

ABSTRACT

Title of dissertation: MODEL-BASED SUPPORT
FOR INFORMATION TECHNOLOGY
SECURITY DECISION MAKING

Danielle Chrun, Doctor of Philosophy, 2011

Dissertation directed by: Associate Professor Michel Cukier
Professor Ali Mosleh
Reliability Engineering Program

With the increase in the number and diversity of attacks, a main concern for organizations is to keep their network and systems secure. Existing frameworks to manage Information Technology (IT) security include empirical evaluations, security risk assessments, cost-benefit analyses, and adversary-based evaluations. These techniques are often not easy to apply and their results are usually difficult to convey. This dissertation presents a model to help reasoning about security and to support communication between IT security experts and managers. The model identifies major components of security: threat, user, organization, asset, and emphasizes the human element. Characteristics for each component are determined and cover the attacker's motivations, the user's risk perception, the IT security team expertise, and the depth of protection of the asset. These characteristics are linked through causal influences that can represent positive or negative relationships and be leveraged to rank alternatives through a set of weights. The described formalism allows IT security officers to brainstorm about IT security issues, to evaluate the impacts

of alternative solutions on characteristics of security, and ultimately on the level of security, and to communicate their findings to managers.

The contributions of this dissertation are three-fold. First, we introduce an approach to develop and validate a model for IT security decision making, given known issues related to this task: difficulties in sharing security data, lack of accepted security metrics, limitation in available information and use of experts. We propose a development and validation process that relies on two sources of information: experts and data. Second, we provide the results of the model development for academic environments. The resulting model is based on extended discussions with the Director of Security at the University of Maryland (UMD), two interviewed experts, fifteen surveyed experts, and empirical data collected at UMD. Finally, we demonstrate the use of the model to justify IT security decisions and present methodological steps towards measuring various characteristics of the model.

MODEL-BASED SUPPORT
FOR INFORMATION TECHNOLOGY SECURITY
DECISION MAKING

by

Danielle Chrun

Dissertation submitted to the Faculty of the Graduate School of the
University of Maryland, College Park in partial fulfillment
of the requirements for the degree of
Doctor of Philosophy
2011

Advisory Committee:

Associate Professor Michel Cukier, Chair/Advisor

Professor Ali Mosleh, Co-Advisor

Professor John S. Baras, Dean's Representative

Associate Professor Atif M. Memon

Professor Mohammad Modarres

Mr. Gerry F. Sneeringer, Special Member

© Copyright by
Danielle Chrun
2011

Acknowledgments

This dissertation closes a substantial chapter of my life: I would like to express my gratitude to all the people who contributed to this achievement, directly or indirectly. I would have liked to cite each and everyone of the people I met and who helped me get where I am now but I would end up with pages of acknowledgement.

First and foremost, I would like to thank my advisors. I would like to express my gratitude to my main advisor, Dr. Michel Cukier. You opened the door to a field that was out of my comfort zone. It was a tedious path but you were patient enough to let me grow by myself in this field. I am thankful to my co-advisor, Dr. Ali Mosleh. Our discussions have always been inspiring, not only for this dissertation but for life in general. I would like to thank both of you for setting such high expectations for myself and for always believing in me. I would like to acknowledge Mr. Gerry F. Sneeringer: you never seemed annoyed by seeing me popping up my head once a week in your office. I hope you enjoyed your first time on an advisory committee as much as I enjoyed working with you.

I would like to express my gratitude to the members of my doctoral committee: Dr. John S. Baras, Dr. Atif M. Memon, and Dr. Mohammad Modarres. Thank you for your valuable feedback that make this dissertation what it is.

I wish to express my appreciation to all professors and staff I met during my graduate studies, for their help, but also for the professional opportunities they provided me with.

My office mates deserve a special mention. Being productive and succeeding

in Graduate School also relies on the work environment and all of you made the office a pleasant place. We shared our frustrations and our happiness, and I could not have dreamt of a better place to work on my research. Thank you all for your support. Special thanks go to Reza for always taking the time to listen to me.

During my graduate studies, I was lucky to build great friendships. I cannot cite everyone but I want to especially recognize Bertrand, Brian, Cristel, Gaurav, Gabriel, Keshav, Jamie, Qinwen, Roland, and Vivien. Having you in my life is a blessing: you made these several years an incredible, unforgettable experience.

This acknowledgement section would not be complete if I did not include all the support I received from France. Especially, many thanks to Pauline for believing in me: despite the distance, you managed to cheer me up every time I needed to be. I would like also to recognize my family. Seeing one of your children/siblings/nieces/cousins leave for a Ph.D. in a foreign country was not easy and you always supported my choices. You all inspired me to achieve great things in life. I am especially thankful to my mother, Kim Sieng, and my sister, Catherine, for their unfailing support. To my little sister: thank you for making me laugh, even when I did not want to.

Finally, my deepest and most sincere thanks go to Robin. Thank you for dragging me in this adventure. Thank you for the guidance and hours long discussions on this work. Thank you for believing in me, and mostly, thank you for inspiring me. I am now looking forward to writing the next chapter of our life together.

Table of Contents

| | |
|--|------|
| List of Tables | viii |
| List of Figures | x |
| 1 Introduction | 1 |
| 1.1 Context: The Importance of Managing Security | 1 |
| 1.2 The Issues in IT Security | 3 |
| 1.2.1 The Lack of Available Sound Security Data and Metrics . . . | 3 |
| 1.2.2 Managing Security | 5 |
| 1.2.3 Communication | 7 |
| 1.2.4 The Human Element | 7 |
| 1.3 Approach | 9 |
| 1.4 Contributions | 10 |
| 1.5 Outline | 12 |
| 2 Related Work | 14 |
| 2.1 Introduction | 14 |
| 2.2 Managing security | 15 |
| 2.2.1 Ad-hoc assessments | 15 |
| 2.2.2 Self Assessments | 16 |
| 2.2.3 Standards and Regulations | 16 |
| 2.2.4 Security Risk Assessments | 19 |
| 2.2.5 Economic Approaches | 22 |
| 2.2.6 Frameworks for Decision Making | 26 |
| 2.2.7 Decision Theory and Game Theory Approaches | 28 |
| 2.2.8 Adversary-Based Evaluations | 29 |
| 2.2.9 Model-based Approaches | 31 |
| 2.2.10 Perspectives | 32 |
| 2.3 Including the Human Element | 34 |
| 2.3.1 The Attacker | 35 |
| 2.3.2 The Organization | 37 |
| 2.3.3 The User | 38 |
| 2.4 Model Validation | 39 |
| 2.5 Summary | 42 |
| 3 An Approach for the Development and Validation of a Model for Decision Making in IT Security | 43 |
| 3.1 Introduction | 43 |
| 3.2 Model Representation | 44 |
| 3.2.1 Motivations | 44 |
| 3.2.2 Model Constituents | 45 |
| 3.2.3 Model Formalism | 46 |
| 3.3 Model Development and Validation | 48 |

