ID variable. The states are arranged in the matrix from the most likely to the least likely. This arrangement helps in giving a qualitative interpretation of the data. In fact, every column can be interpreted as a ranking of the likelihood of the different states according to a different ratio-scale.

Table 6.3. The PCM of the probabilities conditioned on the states of the ID variable

	ID = y	ID = n
ID = y	1	How much more likely there is a threat if ID= y than if ID= n
ID = n		1

The PCM principal eigenvector $\underline{e}$ for Table 6.3 is of the form $[e_{IDy}, e_{IDn}]$ with the sum equal to 1. Since the states are mutually exclusive and exhaustive, the values can be directly adopted as the probabilities of the corresponding state. Consequently, Table 6.4 is obtained from the resolution of Table 6.3

Table 6.4. Estimation of $P(\text{Threat} | \text{ID})$

	ID=y	ID = n
T=y	e_{IDy}	e_{IDn}
T=n	$1 - e_{IDy}$	$1 - e_{IDn}$
TOTAL	1	1

6.4.3.2 Estimation of $P(\text{Threat} | \text{complexity})$

Network security experts need to be interviewed according to the questionnaire in appendix B to estimate $P(\text{Threat} | \text{complexity})$ using AHP. Table 6.5 presents the likelihood matrix used to compare the likelihood of T=y conditioned on the different states that can be taken by the complexity variable. The states are arranged in the matrix from the most likely to the least likely.

Table 6.5. The PCM of the probabilities conditioned on the states of the complexity variable

	C = low	C = med	C = high
C = low	1	How much more likely there is a threat if C = low than if C = Med	How much more likely there is a threat if C = low than if C = high
C = med		1	How much more likely there is a threat if C = Med than if C = high
C = high			1

The PCM principal eigenvector $\underline{e}$ for Table 6.5 is of the form $[e_{Cl}, e_{Cm}, e_{Ch}]$ with the sum equal to 1. Since the states are mutually exclusive and exhaustive, the values can be directly adopted as the probabilities of the corresponding state elicitation [MON 00] .

Consequently, Table 6.6 is obtained from the resolution of Table 6.5

Table 6.6. Estimation of P(Threat| Complexity)

	C=l	C=m	C=h
T= y	e_{Cl}	e_{Cm}	e_{Ch}
T= n	$1 - e_{Cl}$	$1 - e_{Cm}$	$1 - e_{Ch}$
TOTAL	1	1	1

6.4.3.3 Estimation of P(T|M)

Network security experts need to been interviewed according to the questionnaire in appendix C to estimate P(Threat| Motivation) using AHP. Table 6.7 presents the

likelihood matrix used to compare the likelihood of $T=y$ conditioned on the different states that can be taken by the M variable. The states are arranged in the matrix from the most likely to the least likely.

Table 6.7. The PCM of the probabilities conditioned on the states of the motivation variable

	M = high	M= med	M= low
M = high	1	How much more likely there is a threat if M= high than if M= med	How much more likely there is a threat if M= high than if M= low
M = med		1	How much more likely there is a threat if M= med than if M= low
M = low			1

The PCM principal eigenvector $\underline{e}$ for Table 6.7 is of the form $[e_{Ml}, e_{Mm}, e_{Mh}]$ with the sum equal to 1. Since the states are mutually exclusive and exhaustive, the values can be directly adopted as the probabilities of the corresponding state [MON 00] .

Consequently, Table 6.8 is obtained from the resolution of Table 6.7.

Table 6.8. Estimation of $P(\text{Threat} | \text{Motivation})$

	M=l	M=m	M=l
T= y	e_{Ml}	e_{Mm}	e_{Mh}
T= n	$1 - e_{Ml}$	$1 - e_{Mm}$	$1 - e_{Mh}$
TOTAL	1	1	1

6.4.3.4 Estimation of $P(T|ET)$

$P(T|ID)$ is estimated using AHP. A sensitivity analysis on the entries of Table 6.9 was performed. The results are presented in chapter 8. Table 6.9 presents the likelihood matrix used to compare the likelihood of $T=y$ conditioned on the different states that can be taken by the ET variable. The states are arranged in the matrix from the most likely to the least likely.

Table 6.9. The PCM of the probabilities conditioned on the states of the complexity variable

	ET = y	ET = n
ET = y	1	How much more likely there is a threat if ET= y than if ET= n
ET = n		1

The PCM principal eigenvector $\underline{e}$ for Table 6.9 is of the form $[e_{ETy}, e_{ETn}]$ with the sum equal to 1. Since the states are mutually exclusive and exhaustive, the values can be directly adopted as the probabilities of the corresponding state [MON 00] .

Consequently, Table 6.10 is obtained from the resolution of Table 6.9.

Table 6.10. Estimation of $P(\text{Threat} | ET)$

	ET=y	ET = n
T=y	e_{ETy}	e_{ETn}
T=n	$1 - e_{ETy}$	$1 - e_{ETn}$
TOTAL	1	1

6.4.3.5 Estimation of $P(T|ID,C,M,ET)$

Table 6.11 is the CPT of the node “Threat”. The possible values (yes (y) or no (n)) for “Threat” are shown in the first column. The rules of probability specify that some of this information is redundant: $P(T=\text{“No”}) = 1 - P(T=\text{“yes”})$. Consequently, only half of the table needs to be completed.

Table 6.11. $P(\text{Threat}/ID,C,M,ET)$

	ET=y																	
	M=high						M=med						M=low					
	C= high		C= med		C= low		h		m		l		h		m		l	
	ID=y	ID=n	ID=y	ID=n	y	n	y	n	y	n	y	n	y	n	y	n	y	n
T=y																		
T=n	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

	ET=n																	
	M=high						M=med						M=low					
	C= high		C= med		C= low		h		m		l		h		m		l	
	ID=y	ID=n	ID=y	ID=n	y	n	y	n	y	n	y	n	y	n	y	n	y	n
T=y																		
T=n	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-

To complete Table 6.11 we need to find a way to calculate $P(T|ID,C,M, ET)$ based on the probabilities evaluated with the AHP method. In other words, we need to find a method to combine the known probabilities (Table 6.4, 6.6, 6.8, 6.10) into $P(T|ID,C,M,ET)$. The following is a way of doing it. There are four factors causing the threat to be real ($T=y$):

- ID which causes the threat to be real with probabilities e_{IDy} , e_{IDn}

- C which causes the threat to be real with probabilities e_{Cl} , e_{Cm} , e_{Ch}
- M which causes the threat to be real with probabilities e_{Mh} , e_{Mm} , e_{MI}
- ID which causes the threat to be real with probabilities e_{ETy} , e_{ETn}

The above uncertainty can be interpreted in the following way. Any of the factors cause the threat to be real unless some inhibitor prevents it. Now if we assume that the factors are independent, then the combined probabilities are easy to calculate as one minus the product of the appropriate probabilities for the inhibitors. This is in reality an example of the simplifying assumption called “noisy or” [JEN 96]. Following this assumption, it is possible to determine the entries in Table 6.11. For example, from Table 6.4, 6.6, 6.8 and 6.10 the first entry in the table would be calculated as follows:

$$\begin{aligned}
 P(T=y | ET=y, M=h, C=h, ID=y) &= 1 - \\
 (P(T=n | ET=y) * P(T=n | M=h) * P(T=n | C=h) * P(T=n | ID=y)) \\
 &= 1 - (1 - e_{ETy}) * (1 - e_{Mh}) * (1 - e_{Ch}) * (1 - e_{IDy})
 \end{aligned}$$

6.4.4 Conditional attack probability

$P(A | T)$ is estimated using AHP. A sensitivity analysis on the entries of Table 6.12 was performed. The results are presented in chapter 8. Table 6.12 presents the likelihood matrix used to compare the likelihood of $A=y$ conditioned on the different states that can be taken by the T variable. The states are arranged in the matrix from the most likely to the least likely.

Table 6.12. The PCM of the probabilities conditioned on the states of the complexity variable

	T = y	T = n
T = y	1	How much more likely there is an attack if T= y than if T= n
T = n		1

The PCM principal eigenvector $\underline{e}$ for Table 6.12 is of the form $[e_{Ty}, e_{Tn}]$ with the sum equal to 1. Since the states are mutually exclusive and exhaustive, the values can be directly adopted as the probabilities of the corresponding state [MON 00] .

Consequently, Table 6.13 is obtained from the resolution of Table 6.12. Table 6.13 is the CPT of the node A.

Table 6.13. Estimation of $P(A|T)$

	T=y	T = n
A = y	e_{Ty}	e_{Tn}
A=n	$1 - e_{Ty}$	$1 - e_{Tn}$
TOTAL	1	1

P_{ik} ($P(A=y|T)$) is obtained through inference by running the proposed model built in a development environment such as Hugin. Inference used in the Hugin development environment is essentially a clever application of Bayes' Theorem. Details can be found in [JEN 96] .

6.5 Damage value structured analysis

This section presents the steps of P_{ik} assessment with the help of a data flow diagram (DFD). This is presented to clarify the steps of P_{ik} assessment to try to avoid misunderstanding. Figure 6.5 graphically illustrates how the damage value is obtained for a i,k pair. Figure 6.5 first presents the twelve processes involved. The processes are numbered from 11 to 22 as opposed to from 1 to 11 to easily differentiate them from the processes in Figure 5.5.

Figure 6.6. Probabilistic parameter data flow diagram

Let's look at every process in Figure 6.5 in turn.

Process 11: Get expert judgements

As explained in section 6.4.3 $P(T|C)$, $P(T|M)$, $P(T|ID)$ and $P(T|ET)$ are obtained using pairwise comparison judgements from network security experts. These pairwise comparison judgements need to be elicited only once when the RCNS knowledgebase is created. These judgements do not need to be customized for different organizations.

Process 11 represents the work required by the RCNS engineers to elicit network security experts judgements.

Process 12: Calculate $P(T|ID)$

As explained in section 6.4.3.1, $P(T|ID)$ is obtained using AHP. Process 12 represents the work required by the RCNS inference engine to transform the expert judgements obtained during process 11 into Table 6.4.

Process 13: Calculate $P(T|C)$

As explained in section 6.4.3.2, $P(T|C)$ is obtained using AHP. Process 13 represents the work required by the RCNS inference engine to transform the experts judgements obtained during process 11 into Table 6.6.

Process 14: Calculate $P(T|M)$

As explained in section 6.4.3.3, $P(T|M)$ is obtained using AHP. Process 14 represents the work required by the RCNS inference engine to transform the expert judgements obtained during process 11 into Table 6.8.

Process 15: Calculate $P(T|ET)$

As explained in section 6.4.3.4, $P(T|ET)$ is obtained using AHP. Process 15 represents the work required by the RCNS inference engine to transform the expert judgements obtained during process 11 into Table 6.10.

Process 16: Calculate $P(T|ID,C,M,ET)$

As explained in section 6.4.3.5, $P(T|ID,C,M,ET)$ is obtained using the simplifying assumption called “noisy or”[JEN 96] . Process 16 represents the work required by the RCNS inference engine to transform the output of processes 12 to 15 into Table 6.11.

Process 17: Fill up the Threat node CPT

Process 17 represents the work required by the RCNS inference engine to take the results of process 16 and enter them into the threat node CPT of the RCNS knowledgebase pre-built BN (qualitatively presented in Figure 6.1).

Process 18: Calculate $P(A|T)$

As explained in section 6.4.4, $P(A|T)$ is obtained using AHP. Process 18 represents the work required by the RCNS inference engine to transform the expert judgements obtained during process 11 into Table 6.13.

Process 19: Fill up the Attack node CPT

Process 19 represents the work required by the RCNS inference engine to take the results of process 18 and enter them into the Attack node CPT of the RCNS knowledgebase BN (qualitatively presented in Figure 6.1).

Process 20: Define the M State

Process 20 represents the work required by the RCNS inference engine to use (8) to calculate the state of M.

Process 21: Enter the evidences in the BN

Process 21 represents the work performed by the RCNS inference engine to take the evidences from process 20 (M), the exposure database (C), the organization security management tool (ET), and the organization incident analysts (ID) and enter them into the respective node CPT of the RCNS knowledgebase BN (qualitatively presented in Figure 6.1). Process 21 is performed every time P_{ik} needs to be calculated.

Process 22: Calculate $P(A=y)$

Process 22 represents the work performed by the RCNS inference engine to run the BN qualitatively represented in Figure 6.1, considering the evidences entered in process 21. P_{ik} being equal to $P(A=y)$.

Note that processes 11 to 19 are only performed when the RCNS tool is first built.

6.6 Conclusion

This chapter first justified the use of BN to estimate P_{ik} in (1). Later on in the chapter, the reader is introduced to the BN model developed for this purpose. The evidence for the nodes Incident detection, Complexity, Motivation and External threat, as well as the conditional probability tables presented in Tables 6.11 and 6.13 represent the quantitative data required to run the model qualitatively represented in Figure 6.1 to obtain P_{ik} .

PART 4 – EMPIRICAL APPROACH

Chapter 7 – RCNS prototype

7.1 Introduction

The previous chapters were devoted to the risk model and the estimation of its parameters. However, the model remains a conceptual one. To prove that the concept is valid, a prototype needed to be developed to generate global risk value (GRV) scores for different scenarios. For the purpose of the present thesis, the term “prototype” defines the set of tools and knowledge required to implement the various processes of the methodology. The intent of this chapter is to describe how the modeling methodology presented in earlier chapters was implemented to produce the GRV scores. The chapter first explains how the processes presented in Figure 5.5 and 6.5 were implemented. Next, the chapter reviews the eliciting approach used to gather the knowledge data from network security experts.

7.2 Prototype process implementation

A scaled-down version of the RCNS sphere (see Figure 4.4) was created. The prototype did not implement the communication sessions between the different RCNS components, neither did it automate the interaction between the different processes presented in Figures 5.5 and 5.6. These functionalities are believed to fall beyond the scope of the prototype, as its intention is only to test the concept on three case studies (see chapter 8) rather than to show off the skills involved in developing it. Table 7.1 explains how the

processes presented in Figures 5.5 and 5.6 were implemented. This is useful to put things into perspective.

Figure 7.1. RCNS processes implementation

Process	Implementation
Process 1: Get the list of attributes	The standard list of attributes and sensitivity level for every case is part of the case studies description (see appendix D)
Process 2: Get experts judgements	This process refers to the work required by organizational experts to create the baseline PCM. Since we have put the case studies together (see appendix D), we acted as the organizational expert for the three cases. The judgements were kept in a table similar to the one presented in appendix E
Process 3: Get exposure data	The exposure database was built from different Cybercop scans (NES). The data for every case is part of the case studies description (see appendix D)
Process 4: Get service dependency data	Network security experts judgements were elicited to create the template for the services presented in the three cases study (see appendix D).
Process 5: Review data	We did that
Process 6: Identify $s \in S_{ik}$	This was performed by the network security experts for every case study configuration (see appendix D)
Process 7: Identify the covering attributes	This was performed by network security experts according to the cases presented in appendix D
Process 8: Identify the costs to regenerate attributes	This was performed by network security experts according to the cases presented in appendix D
Process 9.1: Create covering attributes PCM	The judgements from the baseline PCM were manually entered in the Expert Choice software [EXP 00] for the three case studies
Process 9.2: Calculate	The eigenvectors were calculated with Expert Choice [EXP

the PCM eigenvector	00] for the three case studies
Process 9.3: Calculate attributes increment of value	The outputs from Expert Choice were manually entered in Microsoft Excel to calculate the increment of values
Process 9.4: Calculates m_{sik}	This was performed in Microsoft Excel
Process 10: Evaluate V_{ik}	This was performed in Microsoft Excel
Process 11: Get experts judgements.	Network security expert judgements were elicited for M and C. Our own judgement was used for ET, ID and T. A sensitivity analysis was then performed on the different judgements possible for ET, ID and T. The results are presented in chapter 8.
Process 12 to 15: Calculate $P(T *)$	The judgements were manually entered in the Expert Choice software where the eigenvectors were calculated
Process 16: Calculate $P(T ID,C,M,ET)$	The results from process 12 to 15 were manually entered in Microsoft excel where $P(T ID,C,M,ET)$ was calculated
Process 17: Fill up Threat node CPT	The probabilities obtained in process 16 were manually entered in Hugin Lite [HUG 02] where the BN qualitatively illustrated in Figure 6.1 was pre-built.
Process 18: Calculate $P(A T)$	The judgements were manually entered in the Expert Choice software where the eigenvectors were calculated
Process 19: Fill up the Attack node CPT	The probabilities obtained in process 18 were manually entered in Hugin Lite [HUG 02] where the BN qualitatively illustrated in Figure 6.1 was pre-built.
Process 20: Define the M State	This was performed in Microsoft Excel
Process 21: Enter evidences in the BN	The evidences were manually entered in Hugin Lite
Process 22: Calculate $P(A=y)$	The BN was run in Hugin Lite
GRV calculation using	This was performed in MS excel. The resulting risk value

equation (1)	scores were then ranked manually
--------------	----------------------------------

In Table 7.1, processes 4, 6, 7, 8 and 11 all refer to expert judgements. Expert judgement is information and data provided by qualified persons in response to specific questions. Expert judgements are formally elicited and analyzed using state-of-the-art techniques to ensure the quality of the data/information and to provide documentation for its use. The validity of expert judgement varies just like the validity of hard data. The literature reports that the meaningfulness of expert judgements depends on the completeness of the expert's mental model of the phenomenon and on the way the expert data are elicited, modeled, analyzed and interpreted [MEY 91] . The next section discusses our way through the elicitation process.

7.3 Eliciting expert judgement

This section explains how we proceeded with our elicitation process. First, there is a discussion regarding the way the experts were selected. Then, the processes used to try to avoid bias are presented. The interested reader can refer to Meyer's book [MEY 91] to get detailed information on expert judgement and the elicitation process involved in collecting data.

7.3.1 Selecting and motivating the experts

This sub-section explains how our experts were chosen. An expert is considered to be anyone especially knowledgeable in the field and at the level of detail being elicited. Our

selection schema was based on having experts name other experts. The problem with using this scheme without modification is that it leaves the project open to later questions of whether people named those with similar views. It is also commonly believed that skewed results arise from selecting the majority of experts from one place, such as the same organization, or class of organization. Consequently, to represent different views and to avoid critics, a balanced group of experts was chosen. In fact, a number of experts were from DND (Red Team) and another group from the Computer Security Establishment. In addition, only experts with particular levels of experience were chosen. It is to be mentioned that logistics also played a role in the selection. The expert had to be willing to participate, have the time to participate and be allowed by their employer¹².

Table 7.1 states that network security expert judgements are used to supply the model with some of the knowledge base data (process 11). The questionnaires in appendices B and C were used to do so. To get all this data, we only needed to focus on experts' answers since the logic behind the type of request was straightforward. In this situation, the literature suggests obtaining quantitative data from 4 to 50 experts[MEY 91] . We were able to elicit data from five experts. For this application the experts were mainly chosen for their experience and for their ability to quantify their judgement in the desired form. The chosen experts needed to have a few years' experience in computer networks

¹² 10 experts were invited to participate and 5 actually participated

operations and at least one year of experience as a “professional hacker”(some kind of red team). Education was not an issue when choosing the experts.

Table 7.1 refers to the use of expert judgements for processes 4, 6, 7 and 8. To validate our work, the five experts were also asked to analyse the case study presented in appendix D.

7.3.2 Eliciting techniques and potential bias

This section presents our elicitation techniques and how we dealt with the potential bias involved. There is a great deal of diversity in elicitation processes. Each specific application has its own set of circumstances and hence its own optimum solution. The literature on the methods, and the few sources that exist provide conflicting advice. It would be very difficult for us to evaluate which methods provide the best results because the experts' answers to our questions are not something which can be externally verified through measurement. For this reason, the elicitation components were not only compared based on the literature but also on practical considerations such as how acceptable they are to the experts or how much time they take to administer. According to Seaver & Stillwell [SEA 83] this is a common way to choose among methods. In this sub section we discuss our steps through the elicitation process.

7.3.2.1 Selecting and refining the questions

The questionnaires we used to elicit the experts judgements for both applications are available in appendix B to D. To make sure that the questions were easy to understand and to make sure that reviewers would not be concerned about bias in the phrasing of the questions, one external expert¹³ was asked to review the questions. This expert has been asked the following:

- Are the questions answerable (e.g do respective experts possess experience relevant to the question)?
- How much diversity of opinion between external experts is there likely to be?
- Would any of the expert judgement data be considered proprietary?
- How many questions can an expert answer in a specific period of time?

This process also helped us in a way in practicing the elicitation process by making sure everything was clear on paper. The planning of the presentation of the questions was divided in two considerations:

- Determining the type of information needed, such as background on the questions, assumptions, and definitions.
- Determining the optimal order for the presentation.

¹³ This expert has the expertise required and knows most of the elicited experts

7.3.2.2 Selecting from elicitation situation

Three major methods can help in eliciting an expert's judgement: Individual interviews, Interactive groups and Delphi [MEY 91] . These situations can be tailored and combined to fit the application. Following, we present the helpful advice we got from the literature.

- Interactive group: The interactive group method is reported to generate more accurate data, particularly for prediction, than the other two situations. Its main disadvantage is that it possesses the potential for group bias [MEY 91] .

According to Seaver [SEA 76] the interactive group method produces a greater quantity of ideas and a higher member satisfaction with the product than the Delphi method. He found that predictions made by groups were more often correct than those made by individual.

- Delphi: The Delphi method was designed to avoid bias from group dynamics. It is not believed to be a suitable method to gather data on how experts solved problems. It is also reported as being the most time consuming of the three methods because of the turnaround time [MEY 91] . Several researchers consider the structured interactive group to work better than the Delphi in terms of avoiding the bias that the Delphi was originally designed to avoid [ARC 93]

Arca, " INFOSEC Handbook, An Information System Security Reference Guide Second Edition" ARCA, San Jose, 1993

- [ARM 81] [SEA 83] . Dalkey [DAL 96] found that the number of rounds in Delphi correspond to increasing agreement but not to increasing accuracy.
- Individual Interview: This method is reported as being the best method for obtaining detailed data. It is also reported as being the main method used for obtaining data on the expert's problem solving process. This method apparently avoids the potential bias from group dynamics. The data can be combined by mathematical aggregation. The main disadvantage of this method is that it is time consuming and that there is no synergic effect from expert discussion [MEY 91] Seaver [SEA 76] states that the mathematical combined estimates from individual interviews outperformed single estimate. However, results from the mathematical combined estimates have been judged poorer than those from interactive groups [VON 71] Then again, the above-mentioned studies were not using the individual interviews to elicit deep problem-solving data, the task for which it is most suited.

From what we have just seen, the Delphi method does not seem appropriate for our research. In reality, the method that stands out right away is the interactive group interview. The individual interview seems to be best suited when deep problem-solving data are required. The group interview is more time consuming than the individual interview but the experts were willing to participate. To save time and to try to avoid group bias, the questionnaires were sent to the experts in advance. The experts were

asked to answer the questions in writing on their own before the interview. The experts were invited to communicate with us in case of misunderstanding. Meyer and Booker [MEY 91] suggest having from five to nine experts to be able to get adequate diversity of information to make inference when face to face meetings are involved. As previously mentioned, five experts participated. During the case study interview, processes 4, 6, 7 and 8 (see Table 7.1) were first performed verbally to make sure that everybody agreed on the information. We acted as a mediator among the participants. A verbal protocol involved asking the expert to "think aloud" and around the problem. At the end of the session, all participants agreed on respectively one solution for each questionnaire. Note that for the process 11 (see Table 7.1) the experts came to the conclusion that the best solution was to average the participant judgements. Expert Choice [EXP 00] was used to make sure that the resulting inconsistency ratio was within the 0.1 confidence limit. The questionnaires completed before the interview were gathered to try to evaluate the importance of biases during the session.

7.3.2.3 Potential bias

A major problem to be dealt with in elicitation, and in particular in the elicitation of probability assessments, is bias. Bias is generally considered as a skewing of reality.

Meyers defines two general categories of bias as follows [MEY 91] :

- **Motivational bias:** This occurs when the elicitation process alters the expert's reports of their thoughts or answers. The reasons may be social pressure, for example wanting to please the interviewer or else wanting to concur or demur

answers. The interviewer may have led the expert. There may be a conflict of interests.

- **Cognitive bias:** Here an expert's judgement does not follow objective rules or standards i.e. what can be observed or measured, if such judgements could be checked. For example, an expert may tend to remember failures with a disproportional frequency to successes in estimating the functioning of some piece of technology.

There are, however, certain steps that can be taken during the elicitation process to assist in the handling of bias[MEY 91] . The best way to deal with biases is to try to anticipate which biases are likely to occur in the planned elicitation [MEY 91] .

Table 7.2 summarized the anticipated bias.

Figure 7.2. Anticipated biases in our elicitation method

Elicitation Component	View of Bias	Source
<i>Elicitation situation</i>		
Interactive Group	Motivational	Social pressure, group thinking
	Motivational	Wishful thinking
	Cognitive	Inconsistency
<i>Modes of communication</i>		
Face to Face	Motivational	Social pressure, group thinking
	Motivational	Wishful thinking
<i>Response Modes</i>		
Complex ones such as probabilities	Motivational	Misinterpretation by expert

	Cognitive	Inconsistency
<i>Aggregation</i>		
Behavioral Aggregation (relies on the experts reaching a consensus during the elicitation session)	Motivational	Social pressure, group thinking

The sources of bias presented in Table 7.2 are defined as follows by Meyer [MEY 91] :

1. Social pressure, group thinking: Experts may alter the description of their thoughts because of social pressure, to gain acceptance and to be seen in the most positive light possible. This altering can take place consciously or unconsciously. The social pressure can come from those physically present, such as the interviewer, or the other experts, or it can come from the expert's internal evaluation of other reactions.
2. Inconsistency: Inconsistency bias occurs when people are inconsistent in their solving of problems. This is the most common bias. As the experts' thinking evolves, their current thoughts or solution may contradict those that they expressed earlier.
3. Wishful thinking: Occurs when individual's hopes influence their judgement.
4. Misinterpretation by expert: Occurs when the methods of elicitation and documentation alter the expert's responses. If the experts cannot adequately translate their judgements into the response mode, misinterpretation can result. Experts usually have difficulties with the probabilities and ranks response mode.

Our approach to deal with bias was to try to focus on handling them. The following points summarize the steps we went through to try to handle biases.

1. Once the biases were anticipated, the elicitation process was reviewed in order to try to handle the sources of bias:

- Social pressure, group thinking: The written answers to the questionnaires were quickly reviewed by the interviewer before the interview. Consequently, during the interview, the mediator was able to ensure that the original opinion of every expert was considered.
- Inconsistency: For the knowledgebase questionnaires (appendices B and C), Saaty's consistency check (appendix A) was used to ensure consistency. For the case studies, inconsistency was minimized by the fact that the solution was the result of a group consensus.
- Wishful thinking: The bias was minimized by the fact that the final answers were the result of a group consensus.
- Misinterpretation by expert: Recall that to make sure that the questions were easy to understand and to make sure that reviewers would not be concerned about bias in the phrasing of the questions, one external expert was asked to review the questions. Also, for the knowledgebase questionnaires (appendices B and C) the AHP method was used. The rationale behind using this approach is that the elicitation of the pairwise comparisons is easier and better accepted by the expert than the direct elicitation of the probabilities of interest.

2. At the beginning of the process the experts were made aware of the potential intrusion of the particular biases and they were also familiarized with the elicitation procedures.
3. The data gathered during the written part of the elicitation process were reviewed in comparison with the group interview solutions to look for bias.

7.4 Conclusion

To prove that the proposed model is tenable, a prototype was developed to be able to analyse the three case studies presented in appendix D. A group of experts had to be consulted to build the prototype. The questionnaires we used to elicit the experts' judgements are available in appendices B to D. To make sure that the questions were easy to understand and to make sure that reviewers would not be concerned about bias in the phrasing of the questions, one external expert was asked to review the questions. Our selection schema to select the group of experts was based on having experts name other experts. Some experts were from DND (Red Team) and others from the Computer Security Establishment. The group interview method was selected to help in eliciting experts' judgements. To try to avoid group bias, the questionnaires were sent to the experts in advance. The experts were asked to answer the questions in writing on their own before the interview. For the knowledgebase questionnaires (appendices B and C), Saaty's consistency check (appendix A) was used to ensure consistency. For the case studies, inconsistency was minimized by the fact that the final ranking was the result of a group consensus.

Chapter 8 - Model validation and performance assessment

8.1 Introduction

Chapter 7 explained how the different processes presented in Figures 5.5 and 6.5 were implemented in what is defined as a prototype. The objective of the present chapter is to validate the proposed risk model, by analysing the GRV scores, produced by the prototype for the exposures presented in three case studies (see appendix D).

Transparency in the model validation is important to prove the value of the research performed. Consequently, this chapter first presents the experimental methodology.

Then, the outputs of the prototype are analysed. Finally, a sensitivity analysis is performed on the knowledgebase data used in the prototype (see Table 7.1, processes 1 and 11).

8.2 Experimental methodology

8.2.1 Case Study

To validate our work an analysis needed to be performed. The testing of three risk assessment case studies allowed this. The cases' analysis all involved determining what the next best step was to improve the security posture of a small network domain. The three case studies considered different types of organization. The analysis of the first case allowed examining the risk involved by the same type of exposure on different assets. The analysis of the first and second cases allowed the analysis of cases where

there was important interdependency between various services. Analyzing the last case permitted an evaluation where all the states for every P_{ik} variable were represented. The three case studies were based on Cybercop¹⁴ scans. The Department of National Defence (DND) facilities were used to get operational data for the first two case studies. The third case was based on a scan of a DND test lab. From this last scan, a fictive scenario was built.

In order to validate the model, the output from the analyses of the three cases using the RCNS prototype needed to be compared with the ranking provided by experts. Hence experts' opinions needed to be used as the standards to validate the research. Our hypothesis was that our method should result in predictions that were more accurate than the ranking furnished by a security auditing tool such as Cybercop and as accurate as the ranking provided by expert analysis. So, a group of experts were asked to analyse the three scenarios presented in appendix D and to rank the i, k pairs. The elicitation process was the same as described in chapter 7. Recall that the case studies were sent to the experts in advance and that the experts were asked to answer the questions in writing on their own before the interview. This allowed the individual analyses to be used to establish a confidence interval. Our main interest was the experts' final rankings. However, the experts' problem-solving processes were also reviewed to make sure that the right information was entered in the prototype (see Table 7.1 processes 4,6,7 and 8). In this situation, the literature suggests gathering data from a select few experts [MEY

¹⁴ Cybercop is a Security Auditing Tool

91] . Recall that five experts agreed to take part in the exercise. For this application, in addition to the experience mentioned in chapter 7, the experts needed to be skilful in solving the problem, articulate in describing the problem solution and willing to commit to this difficult time consuming task. They also needed to have some experience in exploiting different types of exposures.

8.2.2 Basis for ranking comparison

A critical problem in decision analysis is how to evaluate the difference between two or more different rankings. In order to compare the different rankings, it is necessary to convert the differences of the rankings into numerical data. In this section we present three categories of conflict evaluation methods and explain why the normalized Sum-of-Squares of Differences in Rank technique was selected to validate the results.

8.2.2.1 Number of disagreements

One of the easiest ways of comparing the results of rankings is to count the number of disagreements. This method provides good results in situations where there is a minimal difference between the rankings [RAY 99] . The problem with this method is that it does not consider, for example, that a disagreement of two positions is more significant than disagreement in only one position.

8.2.2.2 Sum-of-Squares of differences in rank

This method provides for discrimination between major differences in ranks. Its minimum sum is zero when there is a total agreement in ranking. Its maximum occurs in cases of total inversion of order of ranking. This procedure can also be normalized by dividing each sum by the maximum sum thereby forcing the range of values to fall in the interval $[0, 1]$. The concept behind the method is best illustrated via a simple example [RAY 99]. Let's consider the ranking of five entities A1, A2, and A3, A4, A5. There are 120 (i.e., $5! = 120$) possible rankings for this case. We assume that the reference ranking is: (1, 2, 3, 4, 5). In applying the subject method, the following is revealed:

Case I:

Original Ranking: 1 2 3 4 5

Minimum (non-zero) Deviation: 1 2 3 5 4

$$\text{Sum-of-Squares: } (1-1)^2 + (2-2)^2 + (3-3)^2 + (4-5)^2 + (5-4)^2 = 2$$

Case II:

Original Ranking: 1 2 3 4 5

Specific Ranking: 3 4 1 5 2

$$\text{Sum-of-Squares: } (1-3)^2 + (2-4)^2 + (3-1)^2 + (4-5)^2 + (5-2)^2 = 22$$

Case III:

Original Ranking: 1 2 3 4 5

Maximum Deviation: 5 4 3 2 1

$$\text{Sum-of-Squares: } (1-5)^2 + (2-4)^2 + (3-3)^2 + (4-2)^2 + (5-1)^2 = 40$$

When the above conflict rankings are normalized by dividing each through by the maximum value (i.e., the value 40), the previous numerical results become: 0.05, 0.55, and 1.00, for case I, II, and III, respectively. These values seem relevant as a measure of conflict since they associate a lower value with minimum conflict and the value 1.0 with total disagreement.

8.2.2.3 Sum-of-absolute difference in rank

This method is similar to the previous method except that it assesses accuracy in ranking in terms of absolute difference instead of sum of square. However, this method does not amplify the differences in ranking as the Sum-of-Squares of Differences in Rank method does. In fact, it has been proven that the squares method places more weight upon the positional agreement [RAY 98] .

8.3 Empirical validation

Having described the experimental methodology in the first part of this chapter, we now turn to empirical validation. The accuracy in ranking is assessed in terms of Sum-of-Square. The confidence limit to evaluate acceptable ranking reversal is assigned on a case-by-case basis. The limit is set by the largest difference between the individual expert rankings and the reference ranking. The individual expert rankings were obtained from the written analysis made by the expert prior to the group interview. The reference ranking was obtained as the result of the total agreement between the experts during the group interview. The reference rankings for the three cases studied are summarized in Table 8.1.

Table 8.1. ranking consensus (reference ranking)

CASE 1	CASE 2	CASE 3
Exposure/Asset	Exposure/Asset	Exposure/Asset
1. Syn flood check / router	1. Rip Spoofing check/ Router	1. Omni HTTPD Imagemap CGI / Quartz
2. Syn flood check / Server 1	2. Web site Uploader CGI check / Server1	2. Open news server check/ Quartz
3. IIS showcode.asp / Server 3	3. FTP File write permission check /Server 4	3. IIS newdsn.exe bug / Quartz
4. NetBIOS-SMB Accessible share / Server 2	4. FTP Port open in sequential order / Server 4	4. IIS ism.dll Basic / NTLM Authentication / Quartz
5. SNMP Community check / PC3	5. SMTP Banner check / Server2	5. SNMP Community check / Shale
6. IP Fragmentation- Teradrop-2 attack / PC1 and PC 2	6. Portmapper rgister / unregister check / Server 4	6. MIB-II UDP Table / Granite
7. Windows NT – RPCSS.EXE Denial of Service / PC5	7. Finger access conrol check / Server 4	7. Unpassworded NetBIOS/SMB check / Granit
8. Unpassworded NetBIOS-SMB check / PC4	8. rstatd check / Server 4	8. Unpassworded NetBIOS/SMB check / Shale
	9. HP printer Remote Print check / Printer	
	10. Network time protocol server present /Server 2	

It is to be mentioned that the first case only ranks nine out of ten exposures because the “syn flood” exposure on the network printer cannot be fixed. Also, the third scenario only ranks eight of the ten exposures for the same reason. In addition, in the first case “IP Frag PC1” and “IP Frag PC2” were both ranked six, since according to the scenario, there is no difference between the services provided by PC1 and PC2. However, still in

the first case, “Syn flood router” and “Syn flood server 1” do not have the same rank since both assets provide different services.

Next, we calculated the ranking reversal normalized sum of square for every prediction made by the experts individually to estimate the confidence limit for the three cases. It is to be mentioned that only three of the five experts interviewed were able to analyse the scenarios before the reunion. In consequence, the confidence limit for every case was set as the largest normalized ranking reversal score obtained from the three experts. Tables 8.2 to 8.10 summarize the results obtained from the three experts for every case and highlight the resulting confidence limit in Tables 8.4, 8.7 and 8.9.

Table 8.2. Case 1 - Comparison from expert 1 judgement with the consensus ranking

Reference	1	2	3	4	5	6	6	7	8
Expert 1	1	2	3	4	5	6	6	8	7
Maximum deviation				174					
Normalized ranking reversal score				0.01					

Table 8.3. Case 1 - Comparison from expert 2 judgement with the consensus ranking

Reference	1	2	3	4	5	6	6	7	8
Expert 2	1	2	4	3	6	6	7	8	5
Maximum deviation				174					
Normalized ranking reversal score				0.08					

Table 8.4. Case 1 - Comparison from expert 3 judgement with the consensus ranking

Reference	1	2	3	4	5	6	6	7	8
Expert 3	1	4	2	3	8	6	6	7	5
Maximum deviation				174					
Normalized ranking reversal score				0.13					

Table 8.5. Case 2 - Comparison from expert 1 judgement with the consensus ranking

Reference	1	2	3	4	5	6	7	8	9	10
Expert 1	1	2	3	4	5	6	7	8	10	9
Maximum deviation					330					
Normalized ranking reversal score					0.006					

Table 8.6. Case 2 - Comparison from expert 2 judgement with the consensus ranking

Reference	1	2	3	4	5	6	7	8	9	10
Expert 2	1	2	3	4	5	6	7	8	9	10
Maximum deviation					330					
Normalized ranking reversal score					0					

Table 8.7. Case 2 - Comparison from expert 3 judgement with the consensus ranking

Reference	1	2	3	4	5	6	7	8	9	10
Expert 3	1	2	3	4	5	8	9	7	6	10
Maximum deviation					330					
Normalized ranking reversal score					0.055					

Table 8.8. Case 3 - Comparison from expert 1 judgement with the consensus ranking

Reference	1	2	3	4	5	6	7	8
Expert 1	1	2	3	4	5	6	7	8
Maximum deviation				168				
Normalized ranking reversal score				0				

Table 8.9. Case 3 - Comparison from expert 2 judgement with the consensus ranking

Reference	1	2	3	4	5	6	7	8
Expert 2	1	3	2	4	5	6	8	7
Maximum deviation				168				
Normalized ranking reversal score				0.02				

Table 8.10. Case 3 - Comparison from expert 3 judgement with the consensus ranking

Reference	1	2	3	4	5	6	7	8
Expert 3	1	2	3	4	5	6	7	8
Maximum deviation				168				
Normalized ranking reversal score				0				

The RCNS prototype knowledgebase was built as described in Table 7.1. The bridge attribute selected to compute m_{sik} was \$2500 (see chapter 5). The risk model rankings were then compared to the reference ranking. Tables 8.11 to 8.13 summarize the normalized ranking reversal scores obtained with the prototype for the three case studies.

Table 8.11. Case 1 - Comparison from the RCNS prototype with the consensus ranking

Reference	1	2	3	4	5	6	6	7	8
RCNS	1	2	3	4	5	6	6	7	8
Maximum deviation				174					
Normalized ranking reversal score				0					

Table 8.12. Case 2 - Comparison from the RCNS prototype with the consensus ranking

Reference	1	2	3	4	5	6	7	8	9	10
RCNS	1	2	3	4	5	6	9	7	8	10
Maximum deviation				330						
Normalized ranking reversal score				.018						

Table 8.13. Case 3 - Comparison from the RCNS prototype with the consensus ranking

Reference	1	2	3	4	5	6	7	8
RCNS	1	2	4	3	5	6	7	8
Maximum deviation				168				
Normalized ranking reversal score				0.01				

The scores presented in Tables 8.11 to 8.13 suggest that according to the confidence limits set in Tables 8.4, 8.7 and 8.9, our method results in predictions that are as accurate as the ranking provided by expert analysis. It goes without saying that different baseline PCMs were used for the different case studies. This makes sense since the sensitivity levels of the base attributes can take different values for the same service from one organization to another. For example, in appendix D, the unlimited number of users of the web server in scenario 1 (school) does not have the same value as the unlimited

number of users of the web server in the third scenario (e-business). Table 8.14 summarizes the results for the three cases. The experimental data are available in appendix F.

Table 8.14. Summary of experimental data

Case 1 ($v_{BA} = 2500\$$)			Case 2 ($v_{BA} = 2500\$$)			Case 3 ($v_{BA} = 2500\$$)		
Exposure/ Asset (GRV \$)	$V_{ik} (\$)$	P_{ik}	Exposure/ Asset (GRV \$)	$V_{ik} (\$)$	P_{ik}	Exposure/ Asset (GRV \$)	$V_{ik} (\$)$	P_{ik}
Syn flood check / Router (22,747)	25,825	0.88	Rip Spoofing chek /Router (48,111)	54,622	0.88	Omni HTTPD Imagemap CGI / Quartz (20,568)	23,100	0.89
Syn flood check / Server 1 (16,384)	22,481	0.72	Web site Uploader CGI check / Server 1 (4,481)	5,069	0.88	Open news server check / Quartz (19,305)	21,681	0.89
IIS showcode.as p /Server 3 (6,757)	7,644	0.88	FTP File write permissio n check / Server 4 (2,071)	2,343	0.88	IIS newdsn.ex e/ Quartz (18,693)	20,994	0.89
NetBIOS- SMB Accessible Share / Server 2 (4,159)	7,925	0.52	FTP Port open in sequential order /Server 4 (1,557)	2,343	0.66	IIS ism.dll Basic – NTLM Authentic ation / Quartz (18,972)	21,539	0.88

SNMP Community Check / PC3 (2,766)	3,636	0.76	SMTP banner – check / Server 2 (1,419)	1,866	0.76	SNMP Community check / Shale (1,178)	1,418	0.83
IP Fragmentation-Teardrop-2 Attack / PC1 and PC 2 (2,410)	2,776	0.86	Portmapper register / unregister check / Server 4 (1,321)	2,517	0.52	MIB-II UDP table / Granit (634)	833	0.76
Windows NT – RPCSS.EXE Denial of Service / PC5 (1,650)	2,686	0.61	HP printer remote print check / Printer (1,264)	1661	0.76	Unpassworded NetBIOS-SMB / Granit (512)	833	0.61
Unpassworded NetBIOS-SMB check / PC4 (307)	501	.061	Rstad check / Server 4 (382)	503	0.76	Unpassworded NetBIOS-SMB / Shale (307)	501	0.61
			Finger access control check / Server 4 (382)	503	0.76			
			Network time protocol server present / Server 2 (334)	503	0.66			

As expected, the results for the first case presented in Table 8.14 shows that the same exposure on two different assets does not necessarily entail the same GRV. The summary also makes obvious the fact that both risk value parameters are essential for all

cases. In other words, neither P_{ik} nor V_{ik} could arrive at the same ranking alone. The detailed experimental data (in appendix F) for the three cases demonstrates that it is essential, to obtain a meaningful ranking, to consider the dependency between the different network domain services. In fact, performing the same exercise without considering the interdependencies would lead to a higher-ranking reversal score.

Now, at the beginning of this chapter we mentioned that we also want to demonstrate that our method tended to add value or is able to improve upon the accuracy that can be obtained from security auditing tools (SAT) such as Cybercop. Recall that SAT usually first ranks exposures in terms of qualitative risk factor (high, medium, low). These risk factors are predetermined for every exposure and do not reflect the services value. Once this is done, identification numbers rank the exposures. Tables 8.14 to 8.16 summarize the normalized ranking reversal scores obtained for the three case studies using the Cybercop tool reports.

Table 8.15. Case 1 - Comparison of the Cybercop ranking with the consensus ranking

Reference	1	2	3	4	5	6	6	7	8
Cybercop	1	1	3	5	7	4	2	6	6
Maximum deviation				174					
Normalized ranking reversal score				0.178					

Table 8.16. Case 2 - Comparison of the Cybercop ranking with the consensus ranking

Reference	1	2	3	4	5	6	7	8	9	10
Cybercop	2	1	5	4	8	6	7	3	10	9
Maximum deviation					330					
Normalized ranking reversal score					0.127					

Table 8.17. Case 3 - Comparison of the Cybercop ranking with the consensus ranking

Reference	1	2	3	4	5	6	7	8
Cybercop	1	4	2	3	6	7	5	5
Maximum deviation				168				
Normalized ranking reversal score				0.125				

From Tables 8.15 to 8.17, we can see that none of the scores obtained are inside the acceptable confidence interval (see Tables 8.4, 8.7 and 8.9). This is explained in part by the fact that, as opposed to the expert analysis, Cybercop assumes that the same exposure on two different assets implies the same risk value. The reader can compare with Tables 8.11 to 8.13, which provide the normalized ranking scores for our model, in order to see how our method improves upon the accuracy that can be obtained from Cybercop.

8.4 Sensitivity Analysis

Often knowledgebase data in problems are imprecise and changeable. Therefore, an important step is to perform a sensitivity analysis on the input data. In this section, we explore the impact of modifying the knowledgebase data. Once again, we evaluate the differences among the outputs of the RCNS model in relation with the agreed expert

rankings. The technique used to evaluate the ranking reversal as well as the confidence interval is also the same as previously defined.

8.4.1 Harm value parameter m_{sik} sensitivity analysis

8.4.1.1 Bridge attribute

Let's recall that NCICs require determining a monetary attribute to be able to convert the vectors of covering attributes (eigenvector) into implied increments of value by making a series of pairwise comparisons. The reader can refer to chapter 5 to see how we use a predefined bridge attribute evaluated in monetary terms to express all increments of value in monetary terms. This section presents the result of the sensitivity analysis performed on the bridge attribute. Our hypothesis at first was that the waste value associated with this attribute could be any monetary value. This belief was based on the fact that often data in multi-criteria decision making (MCDM) problems are imprecise and changeable. However, we realized while performing the sensitivity analysis that this is not the case. In fact, as mentioned in chapter 5, the bridge attribute can only take a range of values within a restricted interval. The limit is imposed by the use of Saaty's scale (see Table A.1, appendix A) to fill up the baseline PCM. Chapter 5 introduced the following equation:

$$(v_{Amax}/9) \leq v_{BA} \leq (v_{Amin} * 9)$$

For the three cases under analysis, the limit intervals for the bridge attribute are presented in Table 8.18.

Table 8.18. Bridge attributes limit Interval

	Lower limit		Upper limit	
	Value (\$)	Limitation (v_{Amax})	Value (\$)	Limitation (v_{Amin})
CASE 1	2500	v_{Amax} = (Availability, Very high)	3500	v_{Amin} = (Integrity, low)
CASE 2	2500	v_{Amax} = (Availability, Very high)	3500	v_{Amin} = (Integrity, low)
CASE 3	2500	v_{Amax} = (Availability, Very high)	3500	v_{Amin} = (Integrity, low)

Let's recall that the normalized ranking scores in Tables 8.11 to 8.13 were obtained by using a baseline PCM with a bridge attribute of \$2500. According to Table 8.18, it is possible to obtain similar results, using bridge attributes between \$2500 and \$3500. To verify this hypothesis, the three cases were tested using a bridge attribute of \$3000 and \$3500. The results were conclusive. For the \$3500 bridge attribute, the rankings were the same as presented in Tables 8.11 to 8.13. With the \$3000 bridge attribute, the normalized score for the third case ended up being zero while the scores for the two other cases were identical. The experimental data is presented in appendix F.

8.4.1.2 Baseline PCM

A potential problem with a method that relies upon subjective comparisons is that there is scope for errors. Consequently, one should wonder how vulnerable our method is to such errors. In order to answer this question, we performed a sensitivity analysis in which we successively introduced increasing numbers of erroneous pairwise comparisons. The analysis was performed on the third case study. The third case was chosen since from

section 8.3.1.1 the ranking seems to be more sensitive to a variation in the judgements entered in the baseline PCM. The bridge attribute used for the experiences was \$3000. This allowed starting with a theoretical optimum where it is assumed that all pairwise comparisons are made correctly. In real life environments different organizational expert judgements would most likely lead to different entries in the baseline PCM. For the purpose of this research the baseline PCM entries that differ from our theoretical optimum are referred to as erroneous judgements. The impact of erroneous judgements in this analysis has been examined by simulating the problem of incorrect judgements during the pairwise comparisons. The effect of these incorrect comparisons was assessed by assuming that the estimator could provide one incorrect comparison. This was then augmented in stages from 2 to 10 incorrect judgements. The cases and degree of error were selected randomly. The experimental plan was the following. The pairwise comparison judgements required to analyse the case study were first numbered as presented in italics in Table 8.19. In the table, the covering attributes are represented by the first letter of the base attribute in uppercase, and by the first letter(s) of the sensitivity level in lowercase (see Figure 5.2). Cm represents “confidentiality-medium” for example.

Table 8.19. Essential pairwise comparison judgements

[illegible]

Am	6	21		24	31						
Al	7		13	16							
Uu	8	22		25		1					
U10	9		14	17			29				
Fes	10	23		26		28					
Fnec	11		15	18			30		19		

Then, random numbers between 1 and 31 were generated with Microsoft Excel. These numbers were used to point out the erroneous judgements. The errors from one level were propagated to the next. In this way, the erroneous decisions made for one error were included in two errors, and those made at the two were carried through to three and so on. Thus there was some comparability between different levels of erroneous pairwise judgements. As the judgement of three experts was used to set the ranking confidence limit, performing three experiments seemed adequate. The three experimental scenarios are presented in Tables 8.20 to 8.22.

Table 8.20. Experiment 1

Number of errors										Judgement	Increment
1	2	3	4	5	6	7	8	9	10		
31	31	31	31	31	31	31	31	31	31	Am,Im	Positive
	23	23	23	23	23	23	23	23	23	Fes,Cm	Negative
		21	21	21	21	21	21	21	21	Am,Cm	Positive
			30	30	30	30	30	30	30	Fnec,Al	Positive
				2	2	2	2	2	2	Cm,BA	Positive
					18	18	18	18	18	Fnec,Ih	Positive
						14	14	14	14	U10,Cl	Negative
							9	9	9	U10,BA	Positive
								25	25	Uu,Ih	Positive
									3	Cl,BA	Negative

Table 8.21. Experiment 2

Number of errors										Judgement	Increment
1	2	3	4	5	6	7	8	9	10		
5	5	5	5	5	5	5	5	5	5	Im,BA	Positive
	3	3	3	3	3	3	3	3	3	Cl,BA	Negative
		10	10	10	10	10	10	10	10	Fe,BA	Negative
			2	2	2	2	2	2	2	Cm,BA	Negative
				8	8	8	8	8	8	Uu,BA	Negative
					14	14	14	14	14	U10,Cl	Negative
						23	23	23	23	Fec,Cm	Negative
							28	28	28	Fec,Am	Negative
								30	30	Fnec,Al	Positive
									7	Al,BA	Negative

Table 8.22. Experiment 3

Numbers of errors										Judgement	Increment
1	2	3	4	5	6	7	8	9	10		
30	30	30	30	30	30	30	30	30	30	Fnec,Al	Positive
	19	19	19	19	19	19	19	19	19	Fnec,U10	Positive
		14	14	14	14	14	14	14	14	U10,Cl	Negative
			27	27	27	27	27	27	27	Lm,Cm	Positive
				23	23	23	23	23	23	Fe,Cm	Negative
					16	16	16	16	16	Al,Ih	Positive
						29	29	29	29	U10,Al	Negative
							1	1	1	Ui,Am	Negative
								3	3	Cl,BA	Positive
									31	Am,Im	Negative

The “Judgement” column in Tables 8.20 to 8.22 represents the affected elements in Table 8.19. The “Increment” column is there to define if the error was due to an increase (positive) or a decrease (negative) of the column attribute value with respect to the row attribute value in Table 8.19. A random number generator once again determined the

value of this column. For every experiment the ranking reversal was calculated for an increment of one to three numerical hops in the Saaty Scale. When the inconsistency ratio was 0.1 or more, the ranking reversal score wasn't recorded because it is unlikely that experts would keep results with an inconsistency ratio higher than 0.1 (see appendix A). Figures 8.1 to 8.2 graphically represent the results from the experiments. The complete data sets are presented in appendix F.

Figure 8.1. Case 3: Experiment 1 - accuracy against simulated pairwise comparison error

Figure 8.2. Case 3: Experiment 2 - accuracy against simulated pairwise comparison error

Figure 8.3. Case 3: Experiment 3 - accuracy against simulated pairwise comparison error

The RCNS results for two and three hops were not recorded in Table 8.1 since the inconsistency ratios were higher than 0.1. The horizontal pink lines in Figures 8.1 to 8.3 represent the confidence limit set in Table 8.9. The horizontal yellow line denotes the ranking reversal score obtained in Table 8.17. From these figures, we see that our

method was robust against comparison errors up to a level of 3 errors (10 %). In fact, the ranking reversal scores, when less than 10% erroneous judgements are entered, were below the pink line. Beyond this, there was a small deterioration. However, even when 30% (10 errors) of the judgements were erroneous, our method improved upon the accuracy that can be obtained from Cybercop. It was also often observed that the ranking reversal scores were high when the inconsistency ratios were high. In one sense this is not surprising. It is an encouraging finding if the method is to be practically deployed. In fact, if we redraw Figure 8.2 with an inconsistency ratio cut off of 0.09 instead of 0.1 we get Figure 8.4. If instead, a cut off point of 0.02 is used, as for the theoretical optimum solution, we get Figure 8.5.

Figure 8.4. Case 3: Experiment 2 - accuracy against simulated pairwise comparison error with a cut off inconsistency ratio of 0.09

Figure 8.5. Case 3: Experiment 2 - accuracy against simulated pairwise comparison error with a cut off inconsistency ratio of 0.02

Using a cut off inconsistency ratio of 0.02, similar results were obtained for experiment 1 and 3. In other words, this lead to ranking reversal scores below the pink line. So, we can conclude that when the inconsistency ratio cut off is 0.02 the suggested method is as accurate as the network security experts.

8.4.2 Probabilistic parameter sensitivity analysis

As previously mentioned, a potential problem with a method that relies upon subjective comparisons is that there is scope for errors. As it was explained in chapter 6, the probability parameter P_{ik} just like V_{ik} relies on such judgements. In consequence, one should wonder how vulnerable our method is to such judgements. In order to answer this question, we performed a sensitivity analysis in which we successively modified the value of the pairwise comparisons in Tables 6.3, 6.9 and 6.12. The analysis was performed on three of the five pairwise comparison matrices in section 6.4. It did not seem as important to perform an analysis on Tables 6.5 and 6.7 since the judgments were

coming from the total agreements between a groups of network security experts. The analysis was performed on both the first and third case study. The third case was chosen because it is the only one that implies a variation of the states of the Incident Detection (ID) variable. The first case was studied to see if the conclusion was the same when the state of the ID variable is fix. The bridge attribute used for the first case was \$2500. The bridge attribute used for the third case was \$3000. Once again, this is to allow starting with a theoretical optimum. The analyses only included logic pairwise comparisons. For example, it was always assumed that the threat is more probable if there is an external threat. The relevant results from the analysis are summarized in Tables 8.23 to 8.28. The theoretical optimums are highlighted in blue.

Table 8.23. Case 1 sensitivity analyses on P(T|ID) PCM

Case 1 ($v_{BA} = 2500\\$)		
Exposure / Asset	THEORITICAL OPTIMUM - GRV when it is 2 times more likely that there is a threat if ID= y than if ID= n	GRV when it is 8 times more likely that there is a threat if ID= y than if ID= n
Syn flood check /router	22,747	22,210
Syn flood check / server 1	16,384	15,089
IIS showcode.asp /Server 3	6,757	6,696
NetBIOS-SMB Accessible Share / Server 2	4,159	3,176
SNMP Community check / PC3	2,766	2,600
IP Fragmentation-Teardrop-2 attack / PC1 and PC 2	2,410	2,387
Windows NT –RPCSS.EXE Denial of service / PC5	1,650	1,394

Unpassworded NetBIOS – SMB check / PC4	307	260
---	-----	-----

Table 8.24. Case 3 sensitivity analyses on P(T/ID) PCM

Case 3 (v_{BA} = 3000\$)		
Exposure / Asset	THEORITICAL OPTIMUM - GRV when it is 2 times more likely that there is a threat if ID= y than if ID= n	GRV when it is 8 times more likely that there is a threat if ID= y than if ID= n
Omni HTTPD Imagemap CGI / Quartz	24,064	23,902
Open news server check / Quartz	22,781	22,617
IIS newdsn.exe bug / Quartz	19,218	19,080
IIS ism.dll basic- NTLM Authentication / Quartz	18,870	18,767
SNMP Community check / Shale	1,197	1,263
MIB-II UDP table / Granite	651	612
Unpassworded NetBIOS- SMB check / Granit	525	444
Unpassworded NetBIOS- SMB check / Shale	307	259

Table 8.25. Case 1 sensitivity analyses on P(T|ET) PCM

Case 1 (v_{BA} = 2500\$)		
Exposure / Asset	THEORITICAL OPTIMUM - GRV when it is 9 times more likely that there is a threat if ET= y than if ET= n	GRV when it is 3 times more likely that there is a threat if ET= y than if ET= n
Syn flood check /router	22,747	22,003
Syn flood check / server 1	16,384	19,154

IIS showcode.asp /Server 3	6,757	6,586
NetBIOS-SMB Accessible Share / Server 2	4,159	4,659
SNMP Community check / PC3	2,766	2,850
IP Fragmentation-Teardrop-2 attack / PC1 and PC 2	2,410	2,276
Windows NT –RPCSS.EXE Denial of service / PC5	1,650	1,777
Unpassworded NetBIOS –SMB check / PC4	307	331

Table 8.26. Case 3 sensitivity analyses on P(T/ET) PCM

Case 3 ($v_{BA} = 3000\\$)		
Exposure / Asset	THEORITICAL OPTIMUM - GRV when it is 9 times more likely that there is a threat if ET= y than if ET= n	GRV when it is 3 times more likely that there is a threat if ET= y than if ET= n
Omni HTTPD Imagemap CGI / Quartz	24,064	23,675
Open news server check / Quartz	22,781	22,412
IIS newdsn.exe bug / Quartz	19,218	18,907
IIS ism.dll basic- NTLM Authentication / Quartz	18,870	18,253
SNMP Community check / Shale	1,197	1,214
MIB-II UDP table / Granite	651	671
Unpassworded NetBIOS-SMB check / Granit	525	566
Unpassworded NetBIOS-SMB check / Shale	307	331

Table 8.27. Case 1 sensitivity analyses on P(A|T) PCM

Case 1 ($V_{BA} = 2500\\$)			
Exposure / Asset	THEORITICAL OPTIMUM - GRV when it is 9 times more likely that there is an attack if $T = y$ than if $T = n$	GRV when it is 8 times more likely that there is an attack if $T = y$ than if $T = n$	GRV when it is 2 times more likely that there is an attack if $T = y$ than if $T = n$
Syn flood check /router	22,747	22,476	17,019
Syn flood check / server 1	16,384	16,243	14,815
IIS showcode.asp /Server 3	6,757	6,727	5,047
NetBIOS-SMB Accessible Share / Server 2	4,159	4,153	4,044
SNMP Community check / PC3	2,766	2,740	2,214
IP Fragmentation- Teardrop-2 attack / PC1 and PC 2	2,410	2,382	1,814
Windows NT – RPCSS.EXE Denial of service / PC5	1,650	1,642	1,471
Unpassworded NetBIOS – SMB check / PC4	307	306	274

Table 8.28. Case 3 sensitivity analyses on P(A|T) PCM

Case 3 ($v_{BA} = 3000\\$)			
Exposure / Asset	THEORITICAL OPTIMUM - GRV when it is 9 times more likely that there is an attack if $T = y$ than if $T = n$	GRV when it is 8 times more likely that there is an attack if $T = y$ than if $T = n$	GRV when it is 2 times more likely that there is an attack if $T = y$ than if $T = n$
Omni HTTPD Imagemap CGI / Quartz	24,064	23,775	17,918
Open news server check / Quartz	22,781	22,507	16,963
IIS newdsn.exe bug / Quartz	19,218	18,987	14,310
IIS ism.dll basic- NTLM Authentication / Quartz	18,870	18,647	14,118
SNMP Community check / Shale	1,197	1,441	919
MIB-II UDP table / Granite	651	645	521
Unpassworded NetBIOS-SMB check / Granit	525	523	468
Unpassworded NetBIOS-SMB check / Shale	307	306	274

The tables show that in this case the model is more or less indifferent to errors in judgements. In fact, for the cases studied the errors in judgement did not lead to rank reversal. However, from the results highlighted in bold it is possible to assume that for a different case there could be some rank reversal associated with erroneous judgements. This assumption is based on the fact that the global risk value for some i,k pairs are

getting closer due to errors in judgements. Nevertheless, it is safe to assume that the ranking reversal score that would then be obtained would be inside an acceptable confidence interval. The probabilistic parameter sensitivity analysis just performed is encouraging. In fact, it confirms the belief that getting objective probabilities in Tables 6.11 and 6.13 is not essential to develop a tenable ranking concept. What really needs to be known is that the probability of a successful attack is higher for a pair $i-k$ than for another but not as high as another one.

8.5 Conclusion

This chapter focuses on empirical validation. Three case studies were analysed. The analyses confirmed that our model provides results that are more accurate than the ranking offered by the Cybercop security-auditing tool and as accurate as the ranking provided by expert analysis. The fact that our risk model provides accurate results, as compared to the network security experts, is really encouraging because the proposed model can be automated to dynamically analyse the information from the environment, which results in risk analyses which are less time-consuming and reflect more current results. Also, the RCNS process is not reliant on frequent expert assessments. The RCNS model does not do away with this knowledge and expertise, but rather utilizes this resource better. Less human involvement is, therefore, required.

Often, knowledgebase data in models are imprecise and changeable. Therefore, another important step in this chapter was to perform a sensitivity analysis on the baseline PCM input data. The model was robust against comparison errors up to 10% of erroneous

judgements in the baseline PCM. Beyond this there was a small deterioration. However, even when 30% of the judgements were erroneous our method improved upon the accuracy that was obtained from the security-auditing tool. It was also observed that it was possible to keep the ranking reversal score within the confidence interval by using an inconsistency ratio cut off of 0.02 instead of 0.1.

The probabilistic parameter sensitivity analysis performed was also encouraging. In fact, the analysis confirmed that getting objective probabilities is not essential to develop a tenable ranking concept. What really needs to be known is that the probability of a successful attack is higher for a given asset/exposure pair than for another but not as high as another one.

From the analysis it is concluded that the technique is promising and has the capacity to deal with the new issues brought by the third generation IT environment (see chapter 2).

PART 5 – CONCLUSION

Chapter 9 – Conclusion

9.1 Introduction

This chapter summarizes the topics covered, the lessons learnt from this research and the pros and cons of the proposed model. Let's first summarize the content of the thesis. Part 2 serves as background information, without which the reader would not be able to understand the proposed model. Today's existing risk analysis methods could not easily be used to fulfill today's requirements and a new approach to risk analysis is sorely needed. Part 3 constitutes the main contribution of the thesis, as it contains details of an alternative approach to risk analysis. It presents the reader with an overview of the "RCNS" concepts and introduces the risk value formula that is the heart of the proposed model. The formula is based on the expected loss which is defined as the damages value of the assets at risk multiplied by how exposed they are [PFL 01] [PFL 96] [PEL 01] [NOR 00]. The next two chapters are devoted to discussions on each of the parameters of risk. In this way, chapter 5 provides a detailed explanation of how the damage value parameter can be subjectively estimated. The estimation of this parameter is a multidimensional problem that justifies the use of a Multi-Criteria Decision Making (MADM) methods. Having looked at different MADM method, we decided to use the Nontraditional Capital Investment Criteria (NCIC) principles. The NCIC method provides an easy to use MADM method, which involves the inclusion of multiple, non-monetary attributes of alternatives. The advantage of this method with respect to our

problem is that it represents the final score in monetary terms. Chapter 6 provides a detailed explanation of how the probabilistic parameter can be subjectively estimated. Having looked at different prediction systems, we decided to use Bayesian networks to dynamically evaluate the probabilistic part of our model. The first advantage of doing so is that the Bayesian Networks represents the structure of the arguments in an intuitive, graphical format. The second advantage is that using probability calculus and Bayes theorem, if the evidence changes, it is possible to update the values of all the probabilities in the Bayesian Networks. The beauty of both Bayesian Networks and NCIC is that they are able to accommodate subjective and objective data. Part 4 defines the empirical approach used to evaluate the risk model. First, to prove that the concept was tenable, a prototype needed to be developed. The intent of chapter 7 is to describe how the modeling methodology presented in earlier chapters was implemented using tools such as Hugin Lite [HUG 02] , Expert Choice [EXP 00] and Microsoft Excel. Chapter 8 validates the proposed risk model, by analysing the risk value scores, produced by the prototype for the exposures presented in three case studies described in appendix D. The chapter first presents the experimental methodology. Then, the outputs of the prototype are analysed. Finally, a sensitivity analysis is performed on the knowledgebase data used in the prototype. From the analysis it is concluded that the technique is promising and has the capacity to deal with the new issues brought by the third generation IT environment (see chapter 2).

9.2 Lessons Learnt

The lessons learnt about the proposed methodology are as follows:

- The methodology would be hard to automate without using a baseline PCM. This matrix needs to be customized to fit different organizations. Completing the baseline PCM is time consuming but it needs to be done only once when the risk analysis system is implemented.
- When estimating V_{ik} , a cut off inconsistency ratio of 0.02 instead of 0.1 should be used before accepting the pairwise comparison judgements to ensure a ranking reversal score within the confidence interval (see 8.4.1.2).
- The model tolerated different pairwise comparison judgements to estimate P_{ik} if they remain logical. In fact, for the cases studied the errors in judgement did not lead to rank reversal. However, it is possible to assume that for a different case there could be some rank reversal associated with erroneous judgements. Nevertheless, it is safe to assume that the ranking reversal score that would then be obtained would be inside an acceptable confidence interval (see 8.4.1.3).

The next section is devoted to a discussion on some of the pros and cons of the proposed RCNS approach.