| | | |
|---------|--|----|
| 3.3.1 | Objectives | 48 |
| 3.3.2 | An Ideal Validation Plan | 49 |
| 3.3.3 | Why is the Validation of an IT Security Decision Model so Challenging? | 51 |
| 3.3.3.1 | Experts | 51 |
| 3.3.3.2 | Data | 52 |
| 3.4 | Process | 56 |
| 3.4.1 | Approach | 56 |
| 3.4.2 | Phase 1: Building a Model through Interviews | 56 |
| 3.4.2.1 | Objectives | 56 |
| 3.4.2.2 | Interview Design | 60 |
| 3.4.2.3 | Selection of Experts | 61 |
| 3.4.2.4 | Interview | 62 |
| 3.4.2.5 | Analysis | 62 |
| 3.4.3 | Phase 2: Conducting Surveys to Gather more Information | 62 |
| 3.4.3.1 | Objectives | 62 |
| 3.4.3.2 | Survey Design | 63 |
| 3.4.3.3 | Survey Testing | 66 |
| 3.4.3.4 | Sample of Experts | 67 |
| 3.4.3.5 | Survey Implementation and Analysis | 67 |
| 3.4.4 | Phase 3: Incremental Validation | 68 |
| 3.4.4.1 | Objectives | 68 |
| 3.4.4.2 | Validation through Experts | 68 |
| 3.4.4.3 | Validation through Case Studies | 69 |
| 3.4.4.4 | Use of Indicators | 69 |
| 3.5 | Summary | 70 |
| 4 | Model Development | 72 |
| 4.1 | Introduction | 72 |
| 4.2 | Initial Model | 73 |
| 4.2.1 | A Special Collaboration with the Director of Security | 73 |
| 4.2.2 | Preliminary Model | 74 |
| 4.2.2.1 | Model Components | 74 |
| 4.2.2.2 | Model Development at the University of Maryland | 75 |
| 4.3 | Results of the Interviews | 78 |
| 4.3.1 | Model Developed at other Academic Environments | 78 |
| 4.3.2 | General Insights | 80 |
| 4.3.3 | Outputs | 82 |
| 4.4 | Results of the Surveys | 82 |
| 4.4.1 | Survey Implementation | 83 |
| 4.4.1.1 | Survey Design | 83 |
| 4.4.1.2 | Survey Testing | 83 |
| 4.4.1.3 | Survey Administration | 84 |
| 4.4.2 | General Insights | 84 |
| 4.4.2.1 | Visit and Response Rates | 84 |

| | | |
|---------|--|-----|
| 4.4.2.2 | Technical versus Managerial Positions | 86 |
| 4.4.3 | Components of Security | 90 |
| 4.4.4 | Characteristics of Security | 90 |
| 4.4.5 | Outputs | 95 |
| 4.5 | Developing the Final Model | 99 |
| 4.5.1 | Objective: Aggregating the Results of the Interviews and Surveys | 99 |
| 4.5.2 | Step 1: Vocabulary Checking | 100 |
| 4.5.3 | Step 2: Extensive Listing of all Relationships | 101 |
| 4.5.4 | Step 3: Final Model Development | 105 |
| 4.6 | Summary | 108 |
| 5 | Model Validation | 109 |
| 5.1 | Introduction | 109 |
| 5.2 | Validation by Experts | 110 |
| 5.2.1 | Objectives | 110 |
| 5.2.2 | Results of the Validation by Experts | 110 |
| 5.2.3 | Resulting Model | 111 |
| 5.3 | Validation with Case Studies | 114 |
| 5.3.1 | Objectives | 114 |
| 5.3.2 | The University of Maryland | 116 |
| 5.3.3 | Available Data | 116 |
| 5.3.3.1 | List of Security Measures | 116 |
| 5.3.3.2 | Intrusion Prevention System Data | 119 |
| 5.3.3.3 | Incidents Data | 120 |
| 5.3.3.4 | Number of Corrupted Accounts by Phishing Attacks | 123 |
| 5.3.4 | Laplace Trend Values | 124 |
| 5.3.5 | Approach | 125 |
| 5.3.6 | Results | 129 |
| 5.3.6.1 | Impact of the Hire of an Analyst | 129 |
| 5.3.6.2 | Blocking of the Routing of Microsoft Protocols from Outside Campus | 140 |
| 5.3.6.3 | Installation of IPSs at the Border of the University | 142 |
| 5.3.6.4 | Wireless Networks Put Behind IPSs | 148 |
| 5.3.6.5 | Impact of a Communication Campaign | 152 |
| 5.4 | Summary | 157 |
| 6 | Model Description | 161 |
| 6.1 | Introduction | 161 |
| 6.2 | Model | 162 |
| 6.2.1 | Model Components | 162 |
| 6.2.2 | Model Characteristics | 162 |
| 6.3 | Qualitative Use of the Model | 168 |
| 6.3.1 | How to Use the Model to Decide Security Strategies? | 168 |
| 6.3.2 | How to Identify Causes of Security Issues? | 170 |

| | | |
|-------|---|-----|
| 6.4 | Discussion | 171 |
| 6.5 | Summary | 172 |
| 7 | Towards a Quantitative Model | 173 |
| 7.1 | Introduction | 173 |
| 7.2 | Approach | 175 |
| 7.3 | Attacker-Related Nodes as Parameters of the Model | 177 |
| 7.4 | Using the Model per Category of Assets | 182 |
| 7.5 | Security Team Expertise and Qualities | 186 |
| 7.6 | Security Awareness Communication | 189 |
| 7.7 | User's Risk Perception | 192 |
| 7.8 | Example | 194 |
| 7.8.1 | Overall Security | 194 |
| 7.8.2 | Using Facets | 199 |
| 7.8.3 | Facet 1: Servers | 200 |
| 7.8.4 | Facet 2: Phishing Attacks | 204 |
| 7.9 | Summary | 207 |
| 8 | Conclusions | 210 |
| 8.1 | Summary | 210 |
| 8.2 | Contributions | 213 |
| 8.3 | Future Work | 214 |
| A | Interview Questionnaire | 218 |
| B | Survey Questionnaire | 226 |
| C | Results of the Survey | 238 |
| D | Propagating Values in the Model | 244 |
| D.1 | Method | 244 |
| D.2 | Examples | 246 |
| D.2.1 | Example 1: Two Parent Nodes | 246 |
| D.2.2 | Example 2: Three Parent Nodes | 247 |
| D.2.3 | Example 3: Four Parent Nodes | 249 |
| D.2.4 | Example 4: Five Parent Nodes | 251 |
| | Bibliography | 254 |

List of Tables

| | | |
|-----|--|-----|
| 2.1 | Sample Qualitative Risk Determination Matrix | 22 |
| 2.2 | Sample Semi-Qualitative Risk Determination Matrix | 23 |
| 3.1 | Alternatives for Interviews | 59 |
| 4.1 | List of Characteristics Included in the Survey | 92 |
| 4.2 | Example to Find the Coefficient Associated to the User's Risk Perception for All Respondents | 93 |
| 4.3 | Ranked Coefficients | 97 |
| 4.4 | Characteristics and their Strength on Security | 98 |
| 4.5 | Characteristics and their Influences in Experts' Models | 102 |
| 5.1 | Campus Population between 2001 to 2010 | 117 |
| 5.2 | List of Security Measures Implemented at UMD | 118 |
| 5.3 | Data to Support the Comparison of the Speed of Incidents Detection over Four Years | 146 |
| 5.4 | Summary of the Validation with Case Studies | 160 |
| 6.1 | Characteristics found in the Literature | 164 |
| 6.2 | Characteristics of the User Component and their Description | 165 |
| 6.3 | Characteristics of the Threat Component and their Description | 165 |
| 6.4 | Characteristics of the Organization Component and their Description | 166 |
| 6.5 | Characteristics of the Asset Component and their Description | 167 |
| 7.1 | Attacker Profiles in the Model | 180 |
| 7.2 | Value of Security given Two Possible Values of Attacker's Motivations and Resources and Three Possible Values for Depth of Protection of the Asset | 181 |
| 7.3 | Example of Categories of Assets for a University Environment and Quantitative Value | 184 |
| 7.4 | Example of Categories of Assets for a University Environment and Qualitative Value | 185 |
| 7.5 | Example of Expertise and Qualities of the IT Security Team | 188 |
| 7.6 | List of Possible Awareness Measures | 190 |
| 7.7 | Examples of Awareness Measures in an Organization | 191 |
| 7.8 | Values of the User's Risk Perception based on the Number of Successful Phishing Attacks | 194 |
| C.1 | User's Risk Perception | 238 |
| C.2 | User's Trust | 238 |
| C.3 | User's Exposure to Security (for example through media) | 238 |
| C.4 | User's Theoretical Knowledge in Using Computers or/and in Security | 239 |
| C.5 | User's Experience in Using Computers or/and in Security | 239 |
| C.6 | User's Gender | 239 |

| | | |
|------|---|-----|
| C.7 | User's Age | 239 |
| C.8 | User's Place of Birth | 239 |
| C.9 | User's Role (if the user is an undergraduate/graduate student, a faculty, a staff, an intern, etc...) | 240 |
| C.10 | Security Awareness Communication to Users | 240 |
| C.11 | Management Understanding of Security Needs | 240 |
| C.12 | Security Team Talent | 240 |
| C.13 | Security Team Qualities (for example withstanding stress) | 240 |
| C.14 | Financial Resources Available for Security | 241 |
| C.15 | Available Security Hardware (for example security devices such as intrusion prevention systems) | 241 |
| C.16 | Available Security Software (for example patches, signatures) | 241 |
| C.17 | Risk Assessment Program | 241 |
| C.18 | Security Policies | 241 |
| C.19 | Organizational Attitude towards Security | 242 |
| C.20 | Threat Awareness | 242 |
| C.21 | Attacker's Motivations | 242 |
| C.22 | Attacker's Expertise | 243 |
| C.23 | Attacker's Qualities (for example perseverance) | 243 |
| C.24 | Value of the Asset from the Attacker's Point of View | 243 |
| C.25 | Value of the Asset from the Organization's Point of View | 243 |
| C.26 | Depth of Protection of the Asset (includes all protections of an asset - passwords, firewalls...) | 243 |
| D.1 | Values of the Child Node C based on Values of its Two Parents P_1 and P_2 in Example 1 | 247 |
| D.2 | Value of Security given Values of its Three Parent Nodes | 248 |
| D.3 | Value of "Depth of Protection of the Asset" based on Values of its Four Parents | 250 |
| D.4 | Value of "Depth of Protection of the Asset" based on Values of its Five Parents | 253 |