9.3 Value of RCNS

9.3.1 Pros

Following are some of the pros that have been identified:

- The proposed model can be automated to dynamically analyse the information from the environment which results in a risk analysis which is less time-consuming and reflects more current results. One of the major criticisms of current risk-analysis methods is that the process takes too long to complete, which usually makes for outdated results, owing to the changing environment. In other words, the time lapse between the risk-analysis process and the application of the results is too long. The RCNS approach serves drastically to reduce this time lapse by computing the risk associated with every detected exposure every time the data describing the environment are altered.
- The RCNS process is not reliant on frequent expert assessments. The RCNS model does not do away with this knowledge and expertise, but rather utilizes this resource better. Only the initial design and development process of the knowledge base are reliant on the security and organizational experts, whereafter the processes are automated. Less human involvement is, therefore, required.
- The RCNS can be centrally maintained. The size and complexity of the internal network is irrelevant, as the risk analysis takes place at the RCNS Server. Control over the RCNS process, exercised centrally, facilitates the management of large,

distributed environments. Updates or modifications need only to be effected from one point.

- Better utilization of existing security services and mechanisms. Conventional risk-analysis methodologies focus mainly on the identification of new security services and mechanisms. In many cases, existing security services and mechanisms are considered inadequate or inappropriate, with the result that they are removed. The RCNS, on the other hand, is focused on the better utilization of existing security services and mechanisms, which would, therefore, be more cost-effective.
- The proposed RCNS model considers the dependencies between the different services provided by a network domain. It also considers the fact that the services have different sensitivity levels.

9.3.2 Cons

The RCNS is, however, also associated with a few disadvantages. Following, is a discussion on some of these disadvantages:

- The RCNS model relies on quality of information in its knowledgebase. An analysis is only as good as the information it uses. This, however, is an inherent problem for all analyses and is, therefore, not specific to the proposed RCNS model. This reliance on the quality of information could mean that a poorly designed knowledgebase could render the model useless. The only way to solve

this problem is to make use of knowledgeable experts and to accept only very low inconsistency ratios when using NCIC (see 8.4.1.2).

- The RCNS requires substantial preparation in terms of its knowledgebase. A good deal of groundwork is required before the model could be implemented and this is costly. The baseline PCM must, for instance, first be customized for the organization in question. It is, therefore, not an off-the-shelf solution.
- The RCNS model requires global implementation. The proposed RCNS structure needs to be implemented on every asset of a network domain.
- Additional network capacity is required. Though this would be an insignificant factor in small networks with a low volume of network traffic, one would have to look at the impact in larger networks with a high volume of network traffic.
- The creation of an operational version of the RCNS would be really demanding in terms of knowledgeable engineers, since the system involves many different techniques in different areas.

By comparing these pros and cons, however, it soon becomes evident that the pros outweigh the cons, especially as most of the cons are evident in other technologies too and, therefore, not specific to the RCNS only. The pros, on the other hand, are exclusive to the RCNS, making the proposed model worthwhile of careful consideration. The research is by no means complete and further work is required. The next section is devoted to a closer look at possible research areas that could be explored in order to make the RCNS concept viable.

9.4 Future research

Many research opportunities present themselves for the expansion of the proposed model.

Some of these research topics are as follows:

- Chapter 4 quickly presents our views about the RCNS structure. Figure 4.3 clearly demonstrates how we picture the RCNS as a possessor of three constituents: Consoles, Servers, and Asset Agents. The purpose of our research was not to develop this structure. Additional research needs to be performed to see how the proposed structure could be implemented.
- A scaled-down version of the RCNS server was created. A lot more research is required in order to be able to create an operational version integrating the different components of the proposed concept (the component from the two spheres of influence in Figure 4.5).
- Additional exposures could be analysed on bigger network domains.
- Alternative methods for calculating GRV could be investigated. The use of NCIC and Bayesian Networks for calculating the GRV serves its purpose in this thesis. However, other methods could be investigated and the ranking reversal scores could be compared.

The foregoing suggestions represent a few possible areas for future research, in view of the fact that the proposed RCNS concept still needs to be refined in many ways

before it could become a real-life solution. It is hoped, however, that the research undertaken in this thesis constitutes a first step in that direction.

References

- [AMB 01] Ambler, "The object Primer – The Application Developer's Guide to Object Orienting and UML", Cambridge University Press, SIGS Publications Inc, New York, New York, 2001.
- [AMO 94] Amoroso, "Fundamentals of Computer Security Technology", Prentice-Hall PTR, Upper Saddle River, NJ, 1994.
- [ARC 93] Arca, "INFOSEC Handbook, An Information System Security Reference Guide Second Edition" ARCA, San Jose, 1993
- [ARM 81] Armstrong, "Long range forecasting: From crystal ball to computer", New York, New York, Wiley-Interscience, 1981.
- [AVI 01] Aviel, "White-hat security arsenal: Tackling the threats", Addison Wesley, 2001.
- [BAS 00] Bass, "Intrusion Detection Systems and Multisensor Data Fusion" Communications of the ACM, vol. 43, no. 4, April 2000.
- [BAU 88] Bauer and Koblenz, "NDIX-An expert system for real-time network intrusion detection", Proceedings of the IEEE Computer Networking Symposium, pp. 98–106, April 1988.
- [BEL 83] Belton and Gear, "On the short-coming of Saaty's Method of Analytic Hierachy", Omega, vol. 11, no. 3 pp. 228-230, 1983
- [BOU 91] Boucher and MacStravic "Multiattribute Evaluation Within a Present Worth Framework and Its Relation to the Analytic Hierarchy Process", The Engineering Economist, vol. 37, no. 1, Fall 1991.
- [BOU 96] Boucher, Gogus, Bruins, Descovich and Litman, "Multicriteria Evaluation of a centralized Control Station for a Production Line: A Case study", Engineering Validation and Cost Analysis, vol. 1 pp. 17-32, 1996.
- [BOU 97] Boucher, Gogus and Wicks, "A comparaison between two multiattribute decision methodologies used in Capital Investment Decision Analysis", The engineering Economist, v 42, no. 3, pp. 183-184, spring 1997.

- [CHE 91] Chen and Hwang, "Fuzzy Multiple Attribute Decision Making: Methods and Applications", Lecture Notes in economical and Mathematical Systems, no. 375, Springer-Verlag, Berlin Germany, 1991.
- [CIS 94] "Information Technology Security Architecture Handbook", Communication-Electronic Security, June 1994.
- [CLE 97] Clement and Winkler, "Combining probability distributions from expert in risk analysis", 1997,
http://www.bus.utexas.edu/Faculty/Jim.Dyer/DA_WP/WP970009.pdf.
- [COB 01] COBRA web site <http://www.security-risk-analysis.com/> .
- [COH 95] Cohen, "Protection and Security on the Information Superhighway", John Wiley & Sons, New York, 1995.
- [CVE 01] Common Vulnerabilities and exposure web site <http://www.cve.mitre.org/>.
- [CRO 01] Crocker, "An Examination of Sun Microsystems's Bruce Application and the Mitigation of a Confidentiality and Integrity Weakness Using the Entrust® Public Key Infrastructure", A Thesis Submitted to the faculty of Royal Military College of Canada, June 2001.
- [DAL 96] Dalkey, "An experimental study of group opinion: the Delphi method" Future, 1996.
- [DEN 87] Denning, "An intrusion-detection model", IEEE Transaction Software Engineering, SE-13, 2, pp. 222-232, February 1987.
- [DEN A87] Denning, Edwards, Jagannathan, Lunt, and Neumann, "A Prototype IDIES: A real-time intrusion detection expert system", Computer Science Laboratory, SRI International, August 1997.
- [DYE 90] Dyer, "Remarks on the Analytical Hierachy Process", Management Science, vol. 36. no. 3, pp. 249-258, 1990.
- [EXP 00] <http://www.expertchoice.com/>.
- [FLE 95] Fletcher, Halbgewachs, Jansma, Murphy, Lim and Wyss, "Software System Risk Management and Assurance", Proceedings of the 1995 New Security Paradigms Workshop, San Diego, August 22-25, 1995.
- [GUR 00] Gurley, "Intrusion Detection", Macmilian technical publishing, p. 3, 2000.

- [HAH 99] Hahn and Knott, "Non-conjugate Bayesian analysis using the Analytic Hierarchy Process and sampling/importance resembling", ISAHP, Kobe, Japan, August 12-14, 1999.
- [HOC 93] Hochberg, Jackson, Stallings, McClary, DuBois, and Ford, "An automated system for detecting network intrusion and misuse", Computers & Security, Elsevier Science, New York, pp. 235-248, 1993.
- [HOW 96] Howard, "An Analysis of Security Incidents on the Internet", 1989-1995, <http://www.info-sec.com/internet/howard/>.
- [HUG 93] Hughes, "Consistent Utility and Probability Assessment Using AHP Methodology", Mathematical and Computer Modelling 17/4-5, pp. 171-178, 1993.
- [HUG 02] <http://www.hugin.com/>
- [HUM 00] Humphries and Pooch, "Secure Mobile Agents for Network Vulnerability Scanning", Texas A&M University, June 2000.
- [ISO 01] <http://www.securityauditor.net/iso17799/index.htm>.
- [JEN 90] Jensen, Lauritzen and Olesen. "Bayesian Updating in Causal Probabilistic Networks by Local Computations", Computational Statistics Quarterly, 1990.
- [JEN 96] Jensen, "An Introduction to Bayesian Networks", Springer Verlag, 1996.
- [KOZ 97] Kozar, "The Technique of Data Flow Diagramming", 1997, <http://spot.colorado.edu/~kozar/DFDtechnique.html>.
- [LAB 99] Labuschagne, "Risk Analysis Generations - The evolution of Risk Analysis", August 1999, http://csweb.rau.ac.za/deth/research/article_page.htm.
- [MAN 99] Mann and Christey, "Towards a Common Enumeration of Vulnerabilities", January 21-22, 1999 <http://www.cve.mitre.org/docs/cerias.html>.
- [MAR 01] Martin, "The Vulnerabilities of Developing on the Net", 2001, <http://www.cve.mitre.org/docs/DevelopingOnNet.html>.

- [MEY 91] Meyer and Booker, "Eliciting and Analyzing Expert Judgment: A Practical Guide", Knowledge Acquisition for Knowledge-Based Systems series, United Kingdom: Academic Press, London, 1991.
- [MON 00] Monti and Carenini, "Dealing with the Expert Inconsistency in Probability Elicitation", IEEE Transactions on knowledge and data engineering, vol. 12, no. 4, July/August 2000.
- [MUK 94] Mukherjee, Heberlein, and Levitt, "Network intrusion detection", IEEE Network, pp. 26–41 May/June 1994.
- [NEG 02] Negnevitsky, "Artificial Intelligence: A Guide to Intelligent Systems", Addison Wesley Publishing Company, 2002.
- [NEU 95] Neumann, "Computer-related risks", ACM Press, Addison-Wesley Publishing Company, 1995.
- [NIE 98] Niedermayer, "An Introduction to Bayesian Networks and their Contemporary Applications, December 1998
http://www.gpfn.sk.ca/~daryle/papers/bayesian_networks/bayes.html#abstract
- [NOR 00] Northcutt and Novak, "Network Intrusion detection An Analyst's Handbook", Second edition, p. 360, September 2000.
- [PEL 01] Peltier, "Information Security Risk Analysis", Auerbasc, 2001.
- [PFL 01] Pfleeger, "Business It Strategies Advisory Service Creating and Implementing a Security Strategy", Cutter Consortium, vol. 4, no. 3, 2001.
- [PFL 96] Pfleeger, "Security in computing", Second Edition, Prentice Hall, 1996.
- [PW 02] [http://www.stanford.edu/class/e60/LectureNotes/PresentWorthAnalysis\(5\).pdf](http://www.stanford.edu/class/e60/LectureNotes/PresentWorthAnalysis(5).pdf)
- [RAY 99] Ray and Triantaphyllou, "Procedures for the evaluation of conflicts in rankings of alternatives", Computers and Industrial Engineering, vol. 36, no. 1, pp. 35-44, 1999.
- [RAY 98] Ray and Triantaphyllou, "Evaluation of Rankings With Regard to the Possible Number of Agreements and Conflicts", European Journal of Operational Research, vol. 106, no. 1, pp. 129-136, 1998.
- [ROB 79] Roberts, "Measurement Theory with Applications to decision-making", Utility and the Social Sciences, London, Addison Wesley, 1979.

- [SAA 80] Saaty, "The Analytic Hierarchy Process", New York, N.Y., McGraw Hill, 1980, reprinted by RWS Publications, Pittsburgh, 1996.
- [SCH 00] Schneier, "Secrets and Lies", John Wiley & Sons, New York, NY, 2000.
- [SCR 01] Scambray, McClure and Kurtz, "Hacking Exposed, Network Security Secret & Solutions", Second Edition, McGraw-Hil, 2001.
- [SER 02] www.dcs.qmul.ac.uk/~norman/SERENE_Help/sereneWhat_is_a_BBN.htm
- [SEA 76] Seaver, "Assessment of group preferences and group uncertainty for decision making", Social science research Institute, University of Southern California, 1976.
- [SEA 83] Seaver and Stillwell, "Procedures for using expert judgment to estimate human error probabilities in nuclear power plant operations", Sandia National Laboratory report SAND82-7054, 1993.
- [SMA 02] Smartdraw.com, "How to Draw Data Flow Diagrams (DFD)"
<http://www.smartdraw.com/resources/centers/software/dfd.htm>.
- [SNA 91] Snapp, Dias, Goan, Grance, Heberlein, Ho , Levitt, Mansur, Mukherjee, Pon , and Smaha, "A system for distributed intrusion detection", In Proceedings of IEEE COMPCON, NY, March 1991.
- [SOS 02] <http://www.sosmath.com/matrix/eigen2/eigen2.html>.
- [STE 87] Stephanou and Sage, "Perspectives on imperfect information processing", IEEE Transaction on Systems, Man and Cybernetics, SMC-17(5) pp. 780-798, 1997.
- [TIV 01] http://www.tivoli.com/products/index/secureway_risk_mgr/.
- [TRI 00] Triantaphyllou, "Multi-criteria decision making methods: a comparative study", Kluwer academic publisher, 2000.
- [VON 71] Von Holstein, "Two techniques for assessment of subjective probability distribution and experimental study", Acta Psychologia, 1971.
- [VOO 02] Voorbraak, "Evidence Combination in AI and Robotics",
<http://turing.wins.uva.nl/~fransv/articles/NAIC96.ps>.

- [WRI 99] Wright, "Third generation risk management practices", Computer fraud and security, Elsevier Science Ltd., February 1999.
- [YAG 79] Yager, "An Eigenvalue Method of Obtaining Subjective Probabilities", Behav. Sci. 24, pp 383-387, 1979.

Acronym

AHP: Analytical Hierarchy Process

BN: Bayesian Network

CPF: Conditional Probability Function

CPT: Conditional Probability Table

CI: Consistency Index

CMDS: Computer Misuse Detection System

CR: Consistency Ratio

CSE: Computer Security Establishment

CVE: Common Vulnerability and Exposure

DAG: Directed Acyclic Graph

DoS: Denial of Service attack

DND: Department of National Defence

DNS: Domain Name Service

HES: Host based Exposure assessment System

IDS: Intrusion Detection System

IS: Information System

IT: Information Technology

MADM: Multi-Attribute Decision Making

MODM: Multi-Objective Decision Making

NES: Network based Exposure assessment System

NCIC: Non-traditional Capital Investment Criteria

PC: Personal Computer

PCM: Pairwise Comparison Matrix

RCNS: Risk Control Network Service

SAT: Security Auditing Tool

TRTH: Trace Route to host

TSRM: Tivoli Secure Way Risk Manager

WS: Work Station

WSM: Weight Product Method

WSM: Weight Sum Method

Lexicon

Agreement: This state is a harmony of opinion that occurs when different decision makers conclude that a given concept is of a specified rank.

Alternative: Usually alternatives represent the different choices of action available to the decision maker.[TRI 00]

Attack: An attack is a single unauthorized access attempt, or unauthorized use attempt, regardless of success.

Attribute: Attributes are also referred to as “decision criteria”. Attributes represent the different dimensions from which the alternatives can be viewed. [TRI 00]

Asset: Platform (ex: equipment used for input, storage, processing, transfers...) and interface equipment (ex: router, firewall)

Asset Classification and Control : The objectives of this ISO17799 section are: To maintain appropriate protection of corporate assets and to ensure that information assets receive an appropriate level of protection.

Audit: Audit is defined as the official systematic examination of accounts to ascertain their accuracy[GUR 00]

Availability: The goal of ensuring that information and information processing resources both remain readily accessible to the authorised users [ARC 93]

Bayesian Networks: A Bayesian network consists of the following

- A set of variables and a set of directed edges between variables
- Each variable as a finite set of mutually exclusive states
- The variables together with the directed edges form a directed acyclic graph (DAG). (A directed graph is acyclic if there is no directed path $A_1 \rightarrow \dots \rightarrow A_n$ such that $A_1 = A_n$)
- To each variable A with parents $B_1, \dots, B_n$ there is attached a conditional probability table $P(A|B_1, \dots, B_n)$ [JEN 96]

Business Continuity Planning : The objectives of this ISO17799 section are: To counteract interruptions to business activities and to critical business processes from the effects of major failures or disasters.

C/I/A: stands for confidentiality, Integrity, Availability: “the three objective of security”[PFL 01]

Confidentiality: The property that information is not made available or disclosed to unauthorised individuals, entities, or processes [ARC 93] . Confidentiality is sometimes called secrecy or privacy [PFL 96] .

Configuration Management: The management of security features and assurances through control of changes made to a system’s hardware, software, firmware, documentation and test throught the devlopment and operational life of the sytem.

Conflict: The situation existing when decision makers fail to agree upon two or more concepts

Countermeasure:” Protection to bloc treats or close vulnerabilities “[PFL 01]

Compliance: The objectives of this ISO17799 section are: 1) To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements 2) To ensure compliance of systems with organizational security policies and standards 3) To maximize the effectiveness of and to minimize interference to/from the system audit process.

Computer & Network Management: The objectives of this ISO17799 section are: 1) To ensure the correct and secure operation of information processing facilities; 2) To minimise the risk of systems failures; 3) To protect the integrity of software and information; 4) To maintain the integrity and availability of information processing and communication; 5) To ensure the safeguarding of information in networks and the protection of the supporting infrastructure; 6) To prevent damage to assets and interruptions to business activities; 7) To prevent loss, modification or misuse of information exchanged between organizations

Confidence interval: The confidence interval gives an estimated range of values which is likely to include an unknown population parameter, the estimated range being calculated from a given set of data.

Confidence limit: The confidence limit is the boundary value of the confidence interval, that is the value which define the range of the confidence interval.

Cognitive bias: Here an expert’s judgement does not follow objective rules or standards i.e. what can be observed or measured, if such judgements were able to be checked. For example, an expert may tend to remember failures with a disproportional frequency to successes in estimating the functioning of some piece of technology.

Covering attributes: Attributes at the lowest level of the hierarchy. Some times called leaf attributes.

Critical assets: resources that really matter [PFL 01]

Delphi: Isolated experts give their judgements to a moderator. The moderator then redistributes these anonymously allowing individuals to revise their opinions. If desired, iterations can continue until consensus is achieved.

Dynamic risk analysis: Dynamic risk analysis is based on performing small risk assessments when the environment is modified as opposed to performing a comprehensive risk assessment of the entire environment occasionally

Domain: A domain is a definable boundary within which part or all set of functions are executed. This comprise a group of assets.

Dynamically: marked by continuous random change

Environment: The circumstances, objects or conditions by witch a network is surrounded.

Exposure: Weekness of a network that allows the condition which allows a threat to trigger a loss.

Incident: An Incident can involve more than one successful attack that can be related by the goal of the end result.

Individual interviews: An interviewer interviews the expert in a private, usually face-to-face environment.

Inference: Inference in a Bayesian network means computing the conditional probability for some variables given information (evidence) on other variables.

Integrity: The assurance, under all conditions, that a system will reflect the logical correctness and reliability of the operating system; the logical completeness of the hardware and software that implement the protection mechanisms; and the consistency of the data structures and accuracy of the stored data [ARC 93] .

Interactive groups: A group of experts and a session moderator meet face-to-face and the participants interactions are either totally unstructured or structured to some degree.

Intrusion detection: Intrusion detection is the process of monitoring the events occurring in a computer system or network, analyzing them for signs of security problems. [GUR 00]

ISO17799, is a detailed security standard. It is organised into ten major sections, each covering a different topic or area:

- Business Continuity Planning
- System Access Control
- System Development and Maintenance
- Physical and Environmental Security
- Compliance
- Personnel Security
- Security Organisation
- Computer & Network Management
- Asset Classification and Control
- Security Policy

Motivational bias: This occurs when the elicitation process alters the expert's reports of their thoughts or answers. The reasons may be social pressure, for example wanting to please the interviewer or else wanting to concur or demur answers. The interviewer may have led the expert. There may be a conflict of interests.

Periodically: fixed interval between the issues

Personnel Security: The objectives of this section are: To reduce risks of human error, theft, fraud or misuse of facilities; to ensure that users are aware of information security threats and concerns, and are equipped to support the corporate security policy in the course of their normal work; to minimise the damage from security incidents and malfunctions and learn from such incidents. [ISO 01]

Physical and Environmental Security: The objectives of this section are: To prevent unauthorised access, damage and interference to business premises and information; to prevent loss, damage or compromise of assets and interruption to business activities; to prevent compromise or theft of information and information processing facilities. [ISO 01]

Ranking: an ordering on the set of alternatives.

Rank is the position given to a specific alternative or concept within a given ranking. If there are n concepts to be ranked, then the rank is an integer number between 1 and n . Rank of 1 is assumed to be the highest, while rank of n is

considered to be the lowest. Moreover, it is assumed that no two concepts can have the same rank.

Risk analysis: “Risk analysis is that process in terms of which security threats and vulnerabilities are identified, analyzed and assessed in a bid better to understand the

Security Organisation: The objectives of this ISO17799 section are: 1) To manage information security within the Company; 2) To maintain the security of organizational information processing facilities and information assets accessed by third parties. 3) To maintain the security of information when the responsibility for information processing has been outsourced to another organization.

Security Policy: The objectives of this ISO17799 section are: To provide management direction and support for information security.

Service: A service is a function provided by the network domain to the domain’s users or to the system itself.

System Access Control: The objectives of this ISO17799 section are: 1) To control access to information 2) To prevent unauthorised access to information systems 3) To ensure the protection of networked services 4) To prevent unauthorized computer access 5) To detect unauthorised activities. 6) To ensure information security when using mobile computing and tele-networking facilities

System Development and Maintenance: The objectives of this ISO17799 section are: 1) To ensure security is built into operational systems; 2) To prevent loss, modification or misuse of user data in application systems; 3) To protect the confidentiality, authenticity and integrity of information; 4) To ensure IT projects and support activities are conducted in a secure manner; 5) To maintain the security of application system software and data

Threat: Circumstances that have the potential to cause loss or harm [PFL 96] Threats are raised by threat agents, whom may be people causing the threat or conditions that allow the threat to occur. [PFL 01] Events that could happen at any time [PEL 01]

Total Agreement: Agreement upon each and every rank of the n concepts given for ordering.

Exposure: Weakness in the organisation that would create a condition which would allow the threat to cause an impact to an organisation by triggering a loss [PEL 01] “The opportunity for the attack” Flaw allowing the unauthorized access or use.

Appendix A - The Analytical Hierarchy process

This Appendix describes the theoretical and practical substance of AHP in depth.

Additive weighting principles

A survey of MADM methods leads us to believe that AHP is one of the best known and most widely used of all MADM methods [TRI 00] . This is in part because of its simple and intuitive logic and its multi-purpose functionality. The basic logic of AHP is based on the following for additive weighing principles.

- **Alternative Scores:** AHP uses numerical scores to characterize the desirability of each alternative.
- **Attribute Weights:** The relative importance of attributes is defined to be constant across alternatives, and is described using cardinal weights assigned to each of the attributes. The weights are generally normalized so that they sum to 1.
- **Contributions to Desirability:** The performance of each alternative with respect to each attribute is expressed numerically, and the numerical “attribute scores” is comparable across attributes. An alternative’s characteristics with respect to each attribute contribute a calculable amount to the total desirability score of the alternative. This contribution is calculated as the product of the attribute score with the attribute importance weight.

- **Additive:** The separate contributions of each attribute to the total desirability score of an alternative are considered to be additive. The overall desirability score for an alternative is defined as sum of the individual attributes' contributions.

AHP extension of the additive weighting principles

The AHP, as primarily developed by Saaty [SAA 80] , has been discussed extensively in the reviewed literature [TRI 00] [BOU 91][BOU 97] . There are three important ways in which the AHP method extends the basic additive weighting principles described in the previous section. These are its use of pair wise comparisons, the principal eigenvector method, and hierarchy. The following sections take up these three aspects of AHP in turn.

Making Pairwise Comparisons

Decision makers often find it difficult to accurately determine importance weights for a set of attributes simultaneously. As the number of attributes increases, better results are obtained when the problem is converted to one of making a series of pairwise comparisons. AHP formalizes the conversion of the attribute-weighting problem into the more tractable problem of making a series of pairwise comparisons among competing attributes.

AHP summarizes the results of pairwise comparisons in a Pairwise Comparison Matrix (PCM), as shown in Figure A.1.

Figure A.1. AHP PCM

	Attribute 1	Attribute 2	...	Attribute n
Attribute 1	1	Importance of Attribute 1 relative to Attribute 2	...	Importance of Attribute 1 relative to Attribute n
Attribute 2	Importance of Attribute 2 relative to Attribute 1	1	...	Importance of Attribute 2 relative to Attribute n
...	...	...	1	...
Attribute n	Importance of Attribute n relative to Attribute 1	Importance of Attribute n relative to Attribute 2	...	1

For each pair of attributes, the decision maker specifies a judgment about “how much more important” one attribute is than the other. Each pairwise comparison requires the decision maker to provide an answer to the question: “Attribute A is how much more important than Attribute B, relative to the overall objective?” Saaty has recommended using a 1-9 numerical scale with the verbal equivalents shown in Table A.1 to fill up the table. Note that the judgments in AHP’s pairwise comparisons are cardinal rather than simply ordinal. One specifies not only which attribute is considered to be more important, but also how much more important it is judged to be.

Obviously, the diagonal elements are all equal to 1, because each attribute is “exactly as important as itself. The elements below the diagonal are equal to the reciprocals of the corresponding elements above the diagonal. By consequence, only the shaded elements of the matrix need to be filled in by the decision maker.

Table A.1. Satty’s scale

Judgment	Numerical Equivalents
Extremely more important	9
• Between very strongly and extremely more important	8
Very Strongly more important	7
• Between strongly and very strongly more important	6
Strongly more important	5
• Between moderately and strongly more important	4
Moderately more important	3
• Between equally and moderately more important	2
Equally as important	1

Computing Attribute Weights and consistency check

A second way in which AHP extends the basic Additive weighting principles is that AHP specifies the use of a particular technique (the principal eigenvector method) for converting the paired comparison data into attribute weights, and uses the results of these calculations in a heuristic check of inconsistency among paired comparisons.

Computing Attribute Weights

Once the PCM is complete, a computational procedure is required to translate the comparison data into weights. AHP specifies the use of one particular computational translation method, involving the use of some basic concepts of linear algebra called “eigenvalues” and “eigenvectors”. The attributes weights are the right eigenvector of the PCM. In the following section we explain how the eigenvector is also used to check for consistency among the pairwise comparisons in the PCM.

Saaty’s Heuristic Check of Consistency

Experiments have proven that the human brain is limited in both its short-term memory capacity and its discrimination ability to more than about seven to nine things at a time. Although we do not like to admit it, our brains are quite limited in certain respects. Not only have psychologists demonstrated that humans have difficulty dealing with more than about seven plus or minus two factors at a time, but there is a mathematical basis for this phenomenon. Thomas Saaty [SAA 80] has shown that to maintain reasonable consistency when deriving priorities from paired comparisons, the number of factors being considered must be less or equal to nine. In the most common Saaty approach, the linear scale presented in Table A.1 is used to quantify how much more important an attribute is compared to another one. The Saaty’s scale is deemed adequate to provide the entries into the matrixes. On the other hand, it has been proven [SAA 80] that the use of a linear scale creates an immediate inconsistency in the approach. This happens in spite

of trying as well as possible to provide consistent answers in each of the pair-wise comparisons [SAA 80] .

To be able to verify the judgements coherence, Saaty proposed to calculate the consistency index (CI)

$$CI = (\lambda_{\max} - n) / (n - 1)$$

where $\lambda_{\max}$ is the maximal eigenvalue of the PCM and n is the number of compared elements. The deviation of the maximal eigenvalue from n in the perfectly consistent situation is used to define a inconsistency ratio. Then, the inconsistency ratio (IR) is calculated using the following expression.

$$IR = CI / ACI$$

where ACI is a number found by averaging CI over a large number of random judgement matrices of the same size. The consistency index is useful for identifying possible errors in judgments as well as actual inconsistencies in the judgments themselves. In general, the inconsistency ratio should be less than 0.1 or so to be considered reasonably consistent. Expert Choice 2000 [EXP 00] , a well-known AHP software, automatically perform the calculation when calculating the right eigenvector of a PCM .

Structuring the Problem with Hierarchy

A third way in which AHP extends the basic additive weighting method is that AHP formalizes the use of hierarchy to keep the number of paired comparisons manageable and to facilitate handling MADM problems with numerous or multi-faceted attributes. By structuring a complex MADM problem hierarchically, a decision maker can include detailed attributes where they are useful or essential, while still keeping the number of pairwise comparisons manageable.

The overall goal of the analysis is positioned at the top of the tree structure. At the outermost point (the bottom) of each branch of the tree structure are the so-called covering attributes (leaves attribute). In AHP, the alternatives are compared or scored only with respect to each of the covering attributes. Once the problem has been structured hierarchically, the attribute-weighting problem becomes one of finding normalized weights for each set of attributes (and sub attributes, and sub-sub attributes, etc.) in the hierarchy. It was previously mentioned that when the hierarchy only has one level of attributes, the overall desirability score for an alternative is defined as the weighted sum of that alternative's attribute scores. However, for problems with more than one level of attributes, this formula must include additional "nested" weighted sums. That being said, even for problems with many-level hierarchies, it still comes down to a weighted sum of attribute scores. The weight of the covering attributes are multiplied by the global weight of their parent element, producing global weights throughout the hierarchy and then adding the global weights for the covering attributes. The following section describes

how AHP compute the covering attribute score that are used to evaluate the overall desirability score.

Computing numerical and comparable attribute scores

Having described in the previous sections how to derive the weights using AHP, we now describe the problem of computing numerical and comparable attribute scores. There are two ways to derive numerical and comparable attribute scores. . We describe each approach in turn.

Scoring Alternatives Using PCMs

Often a small number of alternatives (less than 7) are involved. In this case, PCM-based scoring can be used to derive comparable numerical attribute values. To derive attribute values using a PCM, the decision maker uses the same methods, which were previously described for making a series of pairwise comparisons and synthesizing the results. The only difference is that, in this case, the alternatives are compared in terms of strength of preference (rather than importance) with respect to the attribute of interest. The principal eigenvector method can then be used to calculate a vector of attribute values based on the PCM.

Scoring Alternatives using formulas

Often the data characterizing the performance or desirability of the alternatives with respect to the covering attribute can be represented linearly. Other times a large number of alternatives (possibly hundreds or thousands) are involved. In these cases, it is

possible to calculate the covering attribute scores directly by using a ratings approach to rate the alternatives against some defined scale(s). In other words, formulas can be defined under every covering attribute. Each covering attribute's formula converts data about the alternatives to values. Expert choice 2000 [EXP 00] defines four different formula types to create scales to prioritize each alternative

- **Ratings:** Used to "rate" alternatives using intensities such as No, Low, Medium, High and Very high. This is used for subjective aspects of an evaluation or when there is no hard data available. Pairwise comparisons are used to develop ratio scale priorities for the rating intensities.
- **Step Functions:** A Step Function is similar to Ratings in that it consists of a scale of prioritized intensities. However, the Step Function translates the data into the appropriate rating intensity for each alternative.
- **Utility Curves:** Utility curves translate data into priorities. Whereas the Step Function consists of discrete steps, a Utility Curve is continuous.
- **Direct:** enter priorities directly

Appendix B – Elicitation of expert judgement to determine P(Threat|Complexity)

For the purpose of our research the level of complexity related to the exploitation of an exposure needs to be categorised as either: high, medium, or low. This questionnaire is very simple. You are asked to fill in three blank squares with a number from 1 to 9. Your ratings are then going to be used to normalize the scores for Low, Medium, High in order to ensure statistical validity across a group of expert. For the purpose of this exercise complexity is defined as “the difficulty involved in exploiting an exposure”. Some attacks against computer systems are more complicated than others; exploiting an exposure in a www CGI program may involve merely inserting a "magic" character in a form field, while other attacks may require a carefully coordinated series of interactions with obscure network services. The level of difficulty related to the exploitation of an exposure is categorised as either: high, medium, or low. The categories are defined as follow:

- The complexity of exploitation is “low” when the attack can be executed by an unskilled attacker without any special tools (perhaps by using standard Unix utilities, or by using their web browser). The problem may be obvious even to someone who is not familiar with the issues involved in computer security.
- The complexity of exploitation is “medium” if a special-purpose software tool is required to exploit the problem; this tool is probably quite easy to use and understand by a neophyte hacker, but exploitation of this problem may be out of the reach of individuals that are not familiar with the security community or the hacker underground.
- The complexity of exploitation is “high” if the exploitation of this problem requires exploit code, which is difficult to write and may require access to specific types of computer systems. Actually using this tool may require specific knowledge of the exposure and the system on which it is present. The quantitative aspects of this variable are covered in more detail later on in this chapter.