List of Figures

| | | |
|------|---|-----|
| 2.1 | Pyramidal Structure of the Domains of the ISO 27002 Standard . . . | 18 |
| 2.2 | Example of an IT Risk Assessment Methodology Flowchart | 21 |
| 3.1 | Positive and Negative Influences | 47 |
| 3.2 | Strong and Medium Influences | 47 |
| 3.3 | Validation through Case Studies | 51 |
| 3.4 | Diagram of the Model Development and Validation Processes | 57 |
| 3.5 | Interview Process | 60 |
| 3.6 | Survey Process | 63 |
| 3.7 | Components of the Survey | 66 |
| 4.1 | Model Developed at the University of Maryland | 76 |
| 4.2 | Model Developed by Expert 1 | 79 |
| 4.3 | Model Developed by Expert 2 | 80 |
| 4.4 | Model Developed by Expert 3 | 81 |
| 4.5 | Visit and Response Rates | 85 |
| 4.6 | Total Number of Years of Experience: Managerial versus Technical Positions of Respondents | 88 |
| 4.7 | Organization of Respondents: Managerial versus Technical Positions . | 89 |
| 4.8 | Confidence of Experts in the Decomposition and Description Users, Organization, Threat and Assets | 91 |
| 4.9 | Influence of Each Characteristic on Security | 94 |
| 4.10 | Limits between Strong, Medium, Low and No Influence | 96 |
| 4.11 | Flowchart of the Model Development Process | 99 |
| 4.12 | Process to Aggregate Several Influential Models? | 100 |
| 4.13 | Influential Matrix | 104 |
| 4.14 | Initial step (Step 0) of the Final Model Development | 107 |
| 4.15 | Model before Validation | 108 |
| 5.1 | Model Suggested by an Expert after Presentation of the Model De- veloped based on Interviews and Surveys | 112 |
| 5.2 | Model Validated by Experts | 113 |
| 5.3 | Laplace Trend Values for the Hire of the IT Security Officer in 2002 . | 131 |
| 5.4 | Laplace Trend Values for the Hire of an Analyst in 2005 | 133 |
| 5.5 | Cumulative Number of Incidents for Years from 2002 to 2007 | 134 |
| 5.6 | Cumulative Number of Incidents for Years 2002, 2004, 2005, 2006, and 2007 | 134 |
| 5.7 | Cumulative number of incidents for year 2003 | 135 |
| 5.8 | Laplace Trend Values for the Hire of an Analyst in 2006 | 135 |
| 5.9 | Mapping of the Hire of the Security Officer in 2002 to the Model . . . | 137 |
| 5.10 | Mapping of the Hire of the Security Officer in 2006 to the Model . . . | 139 |
| 5.11 | Laplace Trend Values for the Routing of Microsoft Protocols from Outside Campus in 2002 | 142 |

| | | |
|------|--|-----|
| 5.12 | Laplace Trend Values for the Installation of IPSs in 2006 | 144 |
| 5.13 | Comparison of the Percentage of Detected Incidents for the Month of September | 147 |
| 5.14 | Graphical Representation of the Network Address Allocation | 149 |
| 5.15 | Graphical Representation of the Network Address Allocation after the Wireless Networks are Put Behind IPSs | 150 |
| 5.16 | Laplace Trend Values for the Installation of Wireless Networks behind IPSs in 2007 | 151 |
| 5.17 | Laplace Trend Values for the Number of Successful Phishing Attacks at UMD from April 10, 2008 to September 12, 2008 | 154 |
| 5.18 | Laplace Trend Values for the Number of Successful Phishing Attacks at UMD from May 15, 2008 to September 12, 2008 | 155 |
| 5.19 | Laplace Trend Values for the Number of Successful Phishing Attacks at UMD from June 28, 2008 to September 12, 2008 | 156 |
| 6.1 | Final Model | 163 |
| 7.1 | Attacker's Motivations, Resources, and Depth of Protection of the Asset in the Model | 180 |
| 7.2 | Five-Step Method to Use the Model | 195 |
| 7.3 | Model with Pieces of Evidence Gathered in an Organization | 198 |
| 7.4 | Six-Step Method to Use the Model within a Facet | 201 |
| 7.5 | Model with Pieces of Evidence for Servers | 203 |
| 7.6 | Model with Pieces of Evidence for Phishing Attacks | 206 |
| D.1 | Child Node with n Parent Nodes | 245 |
| D.2 | Example of Two Parent Nodes | 246 |
| D.3 | Example of Three Parent Nodes | 248 |
| D.4 | Example of Three Sets of Evidence | 249 |
| D.5 | Example of Four Parent Nodes | 250 |
| D.6 | Example of Three Sets of Evidence | 251 |
| D.7 | Example of Five Parent Nodes | 252 |

List of Abbreviations

| | |
|------|--|
| ALE | Annualized Loss Expectancy |
| ARO | Annual Rate of Occurrence |
| BBN | Bayesian Belief Network |
| CEO | Chief Executive Officer |
| CIO | Chief Information Officer |
| FBI | Federal Bureau of Investigation |
| IDS | Intrusion Detection System |
| IPS | Intrusion Prevention System |
| IT | Information Technology |
| OIT | Office of Information Technology |
| SANS | SysAdmin, Audit, Network, Security institute |
| SLE | Single Loss Expectancy |
| SRM | Security Risk Management |
| SSN | Social Security Number |
| UC | University of California |
| UMD | University of Maryland |
| URL | Uniform Resource Locator |
| VP | Vice President |

Chapter 1

Introduction

1.1 Context: The Importance of Managing Security

For the last years, Information Technology (IT) security has been a major concern for organizations, as successful cyber attacks can lead to costly consequences for organizations, such as the theft of sensitive information for the company or for users. In this section, three stories illustrate some reasons that explain the success of cyber attacks: a successful denial of service that targeted Yahoo and shut it down for several hours, the theft of sensitive information of users on their medical records, and the case of a user falling for a phishing attack that resulted in the compromise of Chinese activists' accounts.

On February 7, 2000, an attacker launched a denial-of-service attack against Yahoo: routers that connected the Yahoo website to the rest of the Internet were overloaded with fake traffic. This resulted in the non-availability of the Yahoo website to users for three hours [8]. The following day, the same attack successfully targeted Buy.com, which had its initial public offering on NASDAQ market that morning, Ebay.com, CNN.com, and Amazon.com [7]. The day after, ZDNet, E*Trade and Excite were then attacked. The direct consequence of these denial-of-service attacks is a complete shutdown of the websites for several hours, resulting in a loss of money for companies.

In April 2009, a restricted database on a computer of the health services center at the University of California (UC), Berkeley, was attacked [9]. According to the 2009 report of the Educational Security Incidents [42], this database contained highly sensitive information on more than 160,000 former and current students at UC Berkeley and Mills College. It included social security numbers, health insurance information, and immunization records. The affected database was taken offline to prevent any further attacks. Mails and emails were sent to people whose information could have been stolen. Although there was no proof that the attack intended to steal this specific information, there was still an attempt to access information that should not have been accessed by a third party. Numerous examples of attacks intending to steal credit card numbers, social security numbers, or credentials exist. In this story, there could have been major consequences related to the confidentiality of individuals' personal information.

In January 2010, Google disclosed that intruders had stolen information from their computers [10]. More precisely, in December 2009, the intruders sent instant messages through Microsoft Messenger Program to an employee of Google in China. The employee clicked on a link that was included in the messages and inadvertently allowed the intruders to access his/her own computer and then, computers at Google in Mountain View, USA. The objective was to access Gaia, which is the famous Google software that enables users to access a range of services with one unique password. The intruders successfully retrieved passwords to access email accounts of two human rights activists in China. Later, Google discovered that dozens of Gmail accounts of other advocates of human rights in China were routinely accessed,

through phishing scams or malware placed on the users' computers [11]. This event had broad repercussions: Google decided to shut down Google China. This story emphasizes two aspects of cyber security: malicious attackers steal information on purpose, and a user fell for social engineering.

Several conclusions can be derived from these three stories. First, successful attacks can lead to severe consequences for companies (Yahoo, Amazon), specific individuals (such as human rights activists in China), or users in general. They include loss of credit card or social security numbers, and shut down of companies. Therefore, organizations need tools to manage IT security to prevent such attacks. Second, these attacks were successful because of two causes: either attackers who intend to harm organizations or users, or a careless user, falling for social engineering attacks. Consequently, humans play an important role in these attacks. In this context, how can organizations ensure security of their systems? In addition, could these attacks have been prevented? There is no easy answer to these questions because IT security is a field where many variables interact. The next section presents challenges related to the IT security field.

1.2 The Issues in IT Security

1.2.1 The Lack of Available Sound Security Data and Metrics

The context of managing IT security is different from managing risk in fields such as the nuclear or aeronautic fields. Two main reasons support this observation. The first reason is the lack of available, meaningful data. Meaningful data are data

that have a meaning for IT security management. Most organizations gather logs of their network activity, which include incidents data or raw data collected by security devices such as intrusion prevention systems. However, organizations are reluctant to share them. The first reason to explain this is that these data contain personal information on users. Through the IP address, the user could be tracked and his/her habits could be determined. Second, organizations are hesitant to disclose the types of successful attacks targeting their organizations and their numbers. This gives the image that the organizations network is unsecure and organizations are not willing to give this image.

Although organizations collect a vast amount of data, data are often raw data and would need interpretation. The issue is that there is no accepted definition of security terms and no agreement on what metrics should be considered for security. For instance, vulnerability, threat, and risk have different meanings from one person to another [53]. Besides, there is no common tool for organizations to exchange data. PREDICT, the Protected Repository for the Defense of Infrastructure against Cyber Threats [4], is a centralized repository of network operations data for research in IT security and is a first step towards a solution for sharing security data. However data made available by PREDICT do not include specifics on the organization (security culture in the organization, size of the IT security team), details on the users (types of users), or on the data collection (for instance the configuration of the intrusion detection system that collected data). As a result of these two facts, it is difficult for organizations to exchange data, leading to a lack of available data.

Another reason that makes managing IT security challenging is the non-

controlled environment. In the case of a failure in a nuclear power plant, conditions of the environment at the instant of the failure can be investigated and a precise scenario can be built, such as in the Three Mile Island accident [23]. In security, it is often impossible to trace back the scenario that led to a successful attack as it is often impossible to find the exact cause that led to a successful cyber attack. For example, if the number of corrupted computers has increased in an organization, it may be due to several reasons: there were more attackers, users did not perceive risks, or a breach in a software was recently discovered. There is not enough information about the context to rule out one of the possible causes of the corrupted computers.

Due to the context of lack of available, meaningful data and metrics, and incomplete information about the context, it seems difficult to efficiently manage security. However, although incomplete, available information allows drawing conclusions on the level of security of an organization and deciding how to make decisions and invest in security.

1.2.2 Managing Security

Frameworks to assess security and manage security already exist. Organizations have the possibility to use IT risk assessment frameworks ([12], [13], [45], [90], [118]), which are inspired from traditional risk assessment methodologies. In these frameworks, threats are identified and the likelihood that the threat is successful and the threat impact are evaluated. These two quantities can be evaluated qual-

itatively or quantitatively. On the one hand, qualitative risk assessments can be accomplished quickly but the conclusions are not as accurate as the conclusions that can be drawn with a quantitative risk assessment. On the other hand, the feasibility of quantitative risk assessments is questionable: experts need to identify all threats and assess the likelihood that the threat is successful as well as the threat impact. Aside from being a time-consuming task, organizations often do not have the data to support such metrics.

Economic frameworks have also been applied [116]. Approaches to analyze security investments and how to invest in security can be based on cost-benefit or return on security investments methodologies ([30], [37]). A cost-benefit analysis can be conducted to determine if it is worth implementing a security solution. One could also investigate another strategy that would mitigate the risk but would cost less. A famous economic model is Gordon and Loeb's model that determines the optimal amount to invest in security [57]. This model allows identifying how to invest in security but applying the model is still challenging for security teams. Indeed, customizing the model for specific companies and collecting data to populate the model are difficult tasks.

Although frameworks to assess IT security are numerous, organizations are reluctant to use them because of their applicability. As a result, IT security officers often end up using best practices to manage security.

1.2.3 Communication

Results of security assessments can be misleading. Let us consider the case where security incidents in organizations are recorded: they are based on IT security officers noticing abnormal behavior on the network. In other words, the number of incidents is potentially limited by the number of people allocated to work on the task of incidents identification. More precisely, if the number of incidents is increasing, it may mean that the organization is more vulnerable to attacks or that more resources (time and staff) were allocated to identify incidents. Miscommunication is therefore an issue in IT security. Moreover, people who make decisions are often not people who actually deal with security (i.e. IT security officers) [44]. There may be a lack of communication or miscommunication between decision makers and IT security officers. As a result, there is a need for a framework that would be a solid basis for communication purposes between decision makers and IT security officers.

1.2.4 The Human Element

Including the human element in security has been an increasing trend ([56], [102]). Schneier stipulated that the user is the weakest link and that security is “as good as its weakest link” [102]. Social engineering is becoming a famous mean of attack to steal users’ credentials [83]. Phishing is one of the numerous techniques of social engineering, in which an attacker (called phisher) sends an email that appears to be from a legitimate sender (bank for example) asking a user to enter his/her identification number and password. Usually, the email contains a link

towards a fraudulent web page that appears to be the user's bank home page. When information is entered by the user, the phisher collects these data for future fraudulent purposes. In this context, an organization can install many devices but it may not totally prevent phishing attacks from being successful.