These categories are illustrated below by presenting three examples extracted from a Cybercop Scan.

Example of an exposure characterized as implying a “Low” complexity level: This exposure allows to traces the route to the host being scanned in the same manner as the traceroute program in UNIX or the tracert program in Windows NT. The route information is stored to the network map file. The network mapper uses this information to build a map of the network.

Example of an exposure characterized as implying a “Medium” complexity level: The system time can be obtained from the target host utilizing a capability present within the ICMP protocol. The ICMP protocol provides an operation to query a remote host for the current system time.

Example of an exposure characterized as implying a “High” complexity level: The RPC scanning direct check performs a UDP RPC scan of the remote host, attempting to find services by

bypassing the portmapper or rpcbind. In many instances, the portmapper (port 111), which translates RPC program numbers to port numbers, is being filtered at an organization's filtering device or firewall. By directly scanning for RPC services, it is still possible to obtain a full listing of RPC services running on the remote host, and then contact them directly rather than querying the portmapper first. This check is unreliable over long haul networks, due to the unreliability of the UDP transport layer. In the case where this check is being run over a long haul network, some RPC programs which are actually running, may not appear in the scan results.

The experts are requested to fill in Table 1. Table one represents the likelihood matrix accounting for the comparison of the likelihood of threat conditioned on the different level of complexity previously presented.

Table 1- Matrix of Pairwise comparison of the likelihood of threat

	Low	Medium	High
Low	1		
Medium		1	
High			1

For each pair of attributes, the decision maker is asked to specify a judgment about "how much more likely" one category is to cause a threat than another. Obviously, the diagonal elements of the matrix are all equal to 1, because each attribute is "exactly as likely as itself. The elements below the diagonal are equal to the reciprocals of the corresponding elements above the diagonal. By consequence, only the shaded elements of the matrix need to be filled in. The expert is asked to provide answers to the following questions:

1. How much more likely is an exposure to be exploited if it is of a lower complexity compared to a medium complexity?
2. How much more likely is an exposure to be exploited if it is of a lower complexity compared to a higher complexity?
3. How much more likely is an exposure to be exploited if it is of a medium complexity compared to a higher complexity?

The 1-9 numerical scale with the verbal equivalents presented below has to be use to answer the questions.

Judgment	Numerical Equivalents
Extremely more likely	9
• Between very strongly and extremely more likely	8
Very Strongly more likely	7
• Between strongly and very strongly more likely	6
Strongly more likely	5
• Between moderately and strongly more likely	4
Moderately more likely	3

• Between equally and moderately more likely	2
Equally as likely	1

Expert Description

Name _____
 Expertise _____

Experience _____

Academic Background _____

Appendix C – Elicitation of expert judgement to determine P(Threat | Motivation)

For the purpose of our research the level of motivation related to the exploitation of an exposure needs to be categorised as either: high, medium, or low. This questionnaire is very simple. You are asked to fill in three blank squares with a number from 1 to 9. Your ratings are then going to be used to normalize the scores for Low, Medium, High in order to ensure statistical validity across a group of expert. To do so the following notation is defined.

K = Set of relevant exposures types for a network domain ($k \in K$)

V_{DK} : The highest potential total damage value caused to a set of service in monetary term on a network domain by a successful exposure k attack on a given asset

V_k : Total damage value caused to the domain services in monetary terms, by a successful exposure k attack on a given asset

M_k : The motivation level associated with a successful exposure attack

From there, the following equation is used to compute the motivation level

$$M_k = \frac{V_k}{V_{DK}}$$

The level of motivation related to the exploitation of an exposure needs to be categorised as either: high, medium, or low. To do so a step function is used. To generate the step function the lower and higher data bound for M_k are defined as follow

State	Lower bound	Higher bound
High	0.66	1
Medium	0.33	0.66
Low	0	0.33

The experts are requested to fill in Table 1. Table one represents the likelihood matrix accounting for the comparison of the likelihood of threat conditioned on the different level of motivation previously presented.

Table 1- Matrix of Pairwise comparison of the likelihood of threat

	High	Medium	Low
High	1		
Medium		1	
Low			1

For each pair of attributes, the decision maker is asked to specify a judgment about “how much more likely” one category is to cause a threat than another. Obviously, the diagonal elements of the matrix are all equal to 1, because each attribute is “exactly as likely as itself. The elements

below the diagonal are equal to the reciprocals of the corresponding elements above the diagonal. By consequence, only the shaded elements of the matrix need to be filled in. In other words, the decision maker is asked to provide answers to the following questions:

1. **How much more likely is an exposure to be exploited if it involves a higher motivation compared to a medium motivation?**
2. **How much more likely is an exposure to be exploited if it involves a higher motivation compared to a lower motivation?**
3. **How much more likely is an exposure to be exploited if it involves a medium motivation compared to a lower motivation?**

The 1-9 numerical scale with the verbal equivalents presented below has to be use to answer the questions.

Judgment	Numerical Equivalents
Extremely more likely	9
• Between very strongly and extremely more likely	8
Very Strongly more likely	7
• Between strongly and very strongly more likely	6
Strongly more likely	5
• Between moderately and strongly more likely	4
Moderately more likely	3
• Between equally and moderately more likely	2
Equally as likely	1

Expert Description

Name _____
Expertise _____

Experience _____

Academic Background _____

Appendix D: Case Study - Experts Analysis

Research: A New Method to Analyze Network Security Risk

Contact : Sophie Martel 682-2309

Sophiemartel@videotron.ca

Expert Self-description

It would be appreciated if the expert could complete the following information

Name _____
Expertise _____

Experience _____

Academic Background _____

Background

Today, Network operators are overwhelmed with security issues to fix. They have too many things to do. Therefore, they need a way to priorities their work to deal with the risk involved with the issues. Our research define a risk model that once implemented could provide a rapid and efficient mean of evaluating the risk associated with every scanned exposure on a domain. Our research is based on developing an algorithm that can be run on a computer to dynamically calculate risk inherent to the various exposures. The risk score could then be used to provide a prioritized list of things to fix, security wise, for system administrators. In order to validate the algorithm, the results from the algorithm need to be compared with the opinion of experts. You are these experts. In other words, the algorithm will be considered valuable if it comes to the same conclusion as you, hence your opinions will become the standards for this research. The work is actually quite simple, although it may appear complex at first. You are presented with a complete description of three networks in three different scenarios. There are exposures in these networks. You are asked to rank these exposures in order of the risk they pose. Of course you have to take into account the importance of the services provided by each device when you rank the exposures. There are spaces reserved in the table listing the exposures for you to enter your ranking.

Case Study 1 – School

Background

Figure 1 and table 1.1 present the background information for this case study. Figure 1 represents the network domain of a small school teaching different subjects in the field of electronic and telecommunication.

Figure 1- Case study 1

Table 1.1 – Services definition

Services	Attributes	Sensitivity Level
System Services		
Routing Service	Confidentiality	Low
	Integrity	Med

	Availability	High
Firewall Service	Confidentiality	Medium
	Integrity	High
	Availability	Very High
Switching Service (Hub)	Confidentiality	Low
	Integrity	High
	Availability	Very High
PC1 Operating Service (WIN 95)	Confidentiality	Low
	Integrity	Low
	Availability	Low
PC2 Operating Service (WIN 95)	Confidentiality	Low
	Integrity	Low
	Availability	Low
PC3 Operating Service (WIN 95)	Confidentiality	Low
	Integrity	Low
	Availability	Low
PC4 Operating Service (WIN 95)	Confidentiality	Low
	Integrity	Low
	Availability	Low
PC5 Operating Service (WIN 95)	Confidentiality	Low
	Integrity	Low
	Availability	Low
Printer Operating Service	Confidentiality	Low
	Integrity	Med
	Availability	Med
Server 1 Operating Service	Confidentiality	Low
	Integrity	Very high
	Availability	Very high
Server 2 Operating Service	Confidentiality	Low
	Integrity	high
	Availability	high
Server 3 Operating Service	Confidentiality	Low
	Integrity	Med
	Availability	Med
Domain Name Service (DNS)	Confidentiality	Low
	Integrity	high
	Availability	high
Dynamic Host Configuration Protocol (DHCP)	Confidentiality	Low
	Integrity	Very high
	Availability	Very high
User Services		
Printer	Confidentiality	Low
	Integrity	Med
	Availability	Med
	Number of users	5
	Function	Nice to have
Office Automation	Confidentiality	Low
	Integrity	Med

	Availability	Med
	Number of users	5
	Function	Necessary
Mail Service	Confidentiality	Low
	Integrity	Low
	Availability	Low
	Number of users	5
	Function	Nice to have
Web Server	Confidentiality	Low
	Integrity	Med
	Availability	Med
	Number of users	Unlimited
	Function	Necessary
Web Browser Service on PC1-5	Confidentiality	Low
	Integrity	Med
	Availability	Med
	Number of users	1 by PC
	Function	Necessary
Outlook on PC1-5	Confidentiality	Low
	Integrity	Low
	Availability	Low
	Number of users	1 by PC
	Function	Nice to Have
Internet Service	Confidentiality	Low
	Integrity	Med
	Availability	Med
	Number of users	1 by PC
	Function	Nec

Table 1.1 defines every service on the network domain in terms of a number of attributes. The services are first assigned a sensitivity level with respect to Confidentiality/Integrity/Availability (C/I/A). The sensitivity levels qualitative scales are represented in Tables 1.2 to 1.4 for each of the C/I/A attributes, respectively.

Table 1.2 - Sensitivity rating definitions with respect to the confidentiality

Confidentiality Rating	Non classified Information	Designated Information	For Classified Information
No Sensitivity			
Low Sensitivity	-Need-to know	Protected A	Unclassified
Medium Sensitivity	Unauthorized disclosure could be prejudicial to the organization interest	Protected B	Confidential
High Sensitivity	Disclosure could endanger the organization under study	Protected C	Secret
Very High	Exceptionally grave danger to the		Top Secret

Sensitivity	organization		
-------------	--------------	--	--

Table 1.3 - Sensitivity rating definitions with respect to the integrity

Integrity Rating	Consequences of inaccurate or incomplete data to user's capability
No Sensitivity	No consequence
Low Sensitivity	Minor reduction
Medium Sensitivity	Moderate reduction
High Sensitivity	Major reduction
Very High Sensitivity	Complete stop

Table 1.4 - Sensitivity rating definitions with respect to the availability

Availability Rating	Acceptable down time for the user
No Sensitivity	
Low Sensitivity	Less than 48 hours
Medium Sensitivity	Less than 8 hours
High Sensitivity	Less than 4 hours
Very High Sensitivity	Restoration must be immediate (Less than 5 minutes)

For the users services, we also include attributes that specify the relative importance of the services with respect to one another. The services importances are classified according to their consequence with respect to the business operations. That way, at an equal risk level, the most important services would be considered first. These attributes are only assigned to user services since if the system services are compromised; the business operations are troubled only if the users services that rely on this specific system service are affected. Two attributes characterize the services. The first attribute refers to the number of service's users affected. The second attribute refer to the importance of the services' function. The classification categorization of the services function is in terms of the effect on the business operations success. Clearly, the definition of the operation success varies depending on the area concerned. In the financial sector the success is related to financial gain. In a military command and control environment the success can be associated with saving lives. For another corporation the success might rely on the level of productivity. Table 1.5 outlines our approach to prioritizing a large inventory of user services. We categorize services according to general operations criticality. We define operation critical user's services as follow: A user's services whose loss would preclude the safe and successful execution of the business critical functions.

Table 1.5 - Sensitivity rating definitions with respect to the service function

Function Rating	
Essential	Services which meet the definition of operation criticality above for the task or function in question. As well, there is no identified manual work-around or backup system that could support this function should the particular service fail

Necessary	These services are identical to the essential services except that a known work-around or backup exists.
Nice-To-Have	These services support the given task or function, but are not critical to its safe and successful completion.
Not Required	These services do not support the task or mission in question.

Exposures to be ranked

The following table lists the exposure to be ranked as well as the host on which they were scanned according to figure 1. The exposures are defined in section 3.3. While analyzing this case, the analysts should assume that there are no false positives and that the firewall does its job and protect the internal services from external traffic as per table 1.6.

Table 1.6- Exposures to be ranked

Expert Ranking	Exposure	Host	Protect from external traffic
	SYN flood check	Network Printer	Y
	IIS showcode.asp Vulnerability	Server 3	N
	NetBIOS/SMB Accessible Share	Server 2	Y
	SYN flood check	Server 1	Y
	IP Fragmentation/Teardrop-2 Attack	PC1	N
	IP Fragmentation/Teardrop-2 Attack	PC2	N
	SNMP Community check	PC3	Y
	Unpassworded NetBIOS/SMB check	PC4	Y
	SYN flood check	Router/ firewall	N
	Windows NT - RPCSS.EXE Denial of Service	PC5	Y

Comments: _____

Exposure definition

The Exposures are defined in terms of **Complexity**, **Impact** and **description**. For the purpose of this questionnaire we define **complexity** as “the difficulty involved in exploiting an exposure”. Some attacks against computer systems are more complicated than others; exploiting an exposure in a www CGI program may involve merely inserting a "magic" character in form field, while other attacks may require a carefully coordinated series of interactions with obscure network services. The level of difficulty related to the exploitation of an exposure is categorized as either: high, medium, or low. The categories are defined as follow:

- The complexity of exploitation is “low” when the attack can be executed by an unskilled attacker without any special tools (perhaps by using standard Unix utilities, or by using their web browser). The problem may be obvious even to someone who is not familiar with the issues involved in computer security.
- The complexity of exploitation is “medium” if a special-purpose software tool is required to exploit the problem; this tool is probably quite easy to use and understand by a neophyte hacker, but exploitation of this problem may be out of the reach of individuals that are not familiar with the security community or the hacker underground.
- The complexity of exploitation is “high” if the exploitation of this problem requires exploit code, which is difficult to write and may require access to specific types of computer systems. Actually using this tool may require specific knowledge of the exposure and the system on which it is present. The quantitative aspects of this variable are covered in more detail later on in this chapter.

Impact indicates the specific threat posed by the exposure. We break the implication of the exposure in terms of Confidentiality, Integrity and availability.

E1: SYN flood check

Complexity: Medium

Impact: Availability

Description: A common and dangerous denial of service of attack is called SYN flooding. This attack can be used to completely disable the network services by flooding them with connection requests. This fills the queue which maintains a list of unestablished incoming connections, forcing it to be unable to accept additional connections. Malicious users can completely disable network services, including Web servers, FTP servers, and email traffic.

E2: IIS showcode.asp Vulnerability

Complexity: Low

Impact: Integrity

Description: The Microsoft Internet Information Web Server Version 4.0 contains a number of sample Active Server Page files designed to view the source code of sample applications. One specific file, showcode.asp, does not correctly verify input allowing unauthorized access to files outside the web root of the IIS server. If the IIS Web Server is vulnerable, a significant portion of files on the web server will be accessible to remote attackers.

E3: NetBIOS/SMB Accessible Share**Complexity:** High**Impact:** Confidentiality, Integrity

Description: Service Message Block (SMB) is the standard resource-sharing protocol used by Windows platforms. The SMB protocol is transmitted using NetBIOS, a networking protocol designed to allow groups of PCs to interoperate. NetBIOS is accessible over TCP/IP using the NBT protocol. SMB resource sharing makes use of two different security models, "share-level" and "user-level". In share-level security, groups of files (directory trees) are protected by a password, allowing simple workgroups to be configured simply by ensuring that they share a password. In user-level security, all attempts to access resources are authenticated with a username and password. By manipulating the SMB protocol and services offered by Windows NT, it is possible to obtain a list of shares exported by an SMB service. In addition, Windows SMB servers tend to have several common shares available, the presence of which can be guessed without attempting to obtain a share list. This check attempts to access all shares which are being served by the remote server. If any shares are accessible, an intruder can possibly read or write data from and to the share. This can lead to data being stolen, or modified on the server.

E4: IP Fragmentation/Teardrop-2 Attack**Complexity:** Medium**Impact:** Availability

Description: This allows to sends out invalid fragmented IP packets that trigger a bug in the IP fragment reassembly code of some operating systems.

E5: SNMP Community check**Complexity:** Low**Impact:** Integrity, Confidentiality, Availability

Description: This allows to talk to a hosts SNMP server using some commonly used community names. When a successful connection is made the community is probed to see if it is read-only or read-write. SNMP access provides an attacker with a wide variety of information from an SNMP enabled device. This information ranges from the type and model of the device, to active network connections, processes running on the host, and users logged into the host. SNMP write access provides an attacker with the ability to alter networking and other device parameters. An attacker with write access can alter the routing and arp tables, bring network interfaces up and down, enable or disable packet forwarding and alter several other networking parameters. In addition, vendor extensions may provide other control parameters that an attacker can manipulate. This level of access can lead to denial of service or the compromise of security or confidential information.

E6: Unpassworded NetBIOS/SMB check**Complexity:** Medium**Impact:** Confidentiality

Description: Service Message Block (SMB) is the standard resource-sharing protocol used by Windows platforms. The SMB protocol is transmitted using NetBIOS, a networking protocol designed to allow groups of PCs to interoperate. NetBIOS is accessible over TCP/IP using the NBT protocol. SMB resource sharing makes use of two different security models, "share-level" and "user-level". In share-level security, groups of files (directory trees) are protected by a password, allowing simple workgroups to be configured simply by ensuring that they share a password. In user-level security, all attempts to access resources are authenticated with a username and password. It is possible to obtain a list of shares offered by

an SMB-speaking computer by initiating an SMB session with no username or password (this is referred to as a "null session"). The information available from this transaction can be used by an attacker to conduct further attacks.

E.7 Windows NT - RPCSS.EXE Denial of Service

Complexity: Medium

Impact: Availability

Description: A vulnerability in the RPCSS.EXE process on Windows NT systems allows for a denial of service attack. This denial of service attack causes the RPCSS.EXE process to run in an infinite loop driving the system CPU usage up to 100%. In addition the RPCSS process stops responding to requests. Malicious users can launch this denial of service attack against your Microsoft Windows NT system.

Warning: If this vulnerability was found on the target host, this means that the CyberCop Scanner Security Auditing System successfully performed this denial of service attack. Please reboot the target server immediately for it to function properly.

Case Study 2 – Research organisation

Scenario 2: Background

Figure 2 and table 2.1 present the background information for this case study. Figure 2 represents the network domain of an organization performing research in different fields.

Figure 2- Case Study 2

Table 2.1 – Services definition

Services	Attributes	Sensitivity Level
System Services		
Routing Service	Confidentiality	Low
	Integrity	Very High
	Availability	Very High
Firewall Service	Confidentiality	Med
	Integrity	low
	Availability	Very High
Switching Service (Hub1)	Confidentiality	Low
	Integrity	High
	Availability	High
Switching Service (Hub2)	Confidentiality	Low
	Integrity	High
	Availability	High
PC1 Operating Service (WIN 95)	Confidentiality	Low
	Integrity	Low
	Availability	Low
PC2 Operating Service (WIN 95)	Confidentiality	Low
	Integrity	Low
	Availability	Low
PC3 Operating Service (WIN 95)	Confidentiality	Low
	Integrity	Low
	Availability	Low
Printer Operating Service	Confidentiality	Low
	Integrity	Med
	Availability	Med
Server 1 Operating Service (NT 4.0)	Confidentiality	Low
	Integrity	Med
	Availability	Med
Server 2 Operating Service (NT 4.0)	Confidentiality	Low
	Integrity	Med
	Availability	Med
Server 3 Operating Service (NT 4.0)	Confidentiality	Low
	Integrity	Med
	Availability	Med
Server 4 Operating Service (Unix)	Confidentiality	Low
	Integrity	Med
	Availability	Med
Domain Name Service (DNS)	Confidentiality	Low
	Integrity	high
	Availability	high
User Services		

Printer	Confidentiality	low
	Integrity	Med
	Availability	Med
	Number of users	3
	Function	Nice to have
File Transfer Service	Confidentiality	low
	Integrity	Med
	Availability	Med
	Number of users	3
	Function	Nice to have
Mail Service	Confidentiality	low
	Integrity	Med
	Availability	Med
	Number of users	3
	Function	Necessary
Web Server	Confidentiality	low
	Integrity	Med
	Availability	Med
	Number of users	unlimited
	Function	Nice to have
Web Browser Service on PC1-3	Confidentiality	low
	Integrity	Med
	Availability	Med
	Number of users	1 by PC
	Function	Necessary
Outlook on PC1-3	Confidentiality	low
	Integrity	Med
	Availability	Med
	Number of users	1 by PC
	Function	Necessary
Office Automation on PC1-3	Confidentiality	low
	Integrity	Med
	Availability	Med
	Number of users	1 by PC
	Function	Necessary
Internet Service	Confidentiality	Low
	Integrity	Med
	Availability	Med
	Number of users	1 by PC
	Function	Nec

Table 2.1 defines every service on the network domain in terms of a number of attributes. The services are first assigned a sensitivity level with respect to Confidentiality/Integrity/Availability (C/I/A). The sensitivity levels qualitative scales are represented in Tables 1.2 to 1.4 for each of the C/I/A attributes, respectively. For the users services, we also include attributes that specify the relative importance of the services with respect to one another according to table 1.5.

9.5 Exposures to be ranked

The following table lists the scanned exposures as well as the host on which they were scanned according to network domain illustrated in figure 2. While analyzing this case, the analysts should assume that there are no false positives and that the firewall does its job and protect the internal services from external traffic as per table 2.2.

Table 2.2- Exposures to be ranked

Expert Ranking	Exposure	Host	Protect from external traffic
	Finger access control check	Server 4	Y
	SMTP banner-check	Server 2	Y
	rstatd" check	Server 4	Y
	Network Time Protocol server present	Server 2	Y
	FTP - ports opened in sequential order	Server 4	Y
	FTP file write permission check	Server 4	N
	HP Printer Remote Print Check	Printer	Y
	Portmapper register/unregister check	Server 4	Y
	WebSite Uploader CGI check	Server 1	N
	RIP spoofing check	Router/firewall	N

Comments: _____

9.6 Exposure definition

The Exposures are defined in terms of Complexity, Impact and description as defined in section 2.3

E8:Finger access control check

Complexity: Low

Impact: Confidentiality

Description: This allows to contact the finger daemon on the target-host and retrieve a list of logged in users. The finger service can provide quite a lot of information to outsiders such as:

- o Real names and phone numbers of users

- o User home directory and login shell
- o Amount of time a user has been idle
- o When a user last read e-mail
- o The remote host that a user is logged in from

In addition to revealing possibly private or sensitive information, some of the information finger provides may be used by an attacker to make inferences about trust relationships between hosts on your network, collect usernames for password guessing attempts, obtain phone numbers for "social engineering" attacks, and to monitor the activity on your system.

E9: SMTP banner-check

Complexity: Low

Impact: Confidentiality

Description: This allows to collect the message displayed upon connection to the SMTP port of the target-host. The SMTP port banner usually contains specific information about version of SMTP agent that you are using. This information can be used to launch specific attacks against software with known vulnerabilities. Sendmail, the most popular SMTP server for unix has an extensive history of security problems. Knowledge of specific version information allows an attacker to predict what sort of attacks may be successful against your system.

E10: "rstatd" check

Complexity: Low

Impact: Confidentiality

Description: "rstatd" is an ONC RPC service that provides information about the status of a system (including uptime and usage statistics) to the public. In addition to disclosing sensitive information about the configuration and capabilities of a server, "rstatd" can also provide information that is used by some programs to generate random numbers, and can thus be used as a tool to compromise other servers on a system. This module attempts to poll information from rstatd. Rstatd provides several pieces of information about hosts which run it. Along with ethernet statistics it also provides kernel paging information. None of these statistics should be of any interest to anyone who is not a system administrator on the target network.

E11: Network Time Protocol server present

Complexity: Medium

Impact: Confidentiality

Description: An NTP server was found to be present on the target host. Many Network Time Protocol servers offer detailed information on their setup, including systems which they peer with, system memory configuration, and time statistics. This module obtains information from the remote NTP server using the NTP version 3 protocol and lists the information which can be obtained from the server. Information which can be obtained via NTP includes the following:

- System time statistics (uptime)
- System IO statistics
- System memory statistics

- Time daemon peer listing

E12: FTP - ports opened in sequential order

Complexity: Medium

Impact: Confidentiality, Integrity

Description: The FTP server on the target host open bound ports, utilized by the PASV feature, in sequential order. By opening ports in sequential order, it is easy for an attacker to predict the next port that the FTP service will use, and then connect to this port, retrieving another user's file.

E13: FTP file write permission check

Complexity: Low

Impact: Integrity, Availability

Description: This allows write-enabled files. Having files write-enabled on the FTP server can cause problems such as allowing the site to become a pirated software drop point.

E14: HP Printer Remote Print Check

Complexity: Low

Impact: Availability

Description: The HP printer is configured for remote network printing over IP listen for requests on port 9099 and 9100. Unauthorized clients can send raw postscript files to these ports and cause their contents to be printed, regardless of the permissions set on the printer's LPD service. If the printer is being relied on for hard-copy of security auditing logs, an attacker can disable the printer by flooding it with requests, avoiding hard-copy audit trails. Also, it is possible to telnet to the printer and change the printer IP or disable logging. It is also possible to restrict the printer to accept connections from either a list of IP addresses or a subnet range.

E15: Portmapper register/unregister check

Complexity: High

Impact: Availability

Description: This module determines whether attackers can register and unregister services on the portmapper/rpcbind by using standard RPC calls. This vulnerability does not require address forgery to succeed and provides any network user with the ability to register new services and unregister existing services. Some versions of ONC RPC for Microsoft Windows NT are also known to contain this vulnerability BSDI 2.1, 3.0 and Ultrix are known to be vulnerable to this attack. If an attacker can unset services, he can deny access to critical services on the machine. An attacker with local access to the machine who can set new services can impersonate a server and compromise the security of clients that depend on that service

E16: WebSite Uploader CGI check

Complexity: Low

Impact: Integrity, Availability

Description: Uploader.exe is a sample CGI script that comes with O'Reilly's WebSite web server for NT. Due to insufficient argument checking, the uploader CGI program will allow attackers to upload files to arbitrary directories under the web server root directory. This allows by example to uploads a text file to one of the CGI directories. An attacker could upload a CGI script and invoke it to get access to the web server.

E17: RIP spoofing check

Complexity: Medium

Impact: Integrity, Availability

Description: The target host was found to be utilizing RIP (Routing Information Protocol) to obtain routing decision information. Version 1 RIP is an easily spoofable protocol. It has been determined that the target host is running RIP version 1.

Case Study 3 – Small Entrepreneur business

9.7 Background

Figure 3 and table 3.1 present the background information for this case study. Figure 3 represents the network domain of a test lab.

Figure 3 - Case study 3

Table 3.1 – Services definition

Services	Attributes	Sensitivity Level
System Services		
Router/Firewall OS	Confidentiality	Med

	Integrity	High
	Availability	Very High
Routing Service	Confidentiality	Low
	Integrity	High
	Availability	High
Firewall Service	Confidentiality	Med
	Integrity	High
	Availability	Very High
IDS Service	Confidentiality	Med
	Integrity	No Sens
	Availability	High
Switching Service (Hub)	Confidentiality	Low
	Integrity	High
	Availability	High
Feldspar Operating Service (WIN NT)	Confidentiality	High
	Integrity	High
	Availability	High
PC2 Operating Service (WIN 95)	Confidentiality	Low
	Integrity	Low
	Availability	Low
PC3 Operating Service (WIN 95)	Confidentiality	Low
	Integrity	Low
	Availability	Low
Granite Operating Service (NT 4.0)	Confidentiality	Med
	Integrity	Med
	Availability	Med
Shale Operating Service (NT 4.0)	Confidentiality	Low
	Integrity	Med
	Availability	Med
Quartz Operating Service (NT 4.0)	Confidentiality	Med
	Integrity	Med
	Availability	Med
DHCP Service	Confidentiality	Med
	Integrity	Med
	Availability	Med
WINS service (Granite)	Confidentiality	Low
	Integrity	Low
	Availability	Low
User Services		
Remote Access	Confidentiality	Med
	Integrity	Med
	Availability	Med
	Number of users	10
	Function	Essential
Web Server (Quartz)	Confidentiality	Med

	Integrity	High
	Availability	Med
	Number of users	unlimited
	Function	Essential
Exchange service	Confidentiality	Med
	Integrity	High
	Availability	High
	Number of users	10
	Function	Essential
Web Browser Service on PC1-3	Confidentiality	Low
	Integrity	Low
	Availability	Low
	Number of users	1 by PC
	Function	Necessary
Outlook on PC1-3	Confidentiality	Low
	Integrity	Low
	Availability	Med
	Number of users	1 by PC
	Function	Necessary
News Service	Confidentiality	Low
	Integrity	High
	Availability	low
	Number of users	10
	Function	Necessary
Internet Service	Confidentiality	Low
	Integrity	Med
	Availability	high
	Number of users	10
	Function	Essential

Table 3.1 defines every service on the network domain in terms of a number of attributes. The services are first assigned a sensitivity level with respect to Confidentiality/Integrity/Availability (C/I/A). The sensitivity levels qualitative scales are represented in Tables 1.2 to 1.4 for each of the C/I/A attributes, respectively. For the users services, we also include attributes that specify the relative importance of the services with respect to one another according to table 1.5.

9.8 Exposures to be ranked

The following table lists the scanned exposures as well as the host on which they were scanned according to network domain illustrated in figure 3. While analyzing this case, the analysts should assume that there are no false positives and that the firewall does its job and protect the internal services from external traffic.

Table 3.2- Exposures to be ranked

Ranking by Expert	Exposure	Host	Protect from external traffic
-------------------	----------	------	-------------------------------

	IIS ism.dll Basic/NTLM Authentication Vulnerability	Quartz	N
	Unpassworded NetBIOS/SMB check	Granite	Y
	Unpassworded NetBIOS/SMB check	Shale	Y
	MIB-II UDP table	Granite	Y
	SYN port scanning	Granite ¹⁵	Y
	Omni HTTPD Imagemap CGI	Quartz	N
	Open news server check	Quartz	N
	SNMP Community check	Shale ¹⁶	Y
	IIS newdsn.exe bug	Quartz	N
	SSH information obtain	Router/firewall	N

Comments: _____

9.9 Exposure definition

The Exposures are defined in terms of Complexity, Impact and description as defined in section 3.3

E18: IIS ism.dll Basic/NTLM Authentication Vulnerability

Complexity: Medium

Impact: Integrity, Availability, Confidentiality

Description: Versions 2 and 3 of Microsoft Internet Information Web Server (IIS) utilized the ism.dll file for remote administration which was located in the /scripts/iisadmin/ directory. If this dynamic linked library is accessible, remote users may be able to use brute force password guessing techniques to log in and remotely administer the web server. Upgrading IIS from version 2 or 3 to version 4 does not remove this file. If ism.dll is accessible, the forms of remote authentication enabled are returned. Additional information regarding authentication methods is below. IIS allows three forms of authentication for access, anonymous, basic and Windows NT challenge / response (NTLM). Anonymous access requires no password and generally allows remote users to access a public web server. Basic authentication requires a username and password before access is granted. This form of authentication uses base64 encoding which is not encrypted allowing passwords to be sniffed as they pass across the network. NTLM authentication does encrypt usernames and passwords although is generally only available when all hosts use a Microsoft operating system and the web server is not accessed through a proxy server. Furthermore, in certain versions of IIS NTLM authentication is enabled by default. If either form of

¹⁵ The Incident detection analysts reported an attack using the same exposure on Quartz in the recent past. Assume that the flaw on Quartz was recently rectified but not the flaw on Shale.

¹⁶ The Incident detection analysts reported an attack using the same exposure on Quartz in the recent past. Assume that the flaw on Quartz was recently rectified but not the flaw on Shale.

authentication is enabled username/password combinations can be brute force attacked from remote hosts. The ism.dll file returns which authentication methods are available and may allow the brute forcing of passwords and possible unauthorized access to an IIS server. If basic authentication is enabled passwords are sent in clear (unencrypted) text. Either form of authentication allows users to access a web server or verify username and passwords combinations.