Another example of potential security breach related to users is the use of passwords. Some users tend to use easy passwords (such as their username, "password", or "1234") because they are easier to remember. These easy passwords are also the first passwords attackers will try to hack a user account. To cope with this issue, organizations are advised to impose a strong password policy, as recommended in [93]. Organizations (IT security team and managers) definitely play a key role in defending their network by making users sensitive to phishing attacks or by imposing a password policy (minimum number of characters, letters versus numbers, lower case versus upper case letters).

The organizations' objective is to protect their network and systems from malicious activity. Behind every malicious activity, a human attacker is hidden: social engineering, virus, denial of service. Attackers' objective is to harm an organization or users. Their motivations can be diverse: some attackers want to steal users' credentials, others launch attacks for fun.

The examples cited in this section show that the human elements play a major role in security. While making decisions for security, the human elements (user, attacker, organization through managers and IT security team) need to be taken into account.

1.3 Approach

In the first section, we presented examples of successful attacks to motivate the need of managing IT security to prevent severe consequences for users and organizations. In the previous subsections, we identified several issues in IT security. First, there is a lack of available, meaningful data and metrics. Second, managing IT security is challenging because current frameworks require many resources (time and people) and are not easily applicable. Third, we emphasized the difficulty of communication between IT security officers and managers. Finally, we showed that the human element plays a major role in IT security, through users, attackers, or security officers.

Therefore, we aim at providing security officers with a model of IT security that focuses on the human element, provides recommendations on metrics, and facilitates communication. Our model includes human elements that are involved in security, that is to say, the attacker, the user, and the organization. We consider four major components of security: attacker, user, organization, and asset. We identify key characteristics for each of the four components, and the interactions between them. The characteristics and their interactions were mainly determined through expert opinions, which rely on three sources: 1) we had months of discussion with the Director of Security at the University Maryland (UMD), who has over fifteen years of experience in dealing with IT security issues at a large public university and who is, through frequent interactions with his colleagues at other universities nationwide, also very familiar with security issues at other US universities, 2) we

interviewed two experts at other universities for a duration of two hours, and 3) we conducted a survey and had fifteen responses. Interviews allowed modifying the four original components to the following decomposition: threat, user, organization, and asset. The model depicted in this dissertation is validated in two ways. It has been first validated qualitatively by experts. Besides, it has been partially validated with available data collected at UMD. The partially validated model can be used in a qualitative manner for communication purposes: the visual and easy-to-interpret representation of the model facilitates communication between IT administrators and managers.

In this dissertation, we also provide suggestions on how to quantify characteristics in the model. We raise the issue that characteristics may not be directly quantified with collected data. To cope with this major issue, we propose the use of indicators to help the quantification process. In both the direct and indirect quantification, we suggest the use of data collected in organizations. More precisely, we provide detailed recommendations on selected characteristics.

1.4 Contributions

This research introduces an approach for developing and validating a model for IT security decision making that improves reasoning and communication among stakeholders (managers and IT security officers). Examples of questions that the model can answer include:

- Should the organization communicate more on security-related risks to users

or pay for seminars to increase the IT team knowledge?

- What will have more impact on security: educating users, buying new security devices or hiring people to deal with security?

Specifically, the contributions of this research are:

- Development of an approach for a model for IT security decision making that includes major characteristics of security and influences among them: This approach relies on involving experts through interviews and surveys,
- Identification of the relevant components of security: Besides the assets (technical system), the model identifies the stakeholders who play a role in security, including the attacker, the user, and the organization,
- Identification of the components' characteristics: The model identifies key characteristics of the previously identified components that particularly impact security, such as the expertise of the security team or the awareness of the user,
- Identification of the impact of characteristics on one another: The model identifies the interactions between characteristics. A characteristic can positively or negatively impact another characteristic. The model also identifies the strength of these influences,
- Suggestion of an approach for model validation in IT security, based on actual security data: Data collected at UMD are used to partially validate the model. They include security logs, such as incidents, and a list of implemented security measures. The objective is to compare the rate of incidents before and after the

implementation of a measure and compare these conclusions to the outcomes of the model,

- Qualitative assessment of security: By identifying the influences among characteristics, it is possible to modify one characteristic and see how the change propagates through the model. This approach aims at facilitating communication between IT administrators and decision makers,
- Step toward quantitative measurements for security: We provide directions on identifying measurements of characteristics.

1.5 Outline

This dissertation is organized as follows. Chapter 2 provides the background related to three topics. First, we discuss existing frameworks for managing IT security and show the limitations of such frameworks. Second, we present what has been done to identify characteristics related to human elements that could be relevant to one of the three stakeholders involved in security: attacker, user, and organization. Third, we discuss the issue of model validation and present the literature supporting model validation.

In Chapter 3, we detail the approach taken to develop and validate a model for managing IT security. In the model, we identify characteristics related to the components of security and the causal influences among them. Identification of these characteristics and relationships is based on expert opinions. The processes of face-to-face interviews and web-based surveys are detailed in this chapter. The difficulty

implied in model validation is raised and suggestions for model validation are made: model validation is based on experts' elicitation and case studies developed at UMD.

The results of the model development are provided in Chapter 4. Results of the interviews and surveys are presented. A model is derived from these insights.

Chapter 5 presents the validation of the model. It relies on validation by experts and validation of parts of the model through case studies developed at UMD. Security data collected at UMD before and after the implementation of measures allow validating impacts of characteristics on security in the model.

In Chapter 6, we present the partially validated model. We provide description of components and characteristics. We also show how the model can be used in a qualitatively manner to facilitate communication between IT security officers and managers.

Chapter 7 presents a step towards the quantitative measurement of characteristics in the model. We select several characteristics and suggest measurements for them. We introduce the concept of facets to show that the model can be used to manage the overall security but also to focus on a specific asset category or attack type.

Chapter 8 concludes this dissertation. We show how the presented model addresses the issues highlighted in the introduction and provide insights into future work.

Chapter 2

Related Work

2.1 Introduction

In this chapter, we present the background related to three topics. First, we provide a literature review on methods for IT security management. IT security teams often use ad-hoc assessments to manage security: they base their assessments on empirical evaluations of their networks and systems. Such approaches are fuzzy and methods are suggested to cope with this issue. They include risk assessment techniques, inspired from traditional risk assessment approaches, and cost-benefit analyses. We present these methods in the first section of this chapter and highlight their major problems: applicability and ease of communication.