E19: Unpassworded NetBIOS/SMB check

Complexity: Medium

Impact: Confidentiality

Description

Service Message Block (SMB) is the standard resource-sharing protocol used by Windows platforms. The SMB protocol is transmitted using NetBIOS, a networking protocol designed to allow groups of PCs to interoperate. NetBIOS is accessible over TCP/IP using the NBT protocol. SMB resource sharing makes use of two different security models, "share-level" and "user-level". In share-level security, groups of files (directory trees) are protected by a password, allowing simple workgroups to be configured simply by ensuring that they share a password. In user-level security, all attempts to access resources are authenticated with a username and password. It is possible to obtain a list of shares offered by an SMB-speaking computer by initiating an SMB session with no username or password (this is referred to as a "null session"). The information available from this transaction can be used by an attacker to conduct further attacks. Resources offered by SMB servers are called "shares", and are often protected by passwords. An attacker that can compromise the security of an SMB server can gain access to files, stealing confidential data and violating the integrity of the system. An attacker can gain a list of shares to attack by manipulating the SMB protocol; this information can be used to further attacks on the server.

E20: MIB-II UDP table

Complexity: Low

Impact: Confidentiality

Description: This allows to retrieve the table of listening UDP ports from the SNMP daemon with the community name provided in the configuration file. This module does not demonstrate any vulnerability, it simply retrieves information that is available to an attacker that has read access to SNMP. This module uses the community name specified in the configuration file and does not attempt to guess the community name. A separate SNMP community module is provided to probe for SNMP access.

E21: SYN port scanning

Complexity: Medium

Impact: Confidentiality

Description: This allows to scan a target host for listening TCP ports in much the same way as the regular TCP port scanning, however does so by sending a packet to initiate a connection and watching for a response.

E22: Omni HTTPD Imagemap CGI

Complexity: Low**Impact:** Confidentiality, Integrity

Description The utility, `imagemap.exe`, distributed with Omnicron's OmniHTTPD contains a lack of bounds checking which can allow for arbitrary code to be executed on the machine. Exploitation of this CGI program could allow a remote attacker to completely compromise the security of the target system. Steps should be taken immediately to update the affected software package

E23: Open news server check**Complexity: Low****Impact:** Confidentiality, Integrity

Description: This allows a remote user to poll news feed causing a strain on the system resources. Moreover they can post erroneous information from the news server, which may be embarrassing for the company image.

E24: SNMP Community check**Complexity: Low****Impact:** Integrity, confidentiality**Description**

This allows talking to a hosts SNMP server using some commonly used community names. SNMP access provides an attacker with a wide variety of information from an SNMP enabled device. This information ranges from the type and model of the device, to active network connections, processes running on the host, and users logged into the host. SNMP write access provides an attacker with the ability to alter networking and other device parameters. An attacker with write access can alter the routing and arp tables, bring network interfaces up and down, enable or disable packet forwarding and alter several other networking parameters. In addition, vendor extensions may provide other control parameters that an attacker can manipulate. This level of access can lead to denial of service or the compromise of security or confidential information.

E25: IIS newdsn.exe bug**Complexity: Low****Impact:** Integrity, Availability

Description: The `newdsn.exe` script that comes with IIS allows users to create databases through a web interface. The script does not check the location of the created database. An attacker can use this script to create or overwrite any file with the permissions of the anonymous internet account (`IUSR_machinename`). Although the attacker does not control the contents of the created file, it may provide the leverage needed to compromise security, and can easily be used to compromise the availability of a vulnerable server and the machine it runs on. CGI programs are programs that a web server executes to handle complicated requests and to serve dynamic information. One such program, called "`newdsn.exe`", is distributed with Microsoft Internet Information Server. This program is vulnerable to a problem that allows an attacker to overwrite an arbitrary file on the server. This can potentially be used to compromise access to the server by reconfiguring it, and can easily be exploited to compromise the availability of the server and the machine it runs on.

E26: SSH information obtained

Complexity: Medium

Impact: Confidentiality

Description: The information which can be gathered remotely from an SSH daemon includes:

- o SSH Version
- o Host key size
- o Public key size
- o Authentication methods in use
- o Encryption methods in use

Appendix E : Example of Baseline PCM for case 1

	Bridge Attribute (\$)	Confidentiality					Integrity					Availability					Number of users			Service Function			
		C1	C2	C3	C4	C5	I1	I2	I3	I4	I5	A1	A2	A3	A4	A5	1	5	u	Fe	Fn	Fnt	Fnr
BA	1											A1	A2	A3	A4	A5							
C1		1																					
C2			1																				
C3				1																			
C4					1																		
C5						1																	
I1							1																
I2								1															
I3									1														
I4										1													
I5											1												
A												1											
A2													1										
A3														1									
A4															1								
A5																1							
1																	1						
5																		1					
Unlimited																			1				
Fe																				1			
Fn																					1		
Fnt																						1	
Fnr																							1

Appendix F - Experimental Data

CASE 1 - THEORITICAL OPTIMUM: BA = \$2500

Syn flood check / Network Printer
CANNOT BE FIXED

IIS Showcode.asp vulnerability / Server 3

Web Server

	$\underline{e}$	ei/el	
BA	0.265		
I=m	0.06	0.226415	\$566.04
u=unlimited	0.616	2.324528	\$5,811.32
f=nc	0.06	0.226415	\$566.04
cost			\$100.00

Server 3 OS

	$\underline{e}$	ei/el	
BA	0.833		
I=m	0.167	0.200480	\$501.20
cost			\$100.00
			\$7,644.60

$$M_{ik} = 0.296005 \quad m=1$$

$$P_{ik} = 88.40\%$$

Score **\$6,757.82**

NetBIOS - SMB Accesible Share / Server 2

Office Automation

	$\underline{e}$	ei/el	
BA	0.385		
c=l	0.077	0.2	\$500.00
I=m	0.077	0.2	\$500.00
u=5	0.385	1	\$2,500.00
f=nc	0.077	0.2	\$500.00
cost			\$100.00

Mail

	$\underline{e}$	ei/el	
BA	0.402		
c=l	0.083	0.206467	\$516.17
I=l	0.057	0.141791	\$354.48
u=5	0.402	1	\$2,500.00

$$M_{ik} = 0.30686809 \quad m=1$$

9

f=nth 0.057 0.141791 \$354.48

cost \$100.00
\$7,925.12

P_{ik} = 52.48%

Score \$4,159.11

SYN Flood Check / Server 1

DHCP

	$\underline{e}$	ei/el	
BA	0.75		
A=h	0.25	0.333333	\$833.33
cost			\$100.00

DNS

	$\underline{e}$	ei/el	
BA	0.75		
A=h	0.25	0.333333	\$833.33
cost			\$100.00

Web Server

	$\underline{e}$	ei/el	
BA	0.265		
a=m	0.06	0.226415	\$566.04
u=unlimited	0.616	2.324528	\$5,811.32
f=nc	0.06	0.226415	\$566.04

Office Automation

	$\underline{e}$	ei/el	
BA	0.417		
a=m	0.083	0.199040	\$497.60
u=5	0.417	1	\$2,500.00
fct=n	0.083	0.199040	\$497.60

Mail

	$\underline{e}$	ei/el	
BA	0.437		
a=l	0.063	0.144164	\$360.41
u=5	0.437	1	\$2,500.00
f=nth	0.063	0.144164	\$360.41

Network Printer

	$\underline{e}$	ei/el	
BA	0.427		
A=m	0.087	0.203747	\$509.37
u=5	0.427	1	\$2,500.00
F=Nth	0.06	0.140515	\$351.29
cost			\$100.00

Internet

	$\frac{e}{e}$	$ei/e1$		$M_{ik} =$	$m=h$
BA	0.417			0.87052176	8
a=m	0.083	0.199040	\$497.60		
u=5	0.417	1	\$2,500.00	$P_{ik} =$	72.88%
fct=n	0.083	0.199040	\$497.60		
			\$22,481.95		
Score \$16,384.85					

IP Fragmentation Teardrop-2 Attack / PC1 & PC2**PC OS**

	$\frac{e}{e}$	$ei/e1$	
BA	0.875		
a=l	0.125	0.142857	\$357.14
cost			\$100.00

Web Browser

	$\frac{e}{e}$	$ei/e1$	
BA	0.667		
a=l	0.087	0.130434	\$326.09
u=l	0.087	0.130434	\$326.09
f=nc	0.159	0.238380	\$595.95

PC Outlook

	$\frac{e}{e}$	$ei/e1$		$M_{ik} =$	$m=l$
BA	0.7			0.10751627	4
a=l	0.1	0.142857	\$357.14		
u=l	0.1	0.142857	\$357.14	$P_{ik} =$	86.80%
f=nth	0.1	0.142857	\$357.14		
			\$2,776.70		
Score \$2,410.17					

SNMP Community check / PC3**OC 3 OS**

	$\frac{e}{e}$	$ei/e1$	
BA	0.672		
a=l	0.094	0.139880	\$349.70
f=l	0.094	0.139880	\$349.70
c=l	0.139	0.206845	\$517.11
cost			\$100.00

Web Browser

	$\frac{e}{e}$	$ei/e1$	
BA	0.667		
a=l	0.087	0.130434	\$326.09
u=l	0.087	0.130434	\$326.09

f=nc	0.159	0.238380	\$595.95
------	-------	----------	----------

**PC
Outlook**

	$\frac{e}{e}$	$\frac{ei}{e1}$	
BA	0.7		
a=l	0.1	0.142857	\$357.14
u=l	0.1	0.142857	\$357.14
f=nth	0.1	0.142857	\$357.14
			\$3,636.07

 $M_{ik} = \frac{0.14079206}{3} \quad m=l$
 $P_{ik} = 76.08\%$
Score **\$2,766.32**

Unpassworded NetBios/SMB check PC4

PC4 OS

	$\frac{e}{e}$	$\frac{ei}{e1}$	
BA	0.833		
C=l	0.167	0.200480	\$501.20

 $M_{ik} = \frac{0.01940694}{3} \quad m=l$
 $P_{ik} = 61.44\%$
Score **\$307.94**

SYN Flood Check / Router

**Routing
Service**

	$\frac{e}{e}$	$\frac{ei}{e1}$	
BA	0.75		
A=h	0.25	0.333333	\$833.33
cost			\$100.00

**Firewall
Service**

	$\frac{e}{e}$	$\frac{ei}{e1}$	
BA	0.1		
A=vh	0.9	9	\$22,500.00
cost			100

Internet

	$\frac{e}{e}$	$\frac{ei}{e1}$	
BA	0.408		
a=m	0.075	0.417	\$1,042.50
u=5	0.43	0.083	\$207.50
fct=n	0.087	0.417	\$1,042.50
		0.083	\$25,825.83

 $M_{ik} = \frac{1}{1} \quad m=h$
 $P_{ik} = 88.08\%$
Score **\$22,747.39**

Win NT - RPCSS.EXE Denial of Service / PC5

PC OS

	<u>e</u>	<u>ei/el</u>			
BA	0.875				
a=l	0.125	0.142857	\$357.14		
cost			\$10.00		
Web Browser					
	<u>e</u>	<u>ei/el</u>			
BA	0.667				
a=l	0.087	0.130434	\$326.09		
u=l	0.087	0.130434	\$326.09		
f=nc	0.159	0.238380	\$595.95		
PC Outlook					
	<u>e</u>	<u>ei/el</u>			
BA	0.7			$M_{ik} = 0.10403139$	$m=l$
				1	
a=l	0.1	0.142857	\$357.14		
u=l	0.1	0.142857	\$357.14	$P_{ik} = 61.44\%$	
f=nth	0.1	0.142857	\$357.14		
			\$2,686.70		
			Score	\$1,650.71	

CASE 2 - THEORITICAL OPTIMUM: BA = \$2500**Finger Access control Check / Server 4****Server 4 OS**

	<u>e</u>	<u>ei/el</u>			
BA	0.83			$M_{ik} = 0.009208$	$m=l$
C=l	0.167	0.201204	\$503.01	$P_{ik} = 76.08\%$	
			\$503.01		
			Score	\$382.69	

SMTP banner-check / Server 2**Mail**

	<u>e</u>	<u>ei/el</u>			
BA	0.572			$M_{ik} = 0.034166$	$m=l$
c=l	0.109	0.190559	\$476.40	$P_{ik} = 76.08\%$	
u=3	0.209	0.365384	\$913.46		
f=ne	0.109	0.190559	\$476.40		
			\$1,866.26		
			Score	\$1,419.85	

rstatd check / server 4**Server 4 OS**

	$\underline{e}$	ei/el	
BA	0.83		
C=l	0.167	0.201204	\$503.01
			\$503.01

$M_{ik} =$	0.009208	$m=l$
$P_{ik} =$		76.08%
Score	\$382.69	

Network Time Protocol server present / Server 2**Server 2 OS**

	$\underline{e}$	ei/el	
BA	0.83		
C=l	0.167	0.201204	\$503.01
			\$503.01

$M_{ik} =$	0.009208	$m=l$
$P_{ik} =$		66.44%
Score	\$334.20	

FTP- ports open in sequential order / Server 4**File Transfer services**

	$\underline{e}$	ei/el	
BA	0.527		
c=l	0.103	0.195445	\$488.61
I=m	0.103	0.195445	\$488.61
u=3	0.198	0.375711	\$939.28
f=nth	0.069	0.130929	\$327.32
cost			\$100.00
			\$2,343.83

$M_{ik} =$	0.042909648	$m=l$
$P_{ik} =$		66.44%
Score	\$1,557.24	

FTP file write permission check / Server 4**File Transfer services**

	$\underline{e}$	ei/el	
BA	0.527		
a=m	0.103	0.195445	\$488.61
I=m	0.103	0.195445	\$488.61
u=3	0.198	0.375711	\$939.28
f=nth	0.069	0.130929	\$327.32
cost			\$100.00
			\$2,343.83

$M_{ik} =$	0.042909648	$m=l$
$P_{ik} =$		88.40%
Score	\$2,071.95	

HP Printer Remote print check / Printer**Printer**

	$\underline{e}$	ei/el	
BA	0.608		
a=l	0.081	0.133223	\$333.06
u=3	0.23	0.378289	\$945.72
f=nth	0.081	0.133223	\$333.06
cost			\$50.00

$M_{ik} =$	0.030424121	$m=l$
$P_{ik} =$		76.08%

\$1,661.84

Score **\$1,264.33****Portmapper register-unregister check / Server 4****Server 4 OS**

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.833		
a=m	0.167	0.200480	\$501.20

FTP Service

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.572		
a=m	0.109	0.190559	\$476.40
u=3	0.209	0.365384	\$913.46
f=nc	0.109	0.190559	\$476.40
cost			\$150.00
			\$2,517.46

 $M_{ik} = 0.046088304$ $m=l$ $P_{ik} = 52.48\%$ Score **\$1,321.16****Website Uploader CGI check / server1****Web Server
OS**

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.714		
i=m	0.143	0.200280	\$500.70
a=m	0.143	0.200280	\$500.70
cost			\$100.00

Web Service

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.393		
a=m	0.08	0.203562	\$508.91
i=m	0.08	0.203562	\$508.91
u=unlimited	0.393	1	\$2,500.00
f=nth	0.055	0.139949	\$349.87
cost			\$100.00
			\$5,069.09

 $M_{ik} = 0.092802112$ $m=l$ $P_{ik} = 88.40\%$ Score **\$4,481.07****Rip spoofing check / Router****Routing
Service**

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.053		
i=vh	0.474	8.943396	\$22,358.49
a=vh	0.474	8.943396	\$22,358.49
cost			\$100.00

Internet Service

	$\underline{e}$	ei/el	
BA	0.572		
a=m	0.109	0.190559	\$476.40
u=3	0.209	0.365384	\$913.46
F=Nc	0.109	0.190559	\$476.40

Web Service

	$\underline{e}$	ei/el	
BA	0.417		
a=m	0.083	0.199040	\$497.60
u=unlimited	0.417	1	\$2,500.00
F=Nth	0.083	0.199040	\$497.60

Mail service

	$\underline{e}$	ei/el	
BA	0.572		
a=m	0.109	0.190559	\$476.40
u=3	0.209	0.365384	\$913.46
F=Nc	0.109	0.190559	\$476.40

FTP service

	$\underline{e}$	ci/el	
BA	0.589		
a=m	0.114	0.193548	\$483.87
u=3	0.219	0.371816	\$929.54
F=Nth	0.078	0.132427	\$331.07

DNS

	$\underline{e}$	ei/el	
BA	0.75		
a=h	0.25	0.333333	\$833.33

\$54,622.52

$M_{ik} =$ 1 $m=h$
 $P_{ik} =$ 88.08%

Score **\$48,111.51**

CASE 3 - BA = \$2500**IIS ism.dll**News
Service

	ϵ	ei/el	
BA	0.302		
C=l	0.061	0.201986	\$504.97
I=h	0.117	0.387417	\$968.54
A=m	0.039	0.129139	\$322.85
U=10	0.416	1.377483	\$3,443.71
F=Nec	0.065	0.215231	\$538.08
cost			\$100.00

Web
Service

	ϵ	ei/el	
BA	0.138		
C=m	0.047	0.340579	\$851.45
I=h	0.043	0.311594	\$778.99
A=m	0.033	0.239130	\$597.83
U=i	0.368	2.666666	\$6,666.67
F=cs	0.368	2.666666	\$6,666.67
cost			\$100.00
			\$21,539.74

$$M_{ik} = 0.932444 \quad m=h$$

$$P_{ik} = 88.08\%$$

Score **\$18,972.20****Unpasswor
ded
NetBios/S
MB check
Granit**

Granit OS

	ϵ	ei/el	
BA	0.75		
C=m	0.25	0.333333	\$833.33

$$M_{ik} = 0.036074585 \quad m=l$$

$$P_{ik} = 61.44\%$$

Score **\$512.00****Unpasswor
ded
NetBios/S
MB check
Shale**

Shale OS

	ϵ	ei/el	
BA	0.833		
C=l	0.167	0.200480	\$501.20

$$M_{ik} = 0.021696719 \quad m=l$$

$$P_{ik} = 61.44\%$$

Score **\$307.94**

**MIB-II
UDP table
Granite**

Granit OS

	$\underline{e}$	ei/el		$M_{ik} =$	0.036074585	$m=l$
BA	0.75					
C=m	0.25	0.333333	\$833.33	$P_{ik} =$	76.08%	

Score **\$634.00**

**SYN port
Scanning
Granite
CANNOT
BE FIXED**

**Omni
HTTPD
Imagemap
CGI
Quartz**

Web Server

	$\underline{e}$	ei/el	
BA	0.135		
c=m	0.047	0.348148	\$870.37
I=h	0.047	0.348148	\$870.37
u=i	0.386	2.859259	\$7,148.15
f=e	0.386	2.859259	\$7,148.15
cost			\$100.00

News
Server

	$\underline{e}$	ei/el	
BA	0.315		
c=l	0.064	0.203174	\$507.94
I=h	0.112	0.355555	\$888.89
u=10	0.446	1.415873	\$3,539.68
f=ne	0.064	0.203174	\$507.94
cost			\$100.00

Quartz OS

	$\underline{e}$	ei/el		$M_{ik} =$	1	$m=h$
BA	0.654					
c=m	0.21	0.321100	\$802.75			
I=m	0.135	0.206422	\$516.06			
cost			\$100.00			
			\$23,100.29	$P_{ik} =$	89.04%	

Score **\$20,568.50**

Open
news
server
check
Quartz

Web Server

	$\underline{e}$	ei/el	
BA	0.135		
c=m	0.047	0.348148	\$870.37
l=h	0.047	0.348148	\$870.37
u=i	0.386	2.859259	\$7,148.15
f=e	0.386	2.859259	\$7,148.15
cost			\$100.00

News
Server

	$\underline{e}$	ei/el	
BA	0.315		
c=l	0.064	0.203174	\$507.94
l=h	0.112	0.355555	\$888.89
u=l0	0.446	1.415873	\$3,539.68
f=nc	0.064	0.203174	\$507.94
cost			\$100.00
			\$21,681.48

$$M_{ik} = 0.938580537 \quad m=h$$

$$P_{ik} = 89.04\%$$

Score **\$19,305.19**

SNMPCo
mmunity
check
Shale

Shale OS

	$\underline{e}$	ei/el	
BA	0.654		
c=m	0.21	0.321100	\$802.75
l=m	0.135	0.206422	\$516.06
cost			\$100.00
			\$1,418.81

$$M_{ik} = 0.061419 \quad m=l$$

$$P_{ik} = 83.04\%$$

(Attack
detected
on
Quartz)

Score **\$1,178.18**

IIS
newdsn.exe
Quartz

Web Server

	$\underline{e}$	ei/el	
BA	0.145		
a=m	0.035	0.241379	\$603.45
l=h	0.053	0.365517	\$913.79
u=i	0.384	2.648275	\$6,620.69

f=e	0.384	2.648275	\$6,620.69			
cost			\$100.00			
News Server						
	e	ei/el				
BA	0.319					
a=l	0.041	0.128526	\$321.32			
l=h	0.122	0.382445	\$956.11			
u=10	0.449	1.407523	\$3,518.81			
f=ne	0.069	0.216300	\$540.75			
cost			\$100.00			
Quartz OS						
	e	ei/el				
BA	0.714					
a=m	0.143	0.200280	\$500.70	$M_{ik} =$	0.926265	$m=h$
l=m	0.143	0.200280	\$500.70			
cost			\$100.00		$P_{ik} =$	89.04%
			\$21,397.01			
				Score	\$19,051.90	

SSH info
obtained
Router/fire
wall
CANNOT
BE FIXED

CASE 1 - BA = \$3000

Syn flood CANNOT
BE FIXED

IIS Server
3

Web Server

	e	ei/el	
BA	0.302		
l=m	0.057	0.1887417	\$566.23
u=unlimited	0.585	1.9370860	\$5,811.26
f=ne	0.057	0.1887417	\$566.23
cost			\$100.00

Server 3

OS					
	<u>€</u>	ei/e1			
BA	0.857			M_{ik}	0.3349470 $m=1$
I=m	0.143	0.1668611	\$500.58		
cost			\$100.00		$P_{ik} = 88.40\%$
			\$7,644.29		
				Score	\$6,757.55
NetBIOS					
Serv 2					
Office Automation					
	<u>€</u>	ei/e1			
BA	0.41				
c=l	0.072	0.1756097	\$526.83		
I=m	0.072	0.1756097	\$526.83		
u=5	0.371	0.9048780	\$2,714.63		
f=nc	0.072	0.1756097	\$526.83		
cost			\$100.00		
Mail					
	<u>€</u>	ei/e1			
BA	0.433				
c=l	0.076	0.1755196	\$526.56	$M_{ik} =$	0.368786929 $m=1$
I=l	0.052	0.1200923	\$360.28		
u=5	0.386	0.8914549	\$2,674.36		
f=nth	0.052	0.1200923	\$360.28	$P_{ik} =$	52.48%
cost			\$100.00		
			\$8,416.60		
				Score	\$4,417.03
SYN Flood					
Server 1					
pas changer trop d'ecart pour faire une difference)					
DHCP					
	<u>€</u>	ei/e1			
BA	0.778				
A=h	0.222	0.2853470	\$998.71		
cost			\$100.00		
DNS					
	<u>€</u>	ei/e1			
BA	0.778				
A=h	0.2	0.2570694	\$899.74		
cost			\$100.00		
Web Server					
	<u>€</u>	ei/e1			
BA	0.342				
a=m	0.054	0.1578947	\$552.63		
u=unlimite	0.549	1.6052631	\$5,618.42		
d					

f=nc	0.054	0.1578947	\$552.63
Office Automation			
	e	ei/el	
BA	0.507		
a=m	0.071	0.1400394	\$490.14
u=5	0.35	0.6903353	\$2,416.17
fct=n	0.071	0.1400394	\$490.14
Mail			
	e	ei/el	
BA	0.525		
a=l	0.054	0.1028571	\$360.00
u=5	0.368	0.7009523	\$2,453.33
f=nth	0.054	0.1028571	\$360.00
Network Printer			
	e	ei/el	
BA	0.516		
A=m	0.074	0.1434108	\$501.94
u=5	0.359	0.6957364	\$2,435.08
F=Nth	0.052	0.1007751	\$352.71
cost			\$100.00
Internet			
	e	ei/el	
BA	0.507		
a=m	0.071	0.1400394	\$490.14
u=5	0.35	0.6903353	\$2,416.17
fct=n	0.071	0.1400394	\$490.14
			\$22,178.10
IP Fragmentation PC1 & PC2			
PC OS			
	e	ei/el	
BA	0.895		
a=l	0.105	0.1173184	\$410.61
cost			\$100.00
Web Browser			
	e	ei/el	
BA	0.708		
a=l	0.076	0.1073446	\$322.03
u=l	0.076	0.1073446	\$322.03
f=nc	0.14	0.1977401	\$593.22
PC Outlook			

$$M_{ik} = 0.971769427 \quad m=h$$

$$P_{ik} = 72.88\%$$

Score **\$16,163.40**

SNMP Community check PC3	BA	$\frac{e}{e1}$ 0.739			$M_{ik} =$ 0.123012633 $m=1$
	a=l	0.087	0.1177266	\$353.18	
	u=l	0.087	0.1177266	\$353.18	$P_{ik} =$ 86.80%
	f=nth	0.087	0.1177266	\$353.18	
				\$2,807.44	Score \$2,436.86
OC 3 OS					
Web Browser	BA	$\frac{e}{e1}$ 0.713			
	a=l	0.083	0.1164095	\$349.23	
	l=l	0.083	0.1164095	\$349.23	
	c=l	0.122	0.1711079	\$513.32	
	cost			\$100.00	
PC Outlook	BA	$\frac{e}{e1}$ 0.708			
	a=l	0.076	0.1073446	\$322.03	
	u=l	0.076	0.1073446	\$322.03	
	f=nc	0.14	0.1977401	\$593.22	
Unpassworded NetBios/SMB check PC4	BA	$\frac{e}{e1}$ 0.739			$M_{ik} =$ 0.158117045 $m=1$
	a=l	0.087	0.1177266	\$353.18	
	u=l	0.087	0.1177266	\$353.18	$P_{ik} =$ 76.08%
	f=nth	0.087	0.1177266	\$353.18	
				\$3,608.61	Score \$2,745.43
PC4 OS					
SYN flood check router	BA	$\frac{e}{e1}$ 0.857			0.021933872 $m=1$
	C=l	0.143	0.1668611	\$500.58	$P_{ik} =$ 61.44%
Routing Service					
Routing Service	BA	$\frac{e}{e1}$ 0.778			
					Score \$307.56

A=h	0.222	0.2853470	\$856.04		
cost			\$100.00		
Firewall					
Service					
	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$			
BA	0.143				
A=vh	0.857	5.9930069	\$17,979.02		
cost			100		
Internet					
	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$			
BA	0.442				
a=m	0.077	0.1742081	\$522.62	$M_{ik} =$	1 m=h
u=5	0.404	0.9140271	\$2,742.08		
fct=n	0.077	0.1742081	\$522.62	$P_{ik} =$	88.08%
			\$22,822.39		
				Score	\$20,101.96
Win NT					
DoS PC5					
PC OS					
	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$			
BA	0.895				
a=l	0.105	0.1173184	\$351.96		
cost			\$10.00		
Web					
Browser					
	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$			
BA	0.708				
a=l	0.076	0.1073446	\$322.03		
u=l	0.076	0.1073446	\$322.03		
f=nc	0.14	0.1977401	\$593.22		
PC Outlook					
	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$			
BA	0.739			$M_{ik} =$	0.116498889 m=l
a=l	0.087	0.1177266	\$353.18		
u=l	0.087	0.1177266	\$353.18		61.44%
f=nth	0.087	0.1177266	\$353.18		
			\$2,658.78	Score	\$1,633.56

CASE 3 - THEORITICAL OPTIMUM : BA = \$3000

IIS ism.dll

News
Service

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.354		
C=l	0.058	0.163841	\$491.53

I=h	0.111	0.313559	\$940.68
A=m	0.037	0.104519	\$313.56
U=10	0.379	1.070621	\$3,211.86
F=Nec	0.061	0.172316	\$516.95
cost			\$100.00

Web
Service

	$\frac{e}{e_i}$	$\frac{e_i}{e_1}$	
BA	0.16		
C=m	0.046	0.2875	\$862.50
I=h	0.046	0.2875	\$862.50
A=m	0.032	0.2	\$600.00
U=i	0.358	2.2375	\$6,712.50
F=es	0.358	2.2375	\$6,712.50
cost			\$100.00
			\$21,424.58

$$M_{ik} = 0.792712 \quad m=h$$

$$P_{ik} = 88.08\%$$

Score **\$18,870.77**

Unpasswor
ded
NetBios/S
MB check
Granit

Granit OS

	$\frac{e}{e_i}$	$\frac{e_i}{e_1}$	
BA	0.778		
C=m	0.222	0.285347	\$856.04

$$M_{ik} = 0.031673632 \quad m=l$$

$$P_{ik} = 61.44\%$$

Score **\$525.95**

Unpasswor
ded
NetBios/S
MB check
Shale

Shale OS

	$\frac{e}{e_i}$	$\frac{e_i}{e_1}$	
BA	0.857		
C=l	0.143	0.166861	\$500.58

$$M_{ik} = 0.018521651 \quad m=l$$

$$P_{ik} = 61.44\%$$

Score **\$307.56**

MIB-II
UDP table
Granite

Granit OS

	$\frac{e}{e_i}$	$\frac{e_i}{e_1}$	
BA	0.778		

$$M_{ik} = 0.031673632 \quad m=l$$

C=m 0.222 0.285347 \$856.04

$P_{ik} = 76.08\%$

Score \$651.28

SYN port
Scanning
Granite

CANNOT Be
FIXED

Omni
HTTPD
Imagemap
CGI
Quartz

Web Server

	$\underline{e}$	ei/el	
BA	0.133		
c=m	0.045	0.338345	\$1,015.04
I=h	0.045	0.338345	\$1,015.04
u=i	0.389	2.924812	\$8,774.44
f=c	0.389	2.924812	\$8,774.44
cost			\$100.00

News
Server

	$\underline{e}$	ei/el	
BA	0.341		
c=l	0.06	0.175953	\$527.86
I=h	0.105	0.307917	\$923.75
u=10	0.435	1.275659	\$3,826.98
f=ne	0.06	0.175953	\$527.86
cost			\$100.00

Quartz OS

	$\underline{e}$	ei/el	
BA	0.691		
c=m	0.189	0.273516	\$820.55
I=m	0.12	0.173661	\$520.98
cost			\$100.00
			\$27,026.93

$M_{ik} = 1 \quad m=h$

$P_{ik} = 89.04\%$

Score \$24,064.78

Open
news
server
check
Quartz

Web Server

	$\underline{e}$	ei/el	
BA	0.133		
c=m	0.045	0.338345	\$1,015.04
I=h	0.045	0.338345	\$1,015.04

u=i	0.389	2.924812	\$8,774.44
f=e	0.389	2.924812	\$8,774.44
cost			\$100.00

News
Server

	$\underline{e}$	ei/el	
BA	0.341		
c=l	0.06	0.175953	\$527.86
I=h	0.105	0.307917	\$923.75
u=10	0.435	1.275659	\$3,826.98
f=nc	0.06	0.175953	\$527.86
cost			\$100.00
			\$25,585.40

$M_{ik} = 0.946663056$ m=h

$P_{ik} = 89.04\%$

Score **\$22,781.24**

SNMPCo
mmunity
check
Shale

Shale OS

	$\underline{e}$	ei/el	
BA	0.691		
c=m	0.189	0.273516	\$820.55
I=m	0.12	0.173661	\$520.98
cost			\$100.00

$M_{ik} = 0.053336$ m=l

(Attack
detected on
Quartz) $P_{ik} = 83.04\%$

\$1,441.53

Score **\$1,197.05**

IIS
newdsn.exe
Quartz

Web Server

	$\underline{e}$	ei/el	
BA	0.168		
a=m	0.034	0.202380	\$607.14
I=h	0.052	0.309523	\$928.57
u=i	0.373	2.220238	\$6,660.71
f=e	0.373	2.220238	\$6,660.71
cost			\$100.00

News
Server

	$\underline{e}$	ei/el	
BA	0.356		
a=l	0.039	0.109550	\$328.65
I=h	0.125	0.351123	\$1,053.37
u=10	0.414	1.162921	\$3,488.76
f=ne	0.066	0.185393	\$556.18
cost			\$100.00

Quartz OS

	$\underline{e}$	ei/el	
BA	0.75		
a=m	0.125	0.166666	\$500.00
I=m	0.125	0.166666	\$500.00
cost			\$100.00
			\$21,584.11

$$M_{ik} = 0.798614 \quad m=h$$

$$P_{ik} = 89.04\%$$

Score **\$19,218.49**

SSH info
obtained
Router/fire
wall

CANNOT
BE FIXED

CASE 1 - BA = \$3500

Syn flood CANNOT
BE FIXED

IIS Server
3

Web Server

	$\underline{e}$	ei/el	
BA	0.342		
I=m	0.054	0.157894	\$552.63
u=unlimited	0.549	1.605263	\$5,618.42
f=ne	0.054	0.157894	\$552.63
cost			\$100.00