In the second section of this chapter, we highlight the recent trend in IT security which is to consider the human element as a major stakeholder of IT security. Human elements include attackers, users, IT security officers, and managers. We present a literature review that supports the characterization of these elements and the quantification of their behavior.

In the third section, we introduce the related work associated to validating a model. Validating a model may rely on two resources: experts and data. Several techniques involving these two resources exist and techniques that could be useful in our study are documented.

Finally, we expose the approach taken to develop a model for managing IT security. Our model aims at providing IT security teams with a tool to discuss with managers on what security measure to implement, that is easy to use. This model focuses on the human element, which is often considered to be the weakest link in security. The model is developed and validated with two sources of information: experts and data.

2.2 Managing security

2.2.1 Ad-hoc assessments

Most organizations base their assessments on empirical assessments done by their IT security staff. In other words, the IT team is able to say that security has increased because fewer attacks are observed, or that security has decreased because more computers in the organization are corrupted. Deciding what security solution to implement often relies on a trade-off between the cost organizations are willing to invest in security and the best decision security wise.

This is not a rigorous method. This method of assessing security may work in small organizations. However, in large organizations, such an assessment cannot be used between security administrators and managers to make security decisions. Communication between the two parties is difficult because there is no framework on which to base the justification of implementing a solution versus another one.

2.2.2 Self Assessments

Swanson suggests a self-assessment questionnaire to assess organizational security [112]. Several controls are inspected (management, operational, and technical controls): for each of them, a set of questions needs to be answered according to a five-level scale. The five levels are the following:

- Level 1: Control objective is documented in a security policy,
- Level 2: Security controls are documented as procedures,
- Level 3: Procedures have been implemented,
- Level 4: Procedures and security controls are tested and reviewed,
- Level 5: Procedures and security controls are fully integrated into a comprehensive program.

Once the questionnaire is completed, the organization can determine what needs to be done to achieve an objective of level 3 for example. This method is easy to implement but it does not seem able to justify the implementation of a security solution over another one.

2.2.3 Standards and Regulations

Best practices are implemented in response to the “problem of standardization where subjective judgments may cause variations in design and implementation” [65]. Best practice frameworks help organizations assess security risks, implement

security controls, and comply with governance requirements. ISO 27002 (formerly ISO 17799 [79], [97]) is an information security standard published by the International Standard Organization which provides best practices for organizations on information security management. This standard originated from the British standard BS 7799. Organizations can be audited and become ISO 17799 compliant. The standard contains the following domains:

1. Security policy,
2. Organization of information security,
3. Asset management,
4. Human resources security,
5. Physical and environmental security,
6. Communications and operations management,
7. Access control,
8. Information systems acquisition, development, and maintenance,
9. Information security incident management,
10. Business continuity management,
11. Compliance.

Each domain contains one or several control objectives and one or more controls that can be applied to achieve the control objectives. These domains cover

organizational, technical, and physical aspects. Saint-Germain provides a schematic top-down structure that includes these domains and that shows that their impact is felt from the management or organizational level to the operational level [97]. This structure is shown in Figure 2.1.

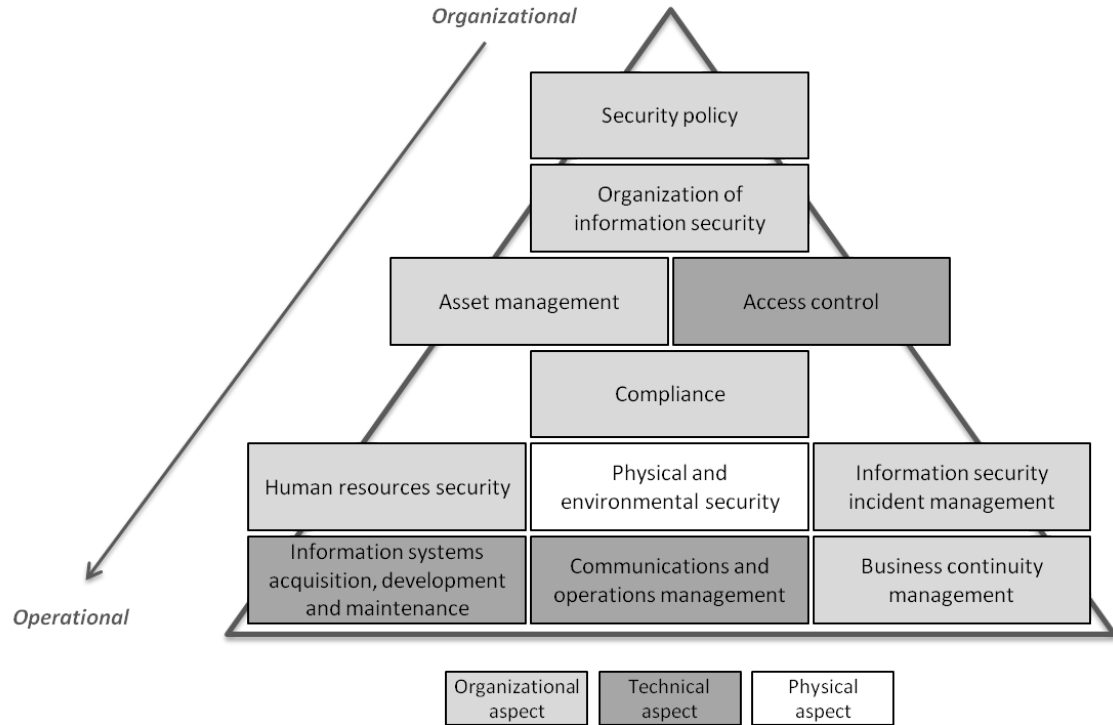


Figure 2.1: Pyramidal Structure of the Domains of the ISO 27002 Standard

Standards are not useful to all organizations. On the one hand, it is useful for e-commerces to be certified so that customers are ensured that the organization complies with governance requirements. On the other hand, standards are not flexible enough for organizations such as universities, where policies cannot be as much enforced as in governmental agencies for example. In addition, standards do not allow deciding among alternatives, what security solution to implement.

2.2.4 Security Risk Assessments

In order to cope with the fuzziness of empirical approaches, frameworks to assess security and decide how to invest in security have been developed. IT risk assessments are based on traditional risk assessments. Examples of proposed risk assessment methodologies are [12], [13], [25], [45], [90], [109], [118]. For instance, Aagedal et al. propose guidelines for each step of the risk assessment process [12]. Especially, the authors suggest how to implement traditional risk assessment techniques (e.g. Hazop method, fault tree analysis) to risk assessment for information systems. However the scope of this work is mainly the security-critical systems such as an e-commerce website.

A typical IT risk assessment consists in 1) defining the system, 2) identifying the threats on the system and the vulnerabilities the system is exposed to, 3) calculating the risk by multiplying the likelihood that a threat is successful and the threat impact (or criticality or severity), and 4) recommending controls.

These terms are defined in different ways, the following being examples [109]:

Threat: “The potential for a threat-source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.”

Threat-source: “Either (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability.”

Vulnerability: “A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered

or intentionally exploited) and result in a security breach or a violation of the system's security policy.”

The steps of an IT risk assessment are shown in Figure 2.2 (inspired from [109]). Step 1 identifies the scope of the risk assessment. For example, boundaries of the IT system, its resources (hardware, software, and human), and information to protect are identified. The output of step 2 is a list of threat-sources that could exploit a specific vulnerability in the organization and a list of vulnerabilities that could be exploited by threat-sources. Step 3 can be done qualitatively or quantitatively. For instance, qualitative assessment consists in assigning a low, medium or high value to the likelihood that a specific vulnerability is successfully exploited by a threat-source and to the threat impact ([13] and [45]). A risk determination matrix allows determining the risk given an assessment of the likelihood and the impact (Step 4). Table 2.1 (from [45]) shows a sample risk matrix suggested by the SysAdmin, Audit, Network, Security (SANS) institute. A semi-qualitative assessment would consist in assigning a number to the likelihood and to the impact rather than a low, medium or high value [109]. A sample risk level matrix for semi-qualitative assessment is shown in Table 2.2 (from [109]). Quantitative risk assessments use the Annualized Loss Expectancy (ALE): this approach is discussed in the next subsection.

After computing the risk (using a qualitative, semi-qualitative or quantitative risk assessment), decision makers can decide what strategies to adopt to mitigate risks (Step 5).

The best strategy for organizations is a trade-off between 1) the cost organizations are willing to pay for security and 2) the best decision security wise.

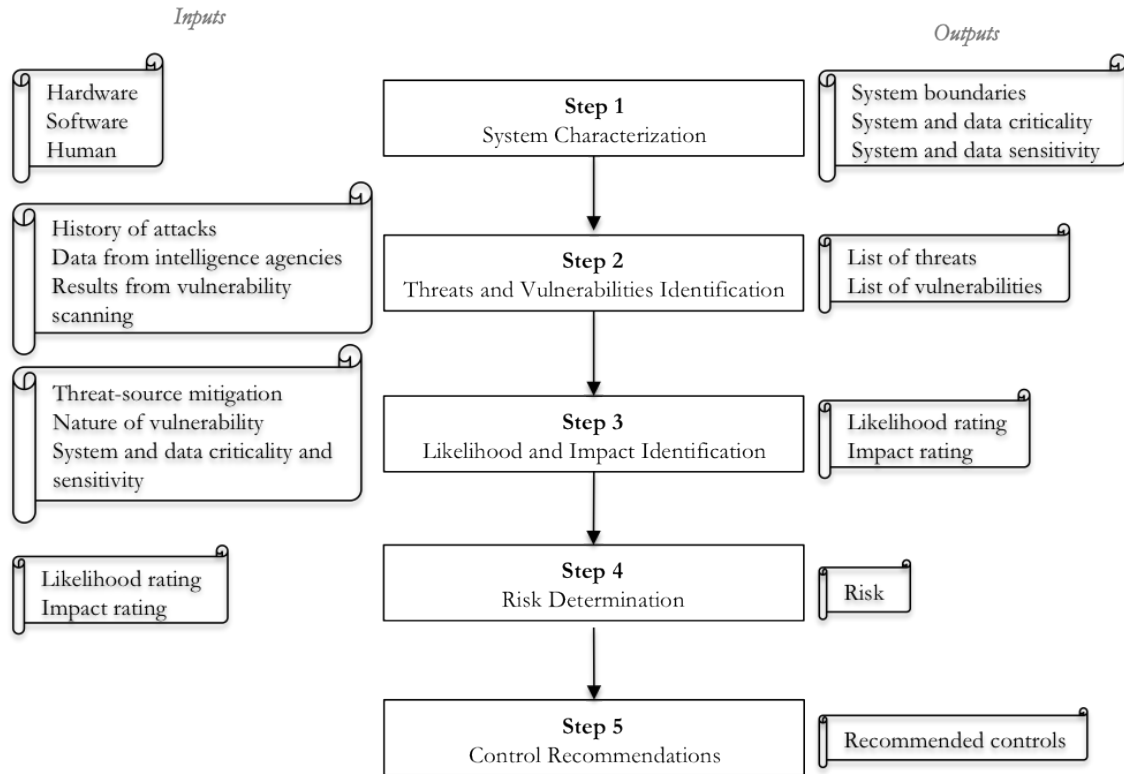


Figure 2.2: Example of an IT Risk Assessment Methodology Flowchart

Limitations are encountered in IT risk assessments:

- **Applicability:** Developing a risk assessment in an organization is resource demanding. Not only do system administrators need to identify threats and vulnerabilities, they also need to identify a frequency of occurrence and a gravity factor (to be linked with the value of losing an asset). Especially for large organizations, risk assessments require that many experts are involved in the process, and that many threats are covered, resulting in a non-manageable number of threat scenarios,
- **Communication:** Results of risk assessments need to be communicated to a variety of people, including security team, decision makers, managers, and

Table 2.1: Sample Qualitative Risk Determination Matrix

| | | Impact | | |
|------------|----------|----------|----------|----------|
| | | Low | Moderate | High |
| Likelihood | Low | Low | Low | Moderate |
| | Moderate | Low | Moderate | High |
| | High | Moderate | High | High |

users, and it is sometimes difficult to convey results of risk assessments to people.

2.2.5 Economic Approaches

Economic approaches have been recently used to assess security. A