Server 3
OS

	$\underline{e}$	ei/el	
BA	0.875		
I=m	0.125	0.142857	\$500.00
cost			\$100.00
			\$7,423.68

$$M_{ik} = 0.256241 \quad m=l$$

$$P_{ik} = 88.40\%$$

Score **\$6,562.54**NetBIOS
Serv 2Office
Automation

	$\underline{e}$	ei/el	
BA	0.472		
c=l	0.067	0.141949	\$496.82
I=m	0.067	0.141949	\$496.82
u=5	0.328	0.694915	\$2,432.20
f=nc	0.067	0.141949	\$496.82

cost			\$100.00			
Mail						
	ϵ	ei/e1				
BA	0.487					
c=l	0.071	0.145790	\$510.27			
l=l	0.049	0.100616	\$352.16			
u=5	0.343	0.704312	\$2,465.09	$M_{ik} =$	0.269311375	m=l
f=nth	0.049	0.100616	\$352.16			
cost			\$100.00	$P_{ik} =$	52.48%	
			\$7,802.34			
SYN Flood Server 1				Score	\$4,094.67	
DHCP						
	ϵ	ei/e1				
BA	0.8					
A=h	0.2	0.25	\$875.00			
cost			\$100.00			
DNS						
	ϵ	ei/e1				
BA	0.8					
A=h	0.2	0.25	\$875.00			
cost			\$100.00			
Web Server						
	ϵ	ei/e1				
BA	0.342					
a=m	0.054	0.157894	\$552.63			
u=unlimited	0.549	1.605263	\$5,618.42			
f=nc	0.054	0.157894	\$552.63			
Office Automation						
	ϵ	ei/e1				
BA	0.507					
a=m	0.071	0.140039	\$490.14			
u=5	0.35	0.690335	\$2,416.17			
fct=n	0.071	0.140039	\$490.14			
Mail						
	ϵ	ei/e1				
BA	0.525					
a=l	0.054	0.102857	\$360.00			
u=5	0.368	0.700952	\$2,453.33			
f=nth	0.054	0.102857	\$360.00			
Network Printer						
	ϵ	ei/e1				
BA	0.516					
A=m	0.074	0.143410	\$501.94			
u=5	0.359	0.695736	\$2,435.08			

F=Nth	0.052	0.100775	\$352.71			
cost			\$100.00			
Internet						
	<u>e</u>	ei/el				
BA	0.507			M _{ik} =	0.760391553	m=h
a=m	0.071	0.140039	\$490.14			
u=5	0.35	0.690335	\$2,416.17	P _{ik} =	72.88%	
fc=n	0.071	0.140039	\$490.14			
			\$22,029.65	Score	\$16,055.21	
IP Fragmenta tion PC1 & PC2						
PC OS						
	<u>e</u>	ei/el				
BA	0.905					
a=l	0.095	0.104972	\$367.40			
cost			\$100.00			
Web Browser						
	<u>e</u>	ei/el				
BA	0.733					
a=l	0.07	0.095497	\$334.24			
u=l	0.07	0.095497	\$334.24			
f=nc	0.127	0.173260	\$606.41			
PC Outlook						
	<u>e</u>	ei/el				
BA	0.76			M _{ik} =	0.098288632	m=l
a=l	0.08	0.105263	\$368.42			
u=l	0.08	0.105263	\$368.42	P _{ik} =	86.80%	
f=nth	0.08	0.105263	\$368.42			
			\$2,847.56	Score	\$2,471.69	
SNMP Communit y check PC3						
OC 3 OS						
	<u>e</u>	ei/el				
BA	0.738					
a=l	0.076	0.102981	\$360.43			
I=l	0.076	0.102981	\$360.43			
c=l	0.111	0.150406	\$526.42			
cost			\$100.00			
Web Browser						
	<u>e</u>	ei/el				

BA	0.733		
a=l	0.07	0.095497	\$334.24
u=l	0.07	0.095497	\$334.24
f=nc	0.127	0.173260	\$606.41

PC Outlook

	e	ei/e1	
BA	0.76		
a=l	0.08	0.105263	\$368.42
u=l	0.08	0.105263	\$368.42
f=nth	0.08	0.105263	\$368.42
			\$3,727.45

$$M_{ik} = 0.128659451 \quad m=l$$

$$P_{ik} = 76.08\%$$

Score **\$2,835.84**Unpassworded
NetBios/SMB
check PC4

PC4 OS

	e	ei/e1	
BA	0.875		
C=l	0.125	0.142857	\$500.00

$$M_{ik} = 0.01725837 \quad m=l$$

$$P_{ik} = 61.44\%$$

Score **\$307.20**SYN flood
check
routerRouting
Service

	e	ei/e1	
BA	0.8		
A=h	0.2	0.25	\$875.00
cost			\$100.00

Firewall
Service

	e	ei/e1	
BA	0.125		
A=vh	0.875	7	\$24,500.00
cost			100

Internet

	e	ei/e1	
BA	0.507		
a=m	0.071	0.140039	\$490.14
u=5	0.35	0.690335	\$2,416.17
fct=n	0.071	0.140039	\$490.14
			\$28,971.45

$$M_{ik} = 1 \quad m=h$$

$$P_{ik} = 88.08\%$$

Score **\$25,518.05**Win NT
DoS PC5

PC OS				
	<u>e</u>	ei/el		
BA	0.905			
a=l	0.095	0.104972	\$367.40	
cost			\$10.00	
Web Browser				
	<u>e</u>	ei/el		
BA	0.733			
a=l	0.07	0.095497	\$334.24	
u=l	0.07	0.095497	\$334.24	
f=nc	0.127	0.173260	\$606.41	
PC Outlook				
	<u>e</u>	ei/el		
BA	0.76			
a=l	0.08	0.105263	\$368.42	$M_{ik=}$ 0.095182125 m=l
u=l	0.08	0.105263	\$368.42	$P_{ik=}$ 61.44%
F=nth	0.08	0.105263	\$368.42	
			\$2,757.56	
			Score	\$1,694.25

CASE 2 - BA = \$3500**Finger Access control****Server 4 OS**

	<u>e</u>	ei/el		
BA	0.875			
C=l	0.125	0.142857	\$500.00	$M_{ik=}$ 0.009153 m=l
			\$500.00	$P_{ik=}$ 76.08%
			Score	\$380.40

SMTP banner-check**Mail**

	<u>e</u>	ei/el		
BA	0.648			
c=l	0.089	0.137345	\$480.71	$M_{ik=}$ 0.034707 m=l
u=3	0.173	0.266975	\$934.41	$P_{ik=}$ 76.08%
f=ne	0.089	0.137345	\$480.71	
			\$1,895.83	
			Score	\$1,442.35

rstatd

**check
server 4**Server 4
OS

	$\underline{e}$	ei/el	
BA	0.875		
C=l	0.125	0.142857	\$500.00
			\$500.00

$M_{ik} = 0.009153$ $m=l$
 $P_{ik} = 76.08\%$
 Score **\$380.40**

**Network
Time
Protocol**Server 2
OS

	$\underline{e}$	ei/el	
BA	0.875		
C=l	0.125	0.142857	\$500.00
			\$500.00

$M_{ik} = 0.009153$ $m=l$
 $P_{ik} = 66.44\%$
 Score **\$332.20**

**FTP-ports
open in
sequential
order**File
Transfer
services

	$\underline{e}$	ei/el	
BA	0.604		
c=l	0.086	0.142384	\$498.34
I=m	0.086	0.142384	\$498.34
u=3	0.167	0.276490	\$967.72
f=nth	0.058	0.096026	\$336.09
cost			\$100.00
			\$2,400.50

$M_{ik} = 0.043947016$ $m=l$
 $P_{ik} = 66.44\%$

Score **\$1,594.89****FTP file
write
permission
check**File
Transfer
services

	$\underline{e}$	ei/el	
BA	0.604		
a=m	0.086	0.142384	\$498.34
I=m	0.086	0.142384	\$498.34
u=3	0.167	0.276490	\$967.72
f=nth	0.058	0.096026	\$336.09

$M_{ik} = 0.043947016$ $m=l$

cost \$100.00
\$2,400.50

PIK = 88.40%

Score **\$2,122.04**

HP Printer Remote print check

Printer

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.676		
a=l	0.067	0.099112	\$346.89
u=3	0.19	0.281065	\$983.73
f=nth	0.067	0.099112	\$346.89
cost			\$50.00
			\$1,727.51

$M_{ik} = 0.031626422$ m=l

$P_{ik} = 76.08\%$

Score **\$1,314.29**

Portmappe r register

Server 4

OS

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.875		
a=m	0.125	0.142857	\$500.00

FTP

Service

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.648		
a=m	0.089	0.137345	\$480.71
u=3	0.173	0.266975	\$934.41
f=nc	0.089	0.137345	\$480.71
cost			\$150.00
			\$2,545.83

$M_{ik} = 0.046607762$ m=l

$P_{ik} = 52.48\%$

Score **\$1,336.05**

Website Uploader CGI check server1

Web

Server OS

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.778		
i=m	0.111	0.142673	\$499.36
a=m	0.111	0.142673	\$499.36
cost			\$100.00

Web

Service	$\underline{e}$	e_i/e_l			
BA	0.413				
a=m	0.069	0.167070	\$584.75		
l=m	0.069	0.167070	\$584.75		
u=unlimited	0.403	0.975786	\$3,415.25	$M_{ik=}$	0.113172474 m=l
d					
f=nth	0.047	0.113801	\$398.31		
cost			\$100.00	$P_{ik} =$	88.40%
			\$6,181.77		

Score **\$5,464.68**

Rip spoofing check

No need to calculate the scores since the interval between the scores are too big

CASE 3 - BA = \$3500**IIS ism.dll**

News Service

	$\underline{e}$	e_i/e_l	
BA	0.378		
C=l	0.055	0.145502	\$509.26
l=h	0.106	0.280423	\$981.48
A=m	0.035	0.092592	\$324.07
U=10	0.368	0.973544	\$3,407.41
F=Nec	0.058	0.153439	\$537.04
cost			\$100.00

Web Service

	$\underline{e}$	e_i/e_l	
BA	0.185		
C=m	0.045	0.243243	\$851.35
l=h	0.045	0.243243	\$851.35
A=m	0.032	0.172972	\$605.41
U=i	0.347	1.875675	\$6,564.86
F=es	0.347	1.875675	\$6,564.86
cost			\$100.00
			\$21,397.10

 $M_{ik=}$ 0.939571 m=h $P_{ik} =$ 88.08%Score **\$18,846.56**

IIS newdsn.exe

Quartz**Web Server**

	$\underline{e}$	ei/el	
BA	0.196		
a=m	0.033	0.168367	\$589.29
l=h	0.051	0.260204	\$910.71
u=i	0.36	1.836734	\$6,428.57
f=e	0.36	1.836734	\$6,428.57
cost			\$100.00

News Server

	$\underline{e}$	ei/el	
BA	0.396		
a=l	0.037	0.093434	\$327.02
l=h	0.11	0.277777	\$972.22
u=10	0.395	0.997474	\$3,491.16
f=ne	0.062	0.156565	\$547.98
cost			\$100.00

Quartz OS

	$\underline{e}$	ei/el	
BA	0.778		
a=m	0.111	0.142673	\$499.36
l=m	0.111	0.142673	\$499.36
cost			\$100.00
			\$20,994.24

$$M_{ik} = 0.921882 \quad m=h$$

$$P_{ik} = 89.04\%$$

Score **\$18,693.27****CASE 3 – Exp 1 : Accuracy Against Pairwise Comparison errors (1 error) : BA = \$3000****IIS
newdsn.exe
Quartz****Web Server**

	$\underline{e}$	ei/el	
BA	0.168		
a=m	0.034	0.202380	\$607.14
l=h	0.052	0.309523	\$928.57
u=i	0.373	2.220238	\$6,660.71
f=e	0.373	2.220238	\$6,660.71
cost			\$100.00

News Server

	$\underline{e}$	ei/el	
BA	0.356		
a=l	0.039	0.109550	\$328.65
l=h	0.125	0.351123	\$1,053.37
u=10	0.414	1.162921	\$3,488.76
f=ne	0.066	0.185393	\$556.18

cost			\$100.00			
Quartz OS						
	$\bar{e}$	ei/el				
BA	0.709					
a=m	0.179	0.252468	\$757.40	$M_{ik} =$	0.807329	m=h
l=m	0.113	0.159379	\$478.14			
cost			\$100.00	$P_{ik} =$	89.04%	
IR=0.05			\$21,819.65			
				Score	\$19,428.22	

CASE 3 – Exp 1 : Accuracy Against Pairwise Comparison errors (2 errors) : BA = \$3000

IIS ism.dll

**News
Service**

	$\bar{e}$	ei/el	
BA	0.354		
C=l	0.058	0.163841	\$491.53
l=h	0.111	0.313559	\$940.68
A=m	0.037	0.104519	\$313.56
U=10	0.379	1.070621	\$3,211.86
F=Nec	0.061	0.172316	\$516.95
cost			\$100.00

**Web
Service**

	$\bar{e}$	ei/el	
BA	0.139		
C=m	0.048	0.345323	\$1,035.97
l=h	0.047	0.338129	\$1,014.39
A=m	0.034	0.244604	\$733.81
U=i	0.37	2.661870	\$7,985.61
F=es	0.362	2.604316	\$7,812.95
cost			\$100.00
IR=0.0			\$24,257.31

$$M_{ik} = 0.903907 \quad m=h$$

$$P_{ik} = 88.08\%$$

Score **\$21,365.84**

**Omni
HTTPD
Imagemap
CGI
Quartz**

Web Server

	$\bar{e}$	ei/el	
BA	0.134		
c=m	0.046	0.343283	\$1,029.85
l=h	0.045	0.335820	\$1,007.46
u=i	0.392	2.925373	\$8,776.12

f=e	0.383	2.858208	\$8,574.63			
cost			\$100.00			
IR=0.01						
News Server						
	ϵ	ei/el				
BA	0.341					
c=l	0.06	0.175953	\$527.86			
l=h	0.105	0.307917	\$923.75			
u=10	0.435	1.275659	\$3,826.98			
f=ne	0.06	0.175953	\$527.86			
cost			\$100.00			
Quartz OS						
	ϵ	ei/el				
BA	0.691					
c=m	0.189	0.273516	\$820.55	$M_{ik} =$	l	m=h
l=m	0.12	0.173661	\$520.98			
cost			\$100.00		$P_{ik} =$	89.04%
			\$26,836.05			
				Score	\$23,894.81	

CASE 3 – Exp 1 : Accuracy Against Pairwise Comparison errors (3 errors) : BA = \$3000**IIS ism.dll**

News Service						
	ϵ	ei/el				
BA	0.354					
C=l	0.058	0.163841	\$491.53			
l=h	0.111	0.313559	\$940.68			
A=m	0.037	0.104519	\$313.56			
U=10	0.379	1.070621	\$3,211.86			
F=Nec	0.061	0.172316	\$516.95			
cost			\$100.00			
Web Service						
	ϵ	ei/el				
BA	0.14					
C=m	0.047	0.335714	\$1,007.14	$M_{ik} =$	0.909342	m=h
l=h	0.047	0.335714	\$1,007.14			
A=m	0.036	0.257142	\$771.43			
U=i	0.372	2.657142	\$7,971.43			
F=es	0.372	2.657142	\$7,971.43		$P_{ik} =$	88.08%
cost			\$100.00			
	IR=0.01		\$24,403.15			
				Score	\$21,494.29	

CASE 3 – Exp 1 : Accuracy Against Pairwise Comparison errors (4 errors) : BA = \$3000**IIS ism.dll**News
Service

	ϵ	ei/el	
BA	0.301		
C=l	0.061	0.202657	\$607.97
I=h	0.116	0.385382	\$1,156.15
A=m	0.037	0.122923	\$368.77
U=10	0.414	1.375415	\$4,126.25
F=Nec	0.07	0.232558	\$697.67
cost			\$100.00

IR=0.02Web
Service

	ϵ	ei/el	
BA	0.14		
C=m	0.047	0.335714	\$1,007.14
I=h	0.047	0.335714	\$1,007.14
A=m	0.036	0.257142	\$771.43
U=i	0.372	2.657142	\$7,971.43
F=cs	0.372	2.657142	\$7,971.43
cost			\$100.00
			\$25,885.38

 $M_{ik} = 0.964575 \quad m=h$ $P_{ik} = 88.08\%$ Score **\$22,799.84****IIS
newdsn.exe
Quartz**

Web Server

	ϵ	ei/el	
BA	0.168		
a=m	0.034	0.202380	\$607.14
I=h	0.052	0.309523	\$928.57
u=i	0.373	2.220238	\$6,660.71
f=e	0.373	2.220238	\$6,660.71
cost			\$100.00

News
Server

	ϵ	ei/el	
BA	0.317		
a=l	0.038	0.119873	\$359.62
I=h	0.121	0.381703	\$1,145.11
u=10	0.447	1.410094	\$4,230.28
f=nc	0.076	0.239747	\$719.24
cost			\$100.00

IR= 0.03

Quartz OS

	$\underline{e}$	ei/el			
BA	0.709				
a=m	0.179	0.252468	\$757.40	$M_{ik} =$	0.851352
I=m	0.113	0.159379	\$478.14		$m=h$
cost			\$100.00	$P_{ik} =$	89.04%
			\$22,846.94		
				Score	\$20,342.92

CASE 3 – Exp 1 : Accuracy Against Pairwise Comparison errors (5 errors) : BA = \$3000

IIS ism.dll

News
Service

	$\underline{e}$	ei/el	
BA	0.301		
C=l	0.061	0.202657	\$607.97
I=h	0.116	0.385382	\$1,156.15
A=m	0.037	0.122923	\$368.77
U=10	0.414	1.375415	\$4,126.25
F=Nec	0.07	0.232558	\$697.67
cost			\$100.00

Web
Service

	$\underline{e}$	ei/el	
BA	0.132		
C=m	0.049	0.371212	\$1,113.64
I=h	0.047	0.356060	\$1,068.18
A=m	0.036	0.272727	\$818.18
U=i	0.372	2.818181	\$8,454.55
F=es	0.363	2.75	\$8,250.00
cost			\$100.00
IR=0.02			\$26,861.36

$M_{ik} =$	0.928979	$m=h$
$P_{ik} =$		88.08%

Score **\$23,659.48**Unpassworded
NetBios/S
MB check
Granit

Granit OS

	$\underline{e}$	ei/el	
BA	0.667		
C=m	0.333	0.49925	\$1497.75
IR=0			

$M_{ik} =$	0.029605527	$m=l$
$P_{ik} =$		61.44%

Score **\$920.22**

**MIB-II
UDP table
Granite**

Granit OS

	$\frac{e}{e}$	$\frac{ei}{ei}$	
BA	0.667		
C=m	0.333	0.499250	\$1,497.75

 $M_{ik} = 0.051798576$ $m=l$ $P_{ik} = 76.08\%$ Score **\$1,139.49**

**Omni
HTTPD
Imagemap
CGI
Quartz**

Web Server

	$\frac{e}{e}$	$\frac{ei}{ei}$	
BA	0.126		
c=m	0.05	0.396825	\$1,190.48
l=h	0.046	0.365079	\$1,095.24
u=i	0.394	3.126984	\$9,380.95
f=e	0.385	3.055555	\$9,166.67
cost			\$100.00

IR=0.01

News
Server

	$\frac{e}{e}$	$\frac{ei}{ei}$	
BA	0.341		
c=l	0.06	0.175953	\$527.86
l=h	0.105	0.307917	\$923.75
u=10	0.435	1.275659	\$3,826.98
f=ne	0.06	0.175953	\$527.86
cost			\$100.00

Quartz OS

	$\frac{e}{e}$	$\frac{ei}{ei}$	
BA	0.603		
c=m	0.254	0.421227	\$1,263.68
l=m	0.143	0.237147	\$711.44
cost			\$100.00
			\$28,914.91

 $M_{ik} = 1$ $m=h$ $P_{ik} = 89.04\%$ Score **\$25,745.84**

**Open
news
server
check
Quartz**

Web Server

	$\bar{e}$	ei/el	
BA	0.126		
c=m	0.05	0.396825	\$1,190.48
I=h	0.046	0.365079	\$1,095.24
u=i	0.394	3.126984	\$9,380.95
f=e	0.385	3.055555	\$9,166.67
cost			\$100.00

IR=0.01

News
Server

	$\bar{e}$	ei/el	
BA	0.341		
c=l	0.06	0.175953	\$527.86
I=h	0.105	0.307917	\$923.75
u=10	0.435	1.275659	\$3,826.98
f=nc	0.06	0.175953	\$527.86
cost			\$100.00
			\$26,839.78

 $M_{ik} = 0.928233412$ m=h $P_{ik} = 89.04\%$ Score **\$23,898.14****CASE 3 – Exp 1 : Accuracy Against Pairwise Comparison errors (6 errors) : BA = \$3000**

IIS ism.dll

News
Service

	$\bar{e}$	ei/el	
BA	0.303		
C=l	0.062	0.204620	\$613.86
I=h	0.104	0.343234	\$1,029.70
A=m	0.037	0.122112	\$366.34
U=10	0.414	1.366336	\$4,099.01
F=Nec	0.079	0.260726	\$782.18
cost			\$100.00

IR=0.02

Web
Service

	$\bar{e}$	ei/el	
BA	0.132		
C=m	0.049	0.371212	\$1,113.64
I=h	0.047	0.356060	\$1,068.18
A=m	0.036	0.272727	\$818.18
U=i	0.372	2.818181	\$8,454.55
F=es	0.363	2.75	\$8,250.00
cost			\$100.00
			\$26,795.63

 $M_{ik} = 0.928893$ m=h $P_{ik} = 88.08\%$ Score **\$23,601.59**

**Omni
HTTPD
Imagemap
CGI
Quartz**

Web Server

	$\underline{e}$	ei/el	
BA	0.126		
c=m	0.05	0.396825	\$1,190.48
l=h	0.046	0.365079	\$1,095.24
u=i	0.394	3.126984	\$9,380.95
f=e	0.385	3.055555	\$9,166.67
cost			\$100.00

News
Server

	$\underline{e}$	ei/el	
BA	0.344		
c=l	0.061	0.177325	\$531.98
l=h	0.093	0.270348	\$811.05
u=10	0.434	1.261627	\$3,784.88
f=ne	0.07	0.203488	\$610.47
cost			\$100.00

IR=0.02

Quartz OS

	$\underline{e}$	ei/el	
BA	0.603		
c=m	0.254	0.421227	\$1,263.68
l=m	0.143	0.237147	\$711.44
cost			\$100.00
			\$28,846.83

$$M_{ik} = \frac{1}{m} = h$$

$$P_{ik} = 89.04\%$$

Score **\$25,685.22**

**Open
news
server
check
Quartz**

Web Server

	$\underline{e}$	ei/el	
BA	0.126		
c=m	0.05	0.396825	\$1,190.48
l=h	0.046	0.365079	\$1,095.24
u=i	0.394	3.126984	\$9,380.95
f=e	0.385	3.055555	\$9,166.67
cost			\$100.00

News
Server

	$\underline{e}$	ei/el
BA	0.344	

c=l	0.061	0.177325	\$531.98
l=h	0.093	0.270348	\$811.05
u=10	0.434	1.261627	\$3,784.88
f=nc	0.07	0.203488	\$610.47
cost			\$100.00
IR=0.02			\$26,771.71

 $M_{ik} = 0.928064041 \quad m=h$
 $P_{ik} = 89.04\%$
Score **\$23,837.53**

IIS
newdsn.exe
Quartz

Web Server

	$\underline{e}$	ei/el	
BA	0.168		
a=m	0.034	0.202380	\$607.14
l=h	0.052	0.309523	\$928.57
u=i	0.373	2.220238	\$6,660.71
f=e	0.373	2.220238	\$6,660.71
cost			\$100.00

News
Server

	$\underline{e}$	ei/el	
BA	0.321		
a=l	0.038	0.118380	\$355.14
l=h	0.106	0.330218	\$990.65
u=10	0.447	1.392523	\$4,177.57
f=ne	0.087	0.271028	\$813.08
cost			\$100.00

IR=0.03

Quartz OS

	$\underline{e}$	ei/el	
BA	0.709		
a=m	0.179	0.252468	\$757.40
l=m	0.113	0.159379	\$478.14
cost			\$100.00
			\$22,729.13

 $M_{ik} = 0.787924 \quad m=h$
 $P_{ik} = 89.04\%$
Score **\$20,238.02****CASE 3 – Exp 1 : Accuracy Against Pairwise Comparison errors (7 errors) : BA = \$3000**

IIS ism.dll

News
Service

	$\underline{e}$	ei/el	
BA	0.306		
C=l	0.065	0.212418	\$637.25
l=h	0.105	0.343137	\$1,029.41

A=m	0.037	0.120915	\$362.75
U=10	0.407	1.330065	\$3,990.20
F=Nec	0.08	0.261437	\$784.31
cost			\$100.00

IR=0.02

Web
Service

	e	ei/el	
BA	0.132		
C=m	0.049	0.371212	\$1,113.64
I=h	0.047	0.356060	\$1,068.18
A=m	0.036	0.272727	\$818.18
U=i	0.372	2.818181	\$8,454.55
F=es	0.363	2.75	\$8,250.00
cost			\$100.00
			\$26,708.47

$$M_{ik} = 0.928861 \quad m=h$$

$$P_{ik} = 88.08\%$$

Score \$23,524.82Omni
HTTPD
Imagemap
CGI
Quartz

Web Server

	e	ei/el	
BA	0.126		
c=m	0.05	0.396825	\$1,190.48
I=h	0.046	0.365079	\$1,095.24
u=i	0.394	3.126984	\$9,380.95
f=e	0.385	3.055555	\$9,166.67
cost			\$100.00

News
Server

	e	ei/el	
BA	0.347		
c=l	0.064	0.184438	\$553.31
I=h	0.094	0.270893	\$812.68
u=10	0.425	1.224783	\$3,674.35
f=ne	0.07	0.201729	\$605.19
cost			\$100.00

IR=0.02

Quartz OS

	e	ei/el	
BA	0.603		
c=m	0.254	0.421227	\$1,263.68
I=m	0.143	0.237147	\$711.44
cost			\$100.00
			\$28,753.99

$$M_{ik} = 1 \quad m=h$$

$$P_{ik} = 89.04\%$$

Score \$25,602.55Open
news

**server
check
Quartz**

Web Server

	$\underline{e}$	ei/el	
BA	0.126		
c=m	0.05	0.396825	\$1,190.48
I=h	0.046	0.365079	\$1,095.24
u=i	0.394	3.126984	\$9,380.95
f=e	0.385	3.055555	\$9,166.67
cost			\$100.00

News
Server

	$\underline{e}$	ei/el	
BA	0.347		
c=l	0.064	0.184438	\$553.31
I=h	0.094	0.270893	\$812.68
u=10	0.425	1.224783	\$3,674.35
f=nc	0.07	0.201729	\$605.19
cost			\$100.00
IR=0.02			\$26,678.87

$$M_{ik} = 0.927831779 \quad m=h$$

$$P_{ik} = 89.04\%$$

Score **\$23,754.86**

CASE 3 – Exp 1 : Accuracy Against Pairwise Comparison errors (8 errors) : BA = \$3000

IIS ism.dll

News
Service

	$\underline{e}$	ei/el	
BA	0.279		
C=l	0.063	0.225806	\$677.42
I=h	0.103	0.369175	\$1,107.53
A=m	0.036	0.129032	\$387.10
U=10	0.441	1.580645	\$4,741.94
F=Nec	0.078	0.279569	\$838.71
cost			\$100.00
IR=0.03			

Web
Service

	$\underline{e}$	ei/el	
BA	0.132		
C=m	0.049	0.371212	\$1,113.64
I=h	0.047	0.356060	\$1,068.18
A=m	0.036	0.272727	\$818.18
U=i	0.372	2.818181	\$8,454.55
F=es	0.363	2.75	\$8,250.00
cost			\$100.00

$$M_{ik} = 0.928836 \quad m=h$$

$$P_{ik} = 88.08\%$$

\$27,657.23

Score **\$24,360.49**

Omni
HTTPD
Imagemap
CGI
Quartz

Web Server

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.126		
c=m	0.05	0.396825	\$1,190.48
l=h	0.046	0.365079	\$1,095.24
u=i	0.394	3.126984	\$9,380.95
f=e	0.385	3.055555	\$9,166.67
cost			\$100.00

News
Server

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.31		
c=l	0.062	0.2	\$600.00
l=h	0.09	0.290322	\$870.97
u=l0	0.469	1.512903	\$4,538.71
f=ne	0.068	0.219354	\$658.06
cost			\$100.00

IR=0.03

Quartz OS

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.603		
c=m	0.254	0.421227	\$1,263.68
l=m	0.143	0.237147	\$711.44
cost			\$100.00
			\$29,776.20

M_{ik}= l m=hP_{ik} = 89.04%Score **\$26,512.73**

Open
news
server
check
Quartz

Web Server

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.126		
c=m	0.05	0.396825	\$1,190.48
l=h	0.046	0.365079	\$1,095.24
u=i	0.394	3.126984	\$9,380.95
f=e	0.385	3.055555	\$9,166.67
cost			\$100.00

News

Server				
	<u>e</u>	ei/el		
BA	0.31			
c=l	0.062	0.2	\$600.00	
l=h	0.09	0.290322	\$870.97	
u=10	0.469	1.512903	\$4,538.71	$M_{ik} = 0.930309294$ $m=h$
f=nc	0.068	0.219354	\$658.06	
cost			\$100.00	$P_{ik} = 89.04\%$
IR=0.03			\$27,701.08	
			Score	\$24,665.04
IIS newdsm.exe Quartz				
Web Server				
	<u>e</u>	ei/el		
BA	0.168			
a=m	0.034	0.202380	\$607.14	
l=h	0.052	0.309523	\$928.57	
u=i	0.373	2.220238	\$6,660.71	
f=e	0.373	2.220238	\$6,660.71	
cost			\$100.00	
News Server				
	<u>e</u>	ei/el		
BA	0.286			
a=l	0.037	0.129370	\$388.11	
l=h	0.103	0.360139	\$1,080.42	
u=10	0.489	1.709790	\$5,129.37	
f=nc	0.085	0.297202	\$891.61	
cost			\$100.00	
IR=0.04				
Quartz OS				
	<u>e</u>	ei/el		
BA	0.709			
a=m	0.179	0.252468	\$757.40	$M_{ik} = 0.802056$ $m=h$
l=m	0.113	0.159379	\$478.14	
cost			\$100.00	$P_{ik} = 89.04\%$
			\$23,882.20	
			Score	\$21,264.71

CASE 3 – Exp 1 : Accuracy Against Pairwise Comparison errors (9 errors) : BA = \$3000

IIS ism.dll

News
Servicee ei/el

BA	0.279		
C=l	0.063	0.225806	\$677.42
I=h	0.103	0.369175	\$1,107.53
A=m	0.036	0.129032	\$387.10
U=10	0.441	1.580645	\$4,741.94
F=Nec	0.078	0.279569	\$838.71
cost			\$100.00

Web Service

	$\underline{e}$	$ei/e1$	
BA	0.131		
C=m	0.049	0.374045	\$1,122.14
I=h	0.046	0.351145	\$1,053.44
A=m	0.036	0.274809	\$824.43
U=i	0.377	2.877862	\$8,633.59
F=es	0.361	2.755725	\$8,267.18
cost			\$100.00
			\$27,853.45

IR=0.01

$$M_{ik} = 0.930219 \quad m=h$$

$$P_{ik} = 88.08\%$$

Score **\$24,533.32**

Omni HTTPD Imagemap CGI Quartz

Web Server

	$\underline{e}$	$ei/e1$	
BA	0.125		
c=m	0.049	0.392	\$1,176.00
I=h	0.044	0.352	\$1,056.00
u=i	0.4	3.2	\$9,600.00
f=e	0.382	3.056	\$9,168.00
cost			\$100.00

IR=0.01

News Server

	$\underline{e}$	$ei/e1$	
BA	0.31		
c=l	0.062	0.2	\$600.00
I=h	0.09	0.290322	\$870.97
u=10	0.469	1.512903	\$4,538.71
f=ne	0.068	0.219354	\$658.06
cost			\$100.00

Quartz OS

	$\underline{e}$	$ei/e1$	
BA	0.603		
c=m	0.254	0.421227	\$1,263.68
I=m	0.143	0.237147	\$711.44
cost			\$100.00
			\$29,942.87

$$M_{ik} = 1 \quad m=h$$

$$P_{ik} = 89.04\%$$

Score **\$26,661.13**

Open
news
server
check
Quartz

Web Server

	ϵ	$ei/e1$	
BA	0.125		
c=m	0.049	0.392	\$1,176.00
l=h	0.044	0.352	\$1,056.00
u=i	0.4	3.2	\$9,600.00
f=e	0.382	3.056	\$9,168.00
cost			\$100.00

IR=0.01

News
Server

	ϵ	$ei/e1$	
BA	0.31		
c=l	0.062	0.2	\$600.00
l=h	0.09	0.290322	\$870.97
u=10	0.469	1.512903	\$4,538.71
f=nc	0.068	0.219354	\$658.06
cost			\$100.00
			\$27,867.74

 $M_{ik} = 0.930697203$ m=h $P_{ik} = 89.04\%$ Score **\$24,813.44**

IIS
newdsn.exe
Quartz

Web Server

	ϵ	$ei/e1$	
BA	0.144		
a=m	0.035	0.243055	\$729.17
l=h	0.051	0.354166	\$1,062.50
u=i	0.39	2.708333	\$8,125.00
f=e	0.38	2.638888	\$7,916.67
cost			\$100.00

IR=0.01

News
Server

	ϵ	$ei/e1$	
BA	0.286		
a=l	0.037	0.129370	\$388.11
l=h	0.103	0.360139	\$1,080.42
u=10	0.489	1.709790	\$5,129.37
f=ne	0.085	0.297202	\$891.61
cost			\$100.00

Quartz OS

	ϵ	$ei/e1$
BA	0.709	

a=m	0.179	0.252468	\$757.40	$M_{ik} =$	0.896987	m=h
I=m	0.113	0.159379	\$478.14			
cost			\$100.00		$P_{ik} =$	89.04%
			\$26,858.39			
				Score	\$23,914.71	

CASE 3 – Exp 1 : Accuracy Against Pairwise Comparison errors (10 errors) : BA = \$3000**IIS ism.dll**News
Service

	ϵ	ei/e1	
BA	0.289		
C=l	0.065	0.224913	\$674.74
I=h	0.104	0.359861	\$1,079.58
A=m	0.039	0.134948	\$404.84
U=10	0.431	1.491349	\$4,474.05
F=Nec	0.072	0.249134	\$747.40
cost	0.289		\$100.00

IR=0.03Web
Service

	ϵ	ei/e1	
BA	0.131		
C=m	0.049	0.374045	\$1,122.14
I=h	0.046	0.351145	\$1,053.44
A=m	0.036	0.274809	\$824.43
U=i	0.377	2.877862	\$8,633.59
F=es	0.361	2.755725	\$8,267.18
cost			\$100.00
			\$27,481.39

 $M_{ik} =$ 0.924384 m=h $P_{ik} =$ 88.08%Score **\$24,205.60****Unpassworded
NetBios/SMB check
Shale**

Shale OS

	ϵ	ei/e1	
BA	0.857		
C=l	0.143	0.166861	\$500.58

IR=0 $M_{ik} =$ 0.016838003 m=l $P_{ik} =$ 61.44%Score **\$307.56****Omni
HTTTPD**

**Imagemap
CGI
Quartz**

Web Server

	<u>e</u>	ei/el	
BA	0.125		
c=m	0.049	0.392	\$1,176.00
l=h	0.044	0.352	\$1,056.00
u=i	0.4	3.2	\$9,600.00
f=e	0.382	3.056	\$9,168.00
cost			\$100.00

**News
Server**

	<u>e</u>	ei/el	
BA	0.317		
c=l	0.06	0.189274	\$567.82
l=h	0.089	0.280757	\$842.27
u=10	0.466	1.470031	\$4,410.09
f=ne	0.067	0.211356	\$634.07
cost			\$100.00

IR=0.04

Quartz OS

	<u>e</u>	ei/el	
BA	0.603		
c=m	0.254	0.421227	\$1,263.68
l=m	0.143	0.237147	\$711.44
cost			\$100.00
			\$29,729.38

$$M_{ik} = \frac{l}{m} = \frac{1}{89.04\%}$$

Score **\$26,471.04**

**Open
news
server
check
Quartz**

Web Server

	<u>e</u>	ei/el	
BA	0.125		
c=m	0.049	0.392	\$1,176.00
l=h	0.044	0.352	\$1,056.00
u=i	0.4	3.2	\$9,600.00
f=e	0.382	3.056	\$9,168.00
cost			\$100.00

**News
Server**

	<u>e</u>	ei/el	
BA	0.317		
c=l	0.06	0.189274	\$567.82
l=h	0.089	0.280757	\$842.27

u=10	0.466	1.470031	\$4,410.09	$M_{ik} =$	0.930199548	$m=h$
f=nc	0.067	0.211356	\$634.07			
cost			\$100.00	$P_{ik} =$	89.04%	
IR=0.04			\$27,654.26			

Score \$24,623.35

CASE 3- Exp 2-1 hop: Accuracy Against Pairwise Comparison errors (1 error): BA = \$3000

Omni
HTTPD
Imagemap
CGI
Quartz

Web Server

	$\bar{e}$	ei/el	
BA	0.134		
c=m	0.046	0.343283	\$1,029.85
l=h	0.045	0.335820	\$1,007.46
u=i	0.392	2.925373	\$8,776.12
f=e	0.383	2.858208	\$8,574.63
cost			\$100.00

IR=0

News
Server

	$\bar{e}$	ei/el	
BA	0.341		
c=l	0.06	0.175953	\$527.86
l=h	0.105	0.307917	\$923.75
u=10	0.435	1.275659	\$3,826.98
f=nc	0.06	0.175953	\$527.86
cost			\$100.00

Quartz OS

	$\bar{e}$	ei/el	
BA	0.63		
c=m	0.218	0.346031	\$1,038.10
l=m	0.151	0.239682	\$719.05
cost			\$100.00
			\$27,251.65

 $M_{ik} = 1$ $m=h$ $P_{ik} = 89.04\%$

Score \$24,264.87

Open
news
server
check
Quartz

Web Server

	$\bar{e}$	ei/el	
BA	0.134		
c=m	0.046	0.343283	\$1,029.85
l=h	0.045	0.335820	\$1,007.46

u=i	0.392	2.925373	\$8,776.12
f=e	0.383	2.858208	\$8,574.63
cost			\$100.00

IR=0

News
Server

	<u>e</u>	ei/el	
BA	0.341		
c=l	0.06	0.175953	\$527.86
l=h	0.105	0.307917	\$923.75
u=10	0.435	1.275659	\$3,826.98
f=nc	0.06	0.175953	\$527.86
cost			\$100.00
			\$25,394.51

M_{ik}= 0.931852105 m=hP_{ik}= 89.04%Score \$22,611.27IIS
newdsn.exe
Quartz

Web Server

	<u>e</u>	ei/el	
BA	0.168		
a=m	0.034	0.202380	\$607.14
l=h	0.052	0.309523	\$928.57
u=u	0.373	2.220238	\$6,660.71
f=e	0.373	2.220238	\$6,660.71
cost			\$100.00

News
Server

	<u>e</u>	ei/el	
BA	0.356		
a=l	0.039	0.109550	\$328.65
l=h	0.125	0.351123	\$1,053.37
u=10	0.414	1.162921	\$3,488.76
f=ne	0.066	0.185393	\$556.18
cost			\$100.00

Quartz OS

	<u>e</u>	ei/el	
BA	0.691		
a=m	0.149	0.215629	\$646.89
l=m	0.16	0.231548	\$694.65
cost			\$100.00
			\$21,925.64

IR=0.01

M_{ik}= 0.804561 m=hP_{ik}= 89.04%Score \$19,522.59**CASE 3— Exp 2-1 hop: Accuracy Against Pairwise Comparison errors (2 errors): BA = \$3000**

IIS ism.dllNews
Service

	ϵ	ei/el	
BA	0.309		
C=l	0.059	0.190938	\$572.82
I=h	0.116	0.375404	\$1,126.21
A=m	0.039	0.126213	\$378.64
U=10	0.413	1.336569	\$4,009.71
F=Nec	0.064	0.207119	\$621.36
cost			\$100.00

IR=0Web
Service

	ϵ	ei/el	
BA	0.16		
C=m	0.046	0.2875	\$862.50
I=h	0.046	0.2875	\$862.50
A=m	0.032	0.2	\$600.00
U=i	0.358	2.2375	\$6,712.50
F=es	0.358	2.2375	\$6,712.50
cost			\$100.00
			\$22,658.74

 $M_{ik} = 0.831306$ $m=h$ $P_{ik} = 88.08\%$ Score **\$19,957.82****Unpassworded
NetBios/SMB check
Shale**

Shale OS

	ϵ	ei/el	
BA	0.857		
C=l	0.143	0.166861	\$500.58

IR=0 $M_{ik} = 0.018365465$ $m=l$ $P_{ik} = 61.44\%$ Score **\$307.56****Omni
HTTPD
Imagemap
CGI
Quartz**

Web Server

	ϵ	ei/el	
BA	0.133		
c=m	0.045	0.338345	\$1,015.04
I=h	0.045	0.338345	\$1,015.04
u=i	0.389	2.924812	\$8,774.44
f=e	0.389	2.924812	\$8,774.44
cost			\$100.00

News
Server

	$\underline{e}$	ei/el	
BA	0.348		
c=l	0.058	0.166666	\$500.00
l=h	0.104	0.298850	\$896.55
u=10	0.431	1.238505	\$3,715.52
f=ne	0.059	0.169540	\$508.62
cost			\$100.00

IR=0.01

Quartz OS

	$\underline{e}$	ei/el	
BA	0.63		
c=m	0.218	0.346031	\$1,038.10
l=m	0.151	0.239682	\$719.05
cost			\$100.00
			\$27,256.78

 $M_{ik} = 1$ $m=h$ $P_{ik} = 89.04\%$ Score **\$24,269.44**Open
news
server
check
Quartz

Web Server

	$\underline{e}$	ei/el	
BA	0.133		
c=m	0.045	0.338345	\$1,015.04
l=h	0.045	0.338345	\$1,015.04
u=i	0.389	2.924812	\$8,774.44
f=e	0.389	2.924812	\$8,774.44
cost			\$100.00

News
Server

	$\underline{e}$	ei/el	
BA	0.348		
c=l	0.058	0.166666	\$500.00
l=h	0.104	0.298850	\$896.55
u=10	0.431	1.238505	\$3,715.52
f=nc	0.059	0.169540	\$508.62
cost			\$100.00

IR=0.01

\$25,399.64

 $M_{ik} = 0.931864921$ $m=h$ $P_{ik} = 89.04\%$ Score **\$22,615.84****CASE 3- Exp 2-1 hop: Accuracy Against Pairwise Comparison errors (3 errors): BA = \$3000**

IIS ism.dllNews
Service

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.309		
C=l	0.059	0.190938	\$572.82
I=h	0.116	0.375404	\$1,126.21
A=m	0.039	0.126213	\$378.64
U=10	0.413	1.336569	\$4,009.71
F=Nec	0.064	0.207119	\$621.36
cost			\$100.00

Web
Service

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.15		
C=m	0.047	0.313333	\$940.00
I=h	0.047	0.313333	\$940.00
A=m	0.034	0.226666	\$680.00
U=i	0.373	2.486666	\$7,460.00
F=cs	0.349	2.326666	\$6,980.00
cost			\$100.00
			\$23,908.74

IR=0 $M_{ik} = 0.937953$ $m=h$ $P_{ik} = 88.08\%$ Score **\$21,058.82**

Shale OS

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.857		
C=l	0.143	0.166861	\$500.58

 0.019638168 $m=l$ $P_{ik} = 61.44\%$ Score **\$307.56****Omni
HTTPD
Imagemap
CGI
Quartz**

Web Server

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.144		
c=m	0.045	0.3125	\$937.50
I=h	0.045	0.3125	\$937.50
u=i	0.397	2.756944	\$8,270.83
f=e	0.368	2.555555	\$7,666.67
cost			\$100.00

IR=0News
Server

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$
BA	0.348	

c=l	0.058	0.166666	\$500.00
l=h	0.104	0.298850	\$896.55
u=10	0.431	1.238505	\$3,715.52
f=ne	0.059	0.169540	\$508.62
cost			\$100.00

Quartz OS

	e	ei/el	
BA	0.63		
c=m	0.218	0.346031	\$1,038.10
l=m	0.151	0.239682	\$719.05
cost			\$100.00
			\$25,490.33

 $M_{ik} =$ l $m=h$
 $P_{ik} =$ 89.04%

Score \$22,696.59

Open
news
server
check
Quartz

Web Server

	e	ei/el	
BA	0.144		
c=m	0.045	0.3125	\$937.50
l=h	0.045	0.3125	\$937.50
u=i	0.397	2.756944	\$8,270.83
f=e	0.368	2.555555	\$7,666.67
cost			\$100.00

IR=0

News
Server

	e	ei/el	
BA	0.348		
c=l	0.058	0.166666	\$500.00
l=h	0.104	0.298850	\$896.55
u=10	0.431	1.238505	\$3,715.52
f=nc	0.059	0.169540	\$508.62
cost			\$100.00
			\$23,633.19

 $M_{ik} =$ 0.927143247 $m=h$
 $P_{ik} =$ 89.04%

Score \$21,042.99

IIS
newdsn.exe
Quartz

Web Server

	e	ei/el	
BA	0.16		
a=m	0.035	0.21875	\$656.25
l=h	0.054	0.3375	\$1,012.50
u=i	0.391	2.44375	\$7,331.25

f=e	0.36	2.25	\$6,750.00			
cost			\$100.00			
IR=0.01						
News						
Server						
	$\frac{e}{e_1}$	$\frac{e_i}{e_1}$				
BA	0.356					
a=l	0.039	0.109550	\$328.65			
I=h	0.125	0.351123	\$1,053.37			
u=10	0.414	1.162921	\$3,488.76			
f=ne	0.066	0.185393	\$556.18			
cost			\$100.00			
Quartz OS						
	$\frac{e}{e_1}$	$\frac{e_i}{e_1}$				
BA	0.691					
a=m	0.149	0.215629	\$646.89	$M_{ik}=$	0.895182	m=h
I=m	0.16	0.231548	\$694.65			
cost			\$100.00		$P_{ik}=$	89.04%
			\$22,818.50			
				Score	\$20,317.59	

CASE 3- Exp 2-1 hop: Accuracy Against Pairwise Comparison errors (4 errors): BA = \$3000**IIS ism.dll**

News						
Service						
	$\frac{e}{e_1}$	$\frac{e_i}{e_1}$				
BA	0.309					
C=l	0.059	0.190938	\$572.82			
I=h	0.116	0.375404	\$1,126.21			
A=m	0.039	0.126213	\$378.64			
U=10	0.413	1.336569	\$4,009.71			
F=Nec	0.064	0.207119	\$621.36			
cost			\$100.00			
Web						
Service						
	$\frac{e}{e_1}$	$\frac{e_i}{e_1}$				
BA	0.156					
C=m	0.045	0.288461	\$865.38	$M_{ik}=$	0.950693	m=h
I=h	0.047	0.301282	\$903.85			
A=m	0.033	0.211538	\$634.62			
U=i	0.372	2.384615	\$7,153.85			
F=es	0.346	2.217948	\$6,653.85		$P_{ik}=$	88.08%
cost			\$100.00			
			\$23,120.28			
IR=0.01				Score	\$20,364.34	

Unpassworded
NetBios/SMB check
Granit

Granit OS

	ϵ	ei/el
BA	0.8	
C=m	0.2	0.25

\$750.00

M_{ik}= 0.030839596 m=lP_{ik}= 61.44%

IR=0

Score \$460.80

MIB-II
UDP table
Granite

Granit OS

	ϵ	ei/el
BA	0.8	
C=m	0.2	0.25

\$750.00

M_{ik}= 0.030839596 m=lP_{ik}= 76.08%

IR=0

Score \$570.60

Omni
HTTPD
Imagemap
CGI
Quartz

Web Server

	ϵ	ei/el
BA	0.151	
c=m	0.043	0.284768
I=h	0.045	0.298013
u=i	0.396	2.622516
f=e	0.366	2.423841
cost		

\$854.30

\$894.04

\$7,867.55

\$7,271.52

\$100.00

IR=0.01

News
Server

	ϵ	ei/el
BA	0.348	
c=l	0.058	0.166666
I=h	0.104	0.298850
u=10	0.431	1.238505
f=ne	0.059	0.169540
cost		

\$500.00

\$896.55

\$3,715.52

\$508.62

\$100.00

Quartz OS

	ϵ	ei/el
--	------------	-------

BA	0.665		
c=m	0.19	0.285714	\$857.14
l=m	0.145	0.218045	\$654.14
cost			\$100.00
			\$24,319.39

$M_{ik} =$	1	$m=h$
$P_{ik} =$		89.04%

Score **\$21,653.98**

Open
news
server
check
Quartz

Web Server

	$\underline{e}$	ei/el	
BA	0.151		
c=m	0.043	0.284768	\$854.30
l=h	0.045	0.298013	\$894.04
u=i	0.396	2.622516	\$7,867.55
f=c	0.366	2.423841	\$7,271.52
cost			\$100.00

IR=0.01

News
Server

	$\underline{e}$	ei/el	
BA	0.348		
c=l	0.058	0.166666	\$500.00
l=h	0.104	0.298850	\$896.55
u=10	0.431	1.238505	\$3,715.52
f=nc	0.059	0.169540	\$508.62
cost			\$100.00
			\$22,708.11

 $M_{ik} = 0.933745109$ $m=h$ $P_{ik} = 89.04\%$ Score **\$20,219.30**

SNMPCo
mmunity
check
Shale

Shale OS

	$\underline{e}$	ei/el	
BA	0.665		
c=m	0.19	0.285714	\$857.14
l=m	0.145	0.218045	\$654.14
cost			\$100.00

IR=0.02

\$1,611.28

 $M_{ik} = 0.066254$ $m=l$

(Attack
detected on
Quartz)

$P_{ik} = 83.04\%$

Score **\$1,338.01**

CASE 3- Exp 2-1 hop: Accuracy Against Pairwise Comparison errors (5 errors): BA = \$3000**IIS ism.dll**News
Service

	ϵ	e_i/e_l	
BA	0.309		
C=l	0.059	0.190938	\$572.82
I=h	0.116	0.375404	\$1,126.21
A=m	0.039	0.126213	\$378.64
U=10	0.413	1.336569	\$4,009.71
F=Nec	0.064	0.207119	\$621.36
cost			\$100.00

Web
Service

	ϵ	e_i/e_l	
BA	0.169		
C=m	0.046	0.272189	\$816.57
I=h	0.048	0.284023	\$852.07
A=m	0.034	0.201183	\$603.55
U=i	0.352	2.082840	\$6,248.52
F=es	0.352	2.082840	\$6,248.52
cost			\$100.00
IR=0			\$21,677.97

 $M_{ik} = 0.950018$ $m=h$ $P_{ik} = 88.08\%$ Score **\$19,093.95****Omni
HTTPD
Imagemap
CGI
Quartz**

Web Server

	ϵ	e_i/e_l	
BA	0.163		
c=m	0.044	0.269938	\$809.82
I=h	0.046	0.282208	\$846.63
u=i	0.373	2.288343	\$6,865.03
f=e	0.373	2.288343	\$6,865.03
cost			\$100.00
IR=0			

News
Server

	ϵ	e_i/e_l	
BA	0.348		
c=l	0.058	0.166666	\$500.00
I=h	0.104	0.298850	\$896.55
u=10	0.431	1.238505	\$3,715.52
f=ne	0.059	0.169540	\$508.62
cost			\$100.00

Quartz OS

	$\underline{e}$	ei/el	
BA	0.665		
c=m	0.19	0.285714	\$857.14
l=m	0.145	0.218045	\$654.14
cost			\$100.00
			\$22,818.47

$$M_{ik} = \frac{l}{m=h} = \frac{P_{ik}}{89.04\%}$$

Score **\$20,317.57**Open
news
server
check
Quartz

Web Server

	$\underline{e}$	ei/el	
BA	0.163		
c=m	0.044	0.269938	\$809.82
l=h	0.046	0.282208	\$846.63
u=i	0.373	2.288343	\$6,865.03
f=e	0.373	2.288343	\$6,865.03
cost			\$100.00

IR=0

News
Server

	$\underline{e}$	ei/el	
BA	0.348		
c=l	0.058	0.166666	\$500.00
l=h	0.104	0.298850	\$896.55
u=10	0.431	1.238505	\$3,715.52
f=nc	0.059	0.169540	\$508.62
cost			\$100.00
			\$21,207.19

$$M_{ik} = \frac{0.929387109}{m=h} = \frac{P_{ik}}{89.04\%}$$

Score **\$18,882.88**IIS
newdsn.exe
Quartz

Web Server

	$\underline{e}$	ei/el	
BA	0.176		
a=m	0.036	0.204545	\$613.64
l=h	0.055	0.3125	\$937.50
u=i	0.367	2.085227	\$6,255.68
f=e	0.367	2.085227	\$6,255.68
cost			\$100.00

IR=0.01

News
Server

	$\underline{e}$	ei/el
BA	0.356	

a=l	0.039	0.109550	\$328.65
I=h	0.125	0.351123	\$1,053.37
u=10	0.414	1.162921	\$3,488.76
f=ne	0.066	0.185393	\$556.18
cost			\$100.00

Quartz OS

	e	ei/el	
BA	0.691		
a=m	0.149	0.215629	\$646.89
I=m	0.16	0.231548	\$694.65
cost			\$100.00
			\$21,131.00

$$M_{ik} = 0.926048 \quad m=h$$

$$P_{ik} = 89.04\%$$

$$\text{Score} = \$18,815.04$$

CASE 3- Exp 2-1 hop: Accuracy Against Pairwise Comparison errors (6 errors): BA = \$3000

IIS ism.dll

News
Service

	e	ei/el	
BA	0.312		
C=l	0.062	0.198717	\$596.15
I=h	0.117	0.375	\$1,125.00
A=m	0.039	0.125	\$375.00
U=10	0.405	1.298076	\$3,894.23
F=Nec	0.064	0.205128	\$615.38
cost			\$100.00

$$IR=0.01$$

Web
Service

	e	ei/el	
BA	0.169		
C=m	0.046	0.272189	\$816.57
I=h	0.048	0.284023	\$852.07
A=m	0.034	0.201183	\$603.55
U=i	0.352	2.082840	\$6,248.52
F=es	0.352	2.082840	\$6,248.52
cost			\$100.00
			\$21,575.00

$$M_{ik} = 0.950236 \quad m=h$$

$$P_{ik} = 88.08\%$$

$$\text{Score} = \$19,003.26$$

Omni
HTTPD
Imagemap
CGI
Quartz

Web Server

	$\underline{e}$	ei/el	
BA	0.163		
c=m	0.044	0.269938	\$809.82
l=h	0.046	0.282208	\$846.63
u=i	0.373	2.288343	\$6,865.03
f=e	0.373	2.288343	\$6,865.03
cost			\$100.00

News
Server

	$\underline{e}$	ei/el	
BA	0.353		
c=l	0.061	0.172804	\$518.41
l=h	0.105	0.297450	\$892.35
u=10	0.422	1.195467	\$3,586.40
f=ne	0.06	0.169971	\$509.92
cost			\$100.00

IR=0.01

Quartz OS

	$\underline{e}$	ei/el	
BA	0.665		
c=m	0.19	0.285714	\$857.14
l=m	0.145	0.218045	\$654.14
cost			\$100.00
			\$22,704.86

 $M_{ik} = 1$ $m=h$ $P_{ik} = 89.04\%$ Score \$20,216.41Open
news
server
check
Quartz

Web Server

	$\underline{e}$	ei/el	
BA	0.163		
c=m	0.044	0.269938	\$809.82
l=h	0.046	0.282208	\$846.63
u=i	0.373	2.288343	\$6,865.03
f=e	0.373	2.288343	\$6,865.03
cost			\$100.00

News
Server

	$\underline{e}$	ei/el	
BA	0.353		
c=l	0.061	0.172804	\$518.41
l=h	0.105	0.297450	\$892.35
u=10	0.422	1.195467	\$3,586.40
f=nc	0.06	0.169971	\$509.92
cost			\$100.00

 $M_{ik} = 0.929033786$ $m=h$ $P_{ik} = 89.04\%$

IR=0.01

\$21,093.59

Score **\$18,781.73****CASE 3- Exp 2-1 hop: Accuracy Against Pairwise Comparison errors (7 errors): BA = \$3000****IIS ism.dll****News
Service**

	$\frac{e}{e_l}$	$\frac{e_i}{e_l}$	
BA	0.312		
C=l	0.062	0.198717	\$596.15
I=h	0.117	0.375	\$1,125.00
A=m	0.039	0.125	\$375.00
U=10	0.405	1.298076	\$3,894.23
F=Nec	0.064	0.205128	\$615.38
cost			\$100.00

**Web
Service**

	$\frac{e}{e_l}$	$\frac{e_i}{e_l}$	
BA	0.17		
C=m	0.047	0.276470	\$829.41
I=h	0.048	0.282352	\$847.06
A=m	0.034	0.2	\$600.00
U=i	0.354	2.082352	\$6,247.06
F=es	0.346	2.035294	\$6,105.88
cost			\$100.00
IR=0			\$21,435.18

 $M_{ik} = 0.953437$ $m=h$ $P_{ik} = 88.08\%$ Score **\$18,880.11****Omni
HTTPD
Imagemap
CGI
Quartz****Web Server**

	$\frac{e}{e_l}$	$\frac{e_i}{e_l}$	
BA	0.165		
c=m	0.045	0.272727	\$818.18
I=h	0.046	0.278787	\$836.36
u=i	0.376	2.278787	\$6,836.36
f=e	0.367	2.224242	\$6,672.73
cost			\$100.00

IR=0**News
Server**

	$\frac{e}{e_l}$	$\frac{e_i}{e_l}$	
BA	0.353		
c=l	0.061	0.172804	\$518.41
I=h	0.105	0.297450	\$892.35

u=10	0.422	1.195467	\$3,586.40
f=nc	0.06	0.169971	\$509.92
cost			\$100.00

Quartz OS

	$\frac{e}{e}$	$\frac{ei}{e1}$	
BA	0.665		
c=m	0.19	0.285714	\$857.14
l=m	0.145	0.218045	\$654.14
cost			\$100.00
			\$22,482.00

$$M_{ik} = \frac{l}{m=h}$$

$$P_{ik} = 89.04\%$$

Score **\$20,017.97**

Open
news
server
check
Quartz

Web Server

	$\frac{e}{e}$	$\frac{ei}{e1}$	
BA	0.165		
c=m	0.045	0.272727	\$818.18
l=h	0.046	0.278787	\$836.36
u=i	0.376	2.278787	\$6,836.36
f=c	0.367	2.224242	\$6,672.73
cost			\$100.00

IR=0

News
Server

	$\frac{e}{e}$	$\frac{ei}{e1}$	
BA	0.353		
c=l	0.061	0.172804	\$518.41
l=h	0.105	0.297450	\$892.35
u=10	0.422	1.195467	\$3,586.40
f=nc	0.06	0.169971	\$509.92
cost			\$100.00
			\$20,870.72

$$M_{ik} = \frac{0.92833029}{m=h}$$

$$P_{ik} = 89.04\%$$

Score **\$18,583.29****CASE 3- Exp 2-1 hop: Accuracy Against Pairwise Comparison errors (8 errors): BA = \$3000**

IIS ism.dll

News
Service

	$\frac{e}{e}$	$\frac{ei}{e1}$	
BA	0.312		
C=l	0.062	0.198717	\$596.15

I=h	0.117	0.375	\$1,125.00
A=m	0.039	0.125	\$375.00
U=10	0.405	1.298076	\$3,894.23
F=Nec	0.064	0.205128	\$615.38
cost			\$100.00

Web
Service

	e	ei/el	
BA	0.171		
C=m	0.047	0.274853	\$824.56
I=h	0.049	0.286549	\$859.65
A=m	0.035	0.204678	\$614.04
U=j	0.356	2.081871	\$6,245.61
F=es	0.342	2	\$6,000.00
cost			\$100.00
IR=0.01			\$21,349.63

$$M_{ik} = 0.949632 \quad m=h$$

$$P_{ik} = 88.08\%$$

Score **\$18,804.75**

IIS
newdsn.exe
Quartz

Web Server

	e	ei/el	
BA	0.177		
a=m	0.037	0.209039	\$627.12
I=h	0.055	0.310734	\$932.20
u=i	0.369	2.084745	\$6,254.24
f=e	0.362	2.045197	\$6,135.59
cost			\$100.00
IR=0.01			

News
Server

	e	ei/el	
BA	0.356		
a=l	0.039	0.109550	\$328.65
I=h	0.125	0.351123	\$1,053.37
u=10	0.414	1.162921	\$3,488.76
f=ne	0.066	0.185393	\$556.18
cost			\$100.00

Quartz OS

	e	ei/el	
BA	0.691		
a=m	0.149	0.215629	\$646.89
I=m	0.16	0.231548	\$694.65
cost			\$100.00
			\$21,017.65

$$M_{ik} = 0.934865 \quad m=h$$

$$P_{ik} = 89.04\%$$

Score **\$18,714.12**

CASE 3- Exp 2-1 hop: Accuracy Against Pairwise Comparison errors (9 errors): BA = \$3000

IIS ism.dllNews
Service

	$\underline{e}$	ei/el	
BA	0.311		
C=l	0.062	0.199356	\$598.07
I=h	0.116	0.372990	\$1,118.97
A=m	0.037	0.118971	\$356.91
U=10	0.404	1.299035	\$3,897.11
F=Nec	0.07	0.225080	\$675.24
cost			\$100.00

IR=0.02Web
Service

	$\underline{e}$	ei/el	
BA	0.171		
C=m	0.047	0.274853	\$824.56
I=h	0.049	0.286549	\$859.65
A=m	0.035	0.204678	\$614.04
U=i	0.356	2.081871	\$6,245.61
F=es	0.342	2	\$6,000.00
cost			\$100.00
			\$21,390.16

 $M_{ik} = 0.951435 \quad m=h$ $P_{ik} = 88.08\%$ Score **\$18,840.45****IIS
newdsn.exe
Quartz**

Web Server

	$\underline{e}$	ei/el	
BA	0.177		
a=m	0.037	0.209039	\$627.12
I=h	0.055	0.310734	\$932.20
u=i	0.369	2.084745	\$6,254.24
f=e	0.362	2.045197	\$6,135.59
cost			\$100.00

News
Server

	$\underline{e}$	ei/el	
BA	0.319		
a=l	0.047	0.147335	\$442.01
I=h	0.124	0.388714	\$1,166.14
u=10	0.449	1.407523	\$4,222.57
f=ne	0.061	0.191222	\$573.67
cost			\$100.00

IR=0.02

Quartz OS

	$\underline{e}$	ei/el	
BA	0.691		
a=m	0.149	0.215629	\$646.89
I=m	0.16	0.231548	\$694.65

 $M_{ik} = 0.978341 \quad m=h$

cost \$100.00
\$21,995.08

$P_{ik} = 89.04\%$

Score \$19,584.42

CASE 3- Exp 2-1 hop: Accuracy Against Pairwise Comparison errors (10 errors): BA = \$3000

IIS ism.dll

News
Service

	ϵ	ei/el	
BA	0.316		
C=l	0.061	0.193037	\$579.11
I=h	0.115	0.363924	\$1,091.77
A=m	0.036	0.113924	\$341.77
U=10	0.402	1.272151	\$3,816.46
F=Nec	0.07	0.221518	\$664.56
cost			\$100.00

IR=0.02

Web
Service

	ϵ	ei/el	
BA	0.171		
C=m	0.047	0.274853	\$824.56
I=h	0.049	0.286549	\$859.65
A=m	0.035	0.204678	\$614.04
U=i	0.356	2.081871	\$6,245.61
F=cs	0.342	2	\$6,000.00
cost			\$100.00
			\$21,237.53

$M_{ik} = 0.944646$ $m=h$

$P_{ik} = 88.08\%$

Score \$18,706.02

**IIS
newdsn.exe
Quartz**

Web Server

	ϵ	ei/el	
BA	0.177		
a=m	0.037	0.209039	\$627.12
I=h	0.055	0.310734	\$932.20
u=i	0.369	2.084745	\$6,254.24
f=e	0.362	2.045197	\$6,135.59
cost			\$100.00

News
Server

	ϵ	ei/el	
BA	0.325		
a=l	0.046	0.141538	\$424.62
I=h	0.122	0.375384	\$1,126.15
u=10	0.325	1	\$3,000.00

f=ne	0.446	1.372307	\$4,116.92
cost	0.06		\$100.00
IR=0.02			

Quartz OS

	<u>e</u>	<u>ei/el</u>	
BA	0.691		
a=m	0.149	0.215629	\$646.89
l=m	0.16	0.231548	\$694.65
cost			\$100.00
			\$24,258.38

M_{ik}= 1.079013 m=hP_{ik} = 89.04%

Score \$21,599.66

CASE 3– Experience 2-2 & 3 hops:Accuracy Against Pairwise Comparison errors BA = \$3000

The experimental data for these experiences are available on demand in MS Excel. A request can be sent to sophiemartel@videotron.ca

CASE 3– Experience 3: Accuracy Against Pairwise Comparison errors BA = \$3000

The experimental data for experience 3 is available on demand in MS Excel. A request can be sent to sophiemartel@videotron.ca

CASE 1 Sensitivity analysis on P(T|ID) PCM : GRV when it is 8 times more likely that there is a threat if ID= y then if ID=n

Syn flood CANNOT
BE FIXED

IIS Server
3

Web Server

	<u>e</u>	<u>ei/el</u>	
BA	0.265		
l=m	0.06	0.226415	\$566.04
u=unlimited	0.616	2.324528	\$5,811.32
f=ne	0.06	0.226415	\$566.04
cost			\$100.00

Server 3 OS

e ei/el

BA	0.833								
I=m	0.167	0.200480	\$501.20		$M_{ik} =$	0.296005	$m=1$		
cost			\$100.00			$P_{ik} =$	87.60%		
			\$7,644.60						
					Score	\$6,696.67			
NetBIOS									
Serv 2									
Office Automation									
	ϵ	ei/el							
BA	0.385								
c=l	0.077	0.2	\$500.00						
I=m	0.077	0.2	\$500.00						
u=5	0.385	1	\$2,500.00						
f=nc	0.077	0.2	\$500.00						
cost			\$100.00						
Mail									
	ϵ	ei/el							
BA	0.402								
c=l	0.083	0.206467	\$516.17						
I=l	0.057	0.141791	\$354.48						
u=5	0.402	1	\$2,500.00		$M_{ik} =$	0.306868099	$m=1$		
f=nth	0.057	0.141791	\$354.48						
cost			\$100.00		$P_{ik} =$	40.08%			
			\$7,925.12						
					Score	\$3,176.39			
SYN Flood									
Server 1									
DHCP									
	ϵ	ei/el							
BA	0.75								
A=h	0.25	0.333333	\$833.33						
cost			\$100.00						
DNS									
	ϵ	ei/el							
BA	0.75								
A=h	0.25	0.333333	\$833.33						
cost			\$100.00						
Web Server									
	ϵ	ei/el							
BA	0.265								
a=m	0.06	0.226415	\$566.04						
u=unlimited	0.616	2.324528	\$5,811.32						
f=nc	0.06	0.226415	\$566.04						
Office Automation									
	ϵ	ei/el							
BA	0.417								

a=m	0.083	0.199040	\$497.60
u=5	0.417	1	\$2,500.00
fct=n	0.083	0.199040	\$497.60

Mail

	<u>e</u>	ei/el	
BA	0.437		
a=l	0.063	0.144164	\$360.41
u=5	0.437	1	\$2,500.00
f=nth	0.063	0.144164	\$360.41

Network
Printer

	<u>e</u>	ei/el	
BA	0.427		
A=m	0.087	0.203747	\$509.37
u=5	0.427	1	\$2,500.00
F=Nth	0.06	0.140515	\$351.29
cost			\$100.00

Internet

	<u>e</u>	ei/el	
BA	0.417		
a=m	0.083	0.199040	\$497.60
u=5	0.417	1	\$2,500.00
fct=n	0.083	0.199040	\$497.60
			\$22,481.95

$$M_{ik} = 0.870521768 \quad m=h$$

$$P_{ik} = 67.12\%$$

Score **\$15,089.88****IP
Fragmenta
tion PC1 &
PC2**

PC OS

	<u>e</u>	ei/el	
BA	0.875		
a=l	0.125	0.142857	\$357.14
cost			\$100.00

Web
Browser

	<u>e</u>	ei/el	
BA	0.667		
a=l	0.087	0.130434	\$326.09
u=l	0.087	0.130434	\$326.09
f=nc	0.159	0.238380	\$595.95

PC Outlook

	<u>e</u>	ei/el	
BA	0.7		
a=l	0.1	0.142857	\$357.14
u=l	0.1	0.142857	\$357.14
f=nth	0.1	0.142857	\$357.14
			\$2,776.70

$$M_{ik} = 0.107516274 \quad m=l$$

$$P_{ik} = 86.00\%$$

Score **\$2,387.96**

**SNMP
Community check
PC3**

OC 3 OS

	<u>e</u>	ei/e1	
BA	0.672		
a=l	0.094	0.139880	\$349.70
f=l	0.094	0.139880	\$349.70
c=l	0.139	0.206845	\$517.11
cost			\$100.00

**Web
Browser**

	<u>e</u>	ei/e1	
BA	0.667		
a=l	0.087	0.130434	\$326.09
u=l	0.087	0.130434	\$326.09
f=nc	0.159	0.238380	\$595.95

PC Outlook

	<u>e</u>	ei/e1	
BA	0.7		
a=l	0.1	0.142857	\$357.14
u=l	0.1	0.142857	\$357.14
f=nth	0.1	0.142857	\$357.14
			\$3,636.07

 $M_{ik} = 0.140792063$ $m=l$
 $P_{ik} = 71.52\%$
Score **\$2,600.52**

**Unpassworded
NetBios/SMB check
PC4**

PC4 OS

	<u>e</u>	ei/e1	
BA	0.833		
C=l	0.167	0.200480	\$501.20

 $M_{ik} = 0.019406943$ $m=l$
 $P_{ik} = 51.92\%$
Score **\$260.22**

**SYN flood
check
router**

**Routing
Service**

	<u>e</u>	ei/e1	
BA	0.75		
A=h	0.25	0.333333	\$833.33
cost			\$100.00

**Firewall
Service**

	<u>e</u>	ei/e1
--	----------	-------

BA	0.1		
A=vh	0.9	9	\$22,500.00
cost			100

Internet

	ϵ	ei/el	
BA	0.408		
a=m	0.075	0.417	\$1,042.50
u=5	0.43	0.083	\$207.50
fct=n	0.087	0.417	\$1,042.50
		0.083	\$25,825.83

 $M_{ik} = 1$ $m=h$ $P_{ik} = 86.00\%$ Score **\$22,210.22****Win NT
DoS PC5**

PC OS

	ϵ	ei/el	
BA	0.875		
a=l	0.125	0.142857	\$357.14
cost			\$10.00

Web
Browser

	ϵ	ei/el	
BA	0.667		
a=l	0.087	0.130434	\$326.09
u=l	0.087	0.130434	\$326.09
f=nc	0.159	0.238380	\$595.95

PC Outlook

	ϵ	ei/el	
BA	0.7		
a=l	0.1	0.142857	\$357.14
u=l	0.1	0.142857	\$357.14
f=nth	0.1	0.142857	\$357.14
			\$2,686.70

 $M_{ik} = 0.104031391$ $m=l$

51.92%

Score **\$1,394.93****CASE 3 Sensitivity analysis on P(T|ID) PCM : GRV when it is 8 times more likely that there is a threat if ID= y****then if ID=n****IIS ism.dll**News
Service

	ϵ	ei/el	
BA	0.354		
C=l	0.058	0.163841	\$491.53
I=h	0.111	0.313559	\$940.68
A=m	0.037	0.104519	\$313.56

U=10	0.379	1.070621	\$3,211.86
F=Nec	0.061	0.172316	\$516.95
cost			\$100.00

Web
Service

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.16		
C=m	0.046	0.2875	\$862.50
I=h	0.046	0.2875	\$862.50
A=m	0.032	0.2	\$600.00
U=i	0.358	2.2375	\$6,712.50
F=cs	0.358	2.2375	\$6,712.50
cost			\$100.00
			\$21,424.58

 $M_{ik} = 0.792712 \quad m=h$
 $P_{ik} = 87.60\%$
Score **\$18,767.93**Unpasswor
ded
NetBios/S
MB check
Granit

Granit OS

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.778		
C=m	0.222	0.285347	\$856.04

 $M_{ik} = 0.031673632 \quad m=l$
 $P_{ik} = 51.92\%$
Score **\$444.46**Unpasswor
ded
NetBios/S
MB check
Shale

Shale OS

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.857		
C=l	0.143	0.166861	\$500.58

 $M_{ik} = 0.018521651 \quad m=l$
 $P_{ik} = 51.92\%$
Score **\$259.90**MIB-II
UDP table
Granite

Granit OS

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.778		
C=m	0.222	0.285347	\$856.04

 $M_{ik} = 0.031673632 \quad m=l$
 $P_{ik} = 71.52\%$

Score **\$612.24**

**SYN port
Scanning
Granite**

**CANNOT Be
FIXED**

**Omni
HTTPD
Imagemap
CGI
Quartz**

Web Server

	<u>e</u>	<u>ei/el</u>	
BA	0.133		
c=m	0.045	0.338345	\$1,015.04
l=h	0.045	0.338345	\$1,015.04
u=i	0.389	2.924812	\$8,774.44
f=e	0.389	2.924812	\$8,774.44
cost			\$100.00

**News
Server**

	<u>e</u>	<u>ei/el</u>	
BA	0.341		
c=l	0.06	0.175953	\$527.86
l=h	0.105	0.307917	\$923.75
u=l0	0.435	1.275659	\$3,826.98
f=nc	0.06	0.175953	\$527.86
cost			\$100.00

Quartz OS

	<u>e</u>	<u>ei/el</u>	
BA	0.691		
c=m	0.189	0.273516	\$820.55
l=m	0.12	0.173661	\$520.98
cost			\$100.00
			\$27,026.93

$M_{ik} = \quad l \quad m=h$

$P_{ik} = \quad 88.44\%$

Score **\$23,902.62**

**Open
news
server
check
Quartz**

Web Server

	<u>e</u>	<u>ei/el</u>	
BA	0.133		
c=m	0.045	0.338345	\$1,015.04
l=h	0.045	0.338345	\$1,015.04
u=i	0.389	2.924812	\$8,774.44
f=e	0.389	2.924812	\$8,774.44

cost			\$100.00			
News Server						
	$\bar{e}$	ei/el				
BA	0.341					
c=l	0.06	0.175953	\$527.86			
I=h	0.105	0.307917	\$923.75			
u=10	0.435	1.275659	\$3,826.98	$M_{ik} =$	0.946663056	m=h
f=nc	0.06	0.175953	\$527.86	$P_{ik} =$	88.40%	
cost			\$100.00			
			\$25,585.40			
				Score	\$22,617.49	
SNMPCom munity check Shale						
Shale OS						
	$\bar{e}$	ei/el				
BA	0.691					
c=m	0.189	0.273516	\$820.55	$M_{ik} =$	0.053336	m=l
I=m	0.12	0.173661	\$520.98			
cost			\$100.00	(Attack detected on Quartz)	$P_{ik} =$	87.68%
			\$1,441.53			
				Score	\$1,263.94	
IIS newdsn.exe Quartz						
Web Server						
	$\bar{e}$	ei/el				
BA	0.168					
a=m	0.034	0.202380	\$607.14			
I=h	0.052	0.309523	\$928.57			
u=i	0.373	2.220238	\$6,660.71			
f=e	0.373	2.220238	\$6,660.71			
cost			\$100.00			
News Server						
	$\bar{e}$	ei/el				
BA	0.356					
a=l	0.039	0.109550	\$328.65			
I=h	0.125	0.351123	\$1,053.37			
u=10	0.414	1.162921	\$3,488.76			
f=ne	0.066	0.185393	\$556.18			
cost			\$100.00			

Quartz OS

	$\underline{e}$	ei/el	
BA	0.75		
a=m	0.125	0.166666	\$500.00
l=m	0.125	0.166666	\$500.00
cost			\$100.00
			\$21,584.11

$$M_{ik} = 0.798614 \quad m=h$$

$$P_{ik} = 88.40\%$$

$$\text{Score} = \$19,080.35$$

CASE 1 Sensitivity analysis on P(T|ET) PCM : GRV when it is 3 times more likely that there is a threat if ET=**y then if ET=n**

Syn flood CANNOT
BE FIXED

**IIS Server
3**

Web Server

	$\underline{e}$	ei/el	
BA	0.265		
l=m	0.06	0.226415	\$566.04
u=unlimited	0.616	2.324528	\$5,811.32
f=ne	0.06	0.226415	\$566.04
cost			\$100.00

Server 3 OS

	$\underline{e}$	ei/el	
BA	0.833		
l=m	0.167	0.200480	\$501.20
cost			\$100.00
			\$7,644.60

$$M_{ik} = 0.296005 \quad m=l$$

$$P_{ik} = 86.16\%$$

$$\text{Score} = \$6,586.58$$

**NetBIOS
Serv 2**Office
Automation

	$\underline{e}$	ei/el	
BA	0.385		
c=l	0.077	0.2	\$500.00
l=m	0.077	0.2	\$500.00
u=5	0.385	1	\$2,500.00
f=nc	0.077	0.2	\$500.00
cost			\$100.00

Mail

$\underline{e}$ ei/el

BA	0.402		
c=l	0.083	0.206467	\$516.17
l=l	0.057	0.141791	\$354.48
u=5	0.402	1	\$2,500.00
f=nth	0.057	0.141791	\$354.48
cost			\$100.00
			\$7,925.12

$$M_{ik} = 0.306868099 \quad m=1$$

$$P_{ik} = 58.80\%$$

Score **\$4,659.97**

SYN Flood Server 1

DHCP

	<u>e</u>	ei/e1	
BA	0.75		
A=h	0.25	0.333333	\$833.33
cost			\$100.00

DNS

	<u>e</u>	ei/e1	
BA	0.75		
A=h	0.25	0.333333	\$833.33
cost			\$100.00

Web Server

	<u>e</u>	ei/e1	
BA	0.265		
a=m	0.06	0.226415	\$566.04
u=unlimited	0.616	2.324528	\$5,811.32
f=nc	0.06	0.226415	\$566.04

Office Automation

	<u>e</u>	ei/e1	
BA	0.417		
a=m	0.083	0.199040	\$497.60
u=5	0.417	1	\$2,500.00
fct=n	0.083	0.199040	\$497.60

Mail

	<u>e</u>	ei/e1	
BA	0.437		
a=l	0.063	0.144164	\$360.41
u=5	0.437	1	\$2,500.00
f=nth	0.063	0.144164	\$360.41

Network Printer

	<u>e</u>	ei/e1	
BA	0.427		
A=m	0.087	0.203747	\$509.37
u=5	0.427	1	\$2,500.00
F=Nth	0.06	0.140515	\$351.29
cost			\$100.00

Internet

	<u>e</u>	ei/el	
BA	0.417		
a=m	0.083	0.199040	\$497.60
u=5	0.417	1	\$2,500.00
fct=n	0.083	0.199040	\$497.60
			\$22,481.95

$$M_{ik} = 0.870521768 \quad m=h$$

$$P_{ik} = 85.20\%$$

Score **\$19,154.62**

IP Fragmenta tion PC1 & PC2

PC OS

	<u>e</u>	ei/el	
BA	0.875		
a=l	0.125	0.142857	\$357.14
cost			\$100.00

Web Browser

	<u>e</u>	ei/el	
BA	0.667		
a=l	0.087	0.130434	\$326.09
u=l	0.087	0.130434	\$326.09
f=nc	0.159	0.238380	\$595.95

PC Outlook

	<u>e</u>	ei/el	
BA	0.7		
a=l	0.1	0.142857	\$357.14
u=l	0.1	0.142857	\$357.14
f=nth	0.1	0.142857	\$357.14
			\$2,776.70

$$M_{ik} = 0.107516274 \quad m=l$$

$$P_{ik} = 82.00\%$$

Score **\$2,276.89**

SNMP Communit y check PC3

OC 3 OS

	<u>e</u>	ei/el	
BA	0.672		
a=l	0.094	0.139880	\$349.70
I=l	0.094	0.139880	\$349.70
c=l	0.139	0.206845	\$517.11
cost			\$100.00

Web Browser

	<u>e</u>	ei/el	
BA	0.667		
a=l	0.087	0.130434	\$326.09
u=l	0.087	0.130434	\$326.09
f=nc	0.159	0.238380	\$595.95

PC Outlook

	$\underline{e}$	ei/el	
BA	0.7		
a=l	0.1	0.142857	\$357.14
u=l	0.1	0.142857	\$357.14
f=nth	0.1	0.142857	\$357.14
			\$3,636.07

$$M_{ik} = 0.140792063 \quad m=l$$

$$P_{ik} = 78.40\%$$

Score **\$2,850.68**Unpassworded
NetBios/SMB check
PC4

PC4 OS

	$\underline{e}$	ei/el	
BA	0.833		
C=l	0.167	0.200480	\$501.20

$$M_{ik} = 0.019406943 \quad m=l$$

$$P_{ik} = 66.16\%$$

Score **\$331.59**SYN flood
check
routerRouting
Service

	$\underline{e}$	ei/el	
BA	0.75		
A=h	0.25	0.333333	\$833.33
cost			\$100.00

Firewall
Service

	$\underline{e}$	ei/el	
BA	0.1		
A=vh	0.9	9	\$22,500.00
cost			100

Internet

	$\underline{e}$	ei/el	
BA	0.408		
a=m	0.075	0.417	\$1,042.50
u=5	0.43	0.083	\$207.50
fct=n	0.087	0.417	\$1,042.50
		0.083	\$25,825.83

$$M_{ik} = 1 \quad m=h$$

$$P_{ik} = 85.20\%$$

Score **\$22,003.61**Win NT
DoS PC5

PC OS

	$\underline{e}$	ei/el	
BA	0.875		
a=l	0.125	0.142857	\$357.14
cost			\$10.00

Web Browser				
	$\underline{e}$	$ei/e1$		
BA	0.667			
a=l	0.087	0.130434	\$326.09	
u=l	0.087	0.130434	\$326.09	
f=nc	0.159	0.238380	\$595.95	
PC Outlook				
	$\underline{e}$	$ei/e1$		
BA	0.7			$M_{ik}= 0.104031391$
a=l	0.1	0.142857	\$357.14	
u=l	0.1	0.142857	\$357.14	$P_{ik} 66.16\%$
f=nth	0.1	0.142857	\$357.14	
			\$2,686.70	
			Score	\$1,777.52

CASE 3 Sensitivity analysis on P(TIET) PCM : GRV when it is 3 times more likely that there is a threat if ET=

y then if ET=n

IIS ism.dll

News Service

	$\underline{e}$	$ei/e1$	
BA	0.354		
C=l	0.058	0.163841	\$491.53
I=h	0.111	0.313559	\$940.68
A=m	0.037	0.104519	\$313.56
U=10	0.379	1.070621	\$3,211.86
F=Nec	0.061	0.172316	\$516.95
cost			\$100.00

Web Service

	$\underline{e}$	$ei/e1$	
BA	0.16		
C=m	0.046	0.2875	\$862.50
I=h	0.046	0.2875	\$862.50
A=m	0.032	0.2	\$600.00
U=i	0.358	2.2375	\$6,712.50
F=es	0.358	2.2375	\$6,712.50
cost			\$100.00
			\$21,424.58

$M_{ik}= 0.792712$ $m=h$

$P_{ik} = 85.20\%$

Score **\$18,253.74**

**Unpassworded
NetBios/SMB check
Granit**

Granit OS

				$M_{ik} =$	0.031673632	$m = 1$
BA	$\underline{e}$	ei/el		$P_{ik} =$	66.16%	
C=m	0.778	0.285347	\$856.04			
				Score	\$566.36	
Unpassworded NetBios/SMB check Shale						
Shale OS						
BA	$\underline{e}$	ei/el		$M_{ik} =$	0.018521651	$m = 1$
C=l	0.857	0.166861	\$500.58	$P_{ik} =$	66.16%	
				Score	\$331.19	
MIB-II UDP table Granite						
Granit OS						
BA	$\underline{e}$	ei/el		$M_{ik} =$	0.031673632	$m = 1$
C=m	0.778	0.285347	\$856.04	$P_{ik} =$	78.40%	
				Score	\$671.14	
SYN port Scanning Granite				CANNOT Be FIXED		
Omni HTTPD Imagemap CGI Quartz						
Web Server						
BA	$\underline{e}$	ei/el				
c=m	0.133	0.338345	\$1,015.04			
I=h	0.045	0.338345	\$1,015.04			
u=i	0.389	2.924812	\$8,774.44			
f=e	0.389	2.924812	\$8,774.44			
cost			\$100.00			
News Server						
	$\underline{e}$	ei/el				

BA	0.341		
c=l	0.06	0.175953	\$527.86
l=h	0.105	0.307917	\$923.75
u=10	0.435	1.275659	\$3,826.98
f=nc	0.06	0.175953	\$527.86
cost			\$100.00

Quartz OS

	<u>e</u>	<u>ci/el</u>	
BA	0.691		
c=m	0.189	0.273516	\$820.55
l=m	0.12	0.173661	\$520.98
cost			\$100.00
			\$27,026.93

$$M_{ik} = \quad l \quad m=h$$

$$P_{ik} = 87.60\%$$

$$\text{Score} = \$23,675.59$$

**Open
news
server
check
Quartz**

Web Server

	<u>e</u>	<u>ci/el</u>	
BA	0.133		
c=m	0.045	0.338345	\$1,015.04
l=h	0.045	0.338345	\$1,015.04
u=i	0.389	2.924812	\$8,774.44
f=c	0.389	2.924812	\$8,774.44
cost			\$100.00

News
Server

	<u>e</u>	<u>ci/el</u>	
BA	0.341		
c=l	0.06	0.175953	\$527.86
l=h	0.105	0.307917	\$923.75
u=10	0.435	1.275659	\$3,826.98
f=nc	0.06	0.175953	\$527.86
cost			\$100.00
			\$25,585.40

$$M_{ik} = 0.946663056 \quad m=h$$

$$P_{ik} = 87.60\%$$

$$\text{Score} = \$22,412.81$$

**SNMPCom
munity
check
Shale**

Shale OS

	<u>e</u>	<u>ci/el</u>	
BA	0.691		
c=m	0.189	0.273516	\$820.55
l=m	0.12	0.173661	\$520.98

$$M_{ik} = 0.053336 \quad m=l$$

cost \$100.00

(Attack
detected on
Quartz) $P_{ik} = 84.24\%$

\$1,441.53

Score \$1,214.35

**IIS
newdsn.exe
Quartz****Web Server**

	$\underline{e}$	ei/el	
BA	0.168		
a=m	0.034	0.202380	\$607.14
l=h	0.052	0.309523	\$928.57
u=i	0.373	2.220238	\$6,660.71
f=e	0.373	2.220238	\$6,660.71
cost			\$100.00

**News
Server**

	$\underline{e}$	ei/el	
BA	0.356		
a=l	0.039	0.109550	\$328.65
l=h	0.125	0.351123	\$1,053.37
u=10	0.414	1.162921	\$3,488.76
f=ne	0.066	0.185393	\$556.18
cost			\$100.00

Quartz OS

	$\underline{e}$	ei/el	
BA	0.75		
a=m	0.125	0.166666	\$500.00
l=m	0.125	0.166666	\$500.00
cost			\$100.00
			\$21,584.11

 $M_{ik} = 0.798614$ $m=h$ $P_{ik} = 87.60\%$

Score \$18,907.68

CASE 1 Sensitivity analysis on $P(A|T)$ PCM : GRV when it is 2 times more likely that there is a threat if $T=y$ **then if $T=n$** **IIS Server
3****Web Server**

	$\underline{e}$	ei/el	
BA	0.265		
l=m	0.06	0.226415	\$566.04
u=unlimited	0.616	2.324528	\$5,811.32
f=ne	0.06	0.226415	\$566.04
cost			\$100.00

Server 3 OS

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$
BA	0.833	

I=m	0.167	0.200480	\$501.20
cost			\$100.00
			\$7,644.60

$M_{ik} =$	0.296005	$m = 1$
$P_{ik} =$	66.03%	

Score **\$5,047.73**NetBIOS
Serv 2Office
Automation

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.385		
c=l	0.077	0.2	\$500.00
I=m	0.077	0.2	\$500.00
u=5	0.385	1	\$2,500.00
f=nc	0.077	0.2	\$500.00
cost			\$100.00

Mail

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.402		
c=l	0.083	0.206467	\$516.17
I=l	0.057	0.141791	\$354.48
u=5	0.402	1	\$2,500.00
f=nth	0.057	0.141791	\$354.48
cost			\$100.00
			\$7,925.12

$M_{ik} =$	0.306868099	$m = 1$
$P_{ik} =$	51.04%	

Score **\$4,044.98**SYN Flood
Server 1

DHCP

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.75		
A=h	0.25	0.333333	\$833.33
cost			\$100.00

DNS

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.75		
A=h	0.25	0.333333	\$833.33
cost			\$100.00

Web Server

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.265		
a=m	0.06	0.226415	\$566.04
u=unlimited	0.616	2.324528	\$5,811.32
f=nc	0.06	0.226415	\$566.04

Office

Automation

	$\underline{e}$	ei/el	
BA	0.417		
a=m	0.083	0.199040	\$497.60
u=5	0.417	1	\$2,500.00
fct=n	0.083	0.199040	\$497.60

Mail

	$\underline{e}$	ei/el	
BA	0.437		
a=l	0.063	0.144164	\$360.41
u=5	0.437	1	\$2,500.00
f=nth	0.063	0.144164	\$360.41

Network

Printer

	$\underline{e}$	ei/el	
BA	0.427		
A=m	0.087	0.203747	\$509.37
u=5	0.427	1	\$2,500.00
F=Nth	0.06	0.140515	\$351.29
cost			\$100.00

Internet

	$\underline{e}$	ei/el	
BA	0.417		
a=m	0.083	0.199040	\$497.60
u=5	0.417	1	\$2,500.00
fct=n	0.083	0.199040	\$497.60
			\$22,481.95

$$M_{ik} = 0.870521768 \quad m=h$$

$$P_{ik} = 65.90\%$$

Score **\$14,815.61**

IP
Fragmenta
tion PC1 &
PC2

PC OS

	$\underline{e}$	ei/el	
BA	0.875		
a=l	0.125	0.142857	\$357.14
cost			\$100.00

Web
Browser

	$\underline{e}$	ei/el	
BA	0.667		
a=l	0.087	0.130434	\$326.09
u=1	0.087	0.130434	\$326.09
f=nc	0.159	0.238380	\$595.95

PC Outlook

	$\underline{e}$	ei/el	
BA	0.7		
a=l	0.1	0.142857	\$357.14

$$M_{ik} = 0.107516274 \quad m=l$$

u=l	0.1	0.142857	\$357.14
f=nth	0.1	0.142857	\$357.14
			\$2,776.70

$P_{ik} = 65.36\%$

Score **\$1,814.85**

**SNMP
Community check
PC3**

OC 3 OS

	$\frac{e}{e_i/e_1}$		
BA	0.672		
a=l	0.094	0.139880	\$349.70
I=l	0.094	0.139880	\$349.70
c=l	0.139	0.206845	\$517.11
cost			\$100.00

**Web
Browser**

	$\frac{e}{e_i/e_1}$		
BA	0.667		
a=l	0.087	0.130434	\$326.09
u=l	0.087	0.130434	\$326.09
f=nc	0.159	0.238380	\$595.95

PC Outlook

	$\frac{e}{e_i/e_1}$		
BA	0.7		
a=l	0.1	0.142857	\$357.14
u=l	0.1	0.142857	\$357.14
f=nth	0.1	0.142857	\$357.14
			\$3,636.07

$M_{ik} = 0.140792063$ $m=l$

$P_{ik} = 60.89\%$

Score **\$2,214.00**

**Unpassworded
NetBios/SMB check
PC4**

PC4 OS

	$\frac{e}{e_i/e_1}$		
BA	0.833		
C=l	0.167	0.200480	\$501.20

$M_{ik} = 0.019406943$ $m=l$

$P_{ik} = 54.78\%$

Score **\$274.56**

**SYN flood
check
router**

**Routing
Service**

	$\frac{e}{e_i/e_1}$		
BA	0.75		
A=h	0.25	0.333333	\$833.33
cost			\$100.00

Firewall
Service

	$\underline{e}$	ei/el	
BA	0.1		
A=vh	0.9	9	\$22,500.00
cost			100

Internet

	$\underline{e}$	ei/el	
BA	0.408		
a=m	0.075	0.417	\$1,042.50
u=5	0.43	0.083	\$207.50
fct=n	0.087	0.417	\$1,042.50
		0.083	\$25,825.83

 $M_{ik} = 1 \quad m=h$ $P_{ik} = 65.90\%$ Score **\$17,019.22**Win NT
DoS PC5

PC OS

	$\underline{e}$	ei/el	
BA	0.875		
a=l	0.125	0.142857	\$357.14
cost			\$10.00

Web
Browser

	$\underline{e}$	ei/el	
BA	0.667		
a=l	0.087	0.130434	\$326.09
u=l	0.087	0.130434	\$326.09
f=nc	0.159	0.238380	\$595.95

PC Outlook

	$\underline{e}$	ei/el	
BA	0.7		
a=l	0.1	0.142857	\$357.14
u=l	0.1	0.142857	\$357.14
f=nth	0.1	0.142857	\$357.14
			\$2,686.70

 $M_{ik} = 0.104031391 \quad m=l$ $P_{ik} = 54.78\%$ Score **\$1,471.77****CASE 3 Sensitivity analysis on P(A/T) PCM : GRV when it is 2 times more likely that there is a threat if T= y****then if T=n**

IIS rsm.dll

News
Service

	$\underline{e}$	ei/el	
BA	0.354		
C=l	0.058	0.163841	\$491.53
I=h	0.111	0.313559	\$940.68
A=m	0.037	0.104519	\$313.56
U=10	0.379	1.070621	\$3,211.86

F=Nec 0.061 0.172316 \$516.95
cost \$100.00

Web
Service

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.16		
C=m	0.046	0.2875	\$862.50
I=h	0.046	0.2875	\$862.50
A=m	0.032	0.2	\$600.00
U=i	0.358	2.2375	\$6,712.50
F=es	0.358	2.2375	\$6,712.50
cost			\$100.00
			\$21,424.58

$M_{ik} = 0.792712$ $m=h$

$P_{ik} = 65.90\%$

Score **\$14,118.80**

Unpasswor
ded
NetBios/S
MB check
Granit

Granit OS

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.778		
C=m	0.222	0.285347	\$856.04

$M_{ik} = 0.031673632$ $m=l$

$P_{ik} = 54.78\%$

Score **\$468.94**

Unpasswor
ded
NetBios/S
MB check
Shale

Shale OS

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.857		
C=l	0.143	0.166861	\$500.58

$M_{ik} = 0.018521651$ $m=l$

$P_{ik} = 54.78\%$

Score **\$274.22**

MIB-II
UDP table
Granite

Granit OS

	$\frac{e}{e_i}$	$\frac{e_i}{e_l}$	
BA	0.778		
C=m	0.222	0.285347	\$856.04

$M_{ik} = 0.031673632$ $m=l$

$P_{ik} = 60.89\%$

Score **\$521.24**

SYN port
Scanning
Granite

CANNOT Be
FIXED

Omni
HTTPD
Imagemap
CGI
Quartz

Web Server

	$\frac{e}{e1}$	$\frac{ei}{e1}$	
BA	0.133		
c=m	0.045	0.338345	\$1,015.04
I=h	0.045	0.338345	\$1,015.04
u=i	0.389	2.924812	\$8,774.44
f=e	0.389	2.924812	\$8,774.44
cost			\$100.00

News
Server

	$\frac{e}{e1}$	$\frac{ei}{e1}$	
BA	0.341		
c=l	0.06	0.175953	\$527.86
I=h	0.105	0.307917	\$923.75
u=10	0.435	1.275659	\$3,826.98
f=ne	0.06	0.175953	\$527.86
cost			\$100.00

Quartz OS

	$\frac{e}{e1}$	$\frac{ei}{e1}$	
BA	0.691		
c=m	0.189	0.273516	\$820.55
I=m	0.12	0.173661	\$520.98
cost			\$100.00
			\$27,026.93

$M_{ik} =$ l $m=h$

$P_{ik} = 66.30\%$

Score **\$17,918.86**

Open
news
server
check
Quartz

Web Server

	$\frac{e}{e1}$	$\frac{ei}{e1}$	
BA	0.133		
c=m	0.045	0.338345	\$1,015.04
I=h	0.045	0.338345	\$1,015.04
u=i	0.389	2.924812	\$8,774.44
f=e	0.389	2.924812	\$8,774.44
cost			\$100.00

News
Server

	e	ei/el	
BA	0.341		
c=l	0.06	0.175953	\$527.86
l=h	0.105	0.307917	\$923.75
u=10	0.435	1.275659	\$3,826.98
f=nc	0.06	0.175953	\$527.86
cost			\$100.00
			\$25,585.40

$$M_{ik} = 0.946663056 \quad m=h$$

$$P_{ik} = 66.30\%$$

Score **\$16,963.12**

SNMPCom
munity
check
Shale

Shale OS

	e	ei/el	
BA	0.691		
c=m	0.189	0.273516	\$820.55
l=m	0.12	0.173661	\$520.98
cost			\$100.00

$$M_{ik} = 0.053336 \quad m=l$$

$$P_{ik} = 63.79\%$$

(Attack
detected on
Quartz)

\$1,441.53

Score **\$919.55**

IIS
newdsn.exe
Quartz

Web Server

	e	ei/el	
BA	0.168		
a=m	0.034	0.202380	\$607.14
l=h	0.052	0.309523	\$928.57
u=i	0.373	2.220238	\$6,660.71
f=e	0.373	2.220238	\$6,660.71
cost			\$100.00

News
Server

	e	ei/el	
BA	0.356		
a=l	0.039	0.109550	\$328.65
l=h	0.125	0.351123	\$1,053.37
u=10	0.414	1.162921	\$3,488.76
f=ne	0.066	0.185393	\$556.18
cost			\$100.00

Quartz OS

	$\underline{e}$	e_i/e_l	
BA	0.75		
a=m	0.125	0.166666	\$500.00
l=m	0.125	0.166666	\$500.00
cost			\$100.00
			\$21,584.11

$M_{ik} = 0.798614 \quad m=h$
 $P_{ik} = 66.30\%$

Score $\$14,310.26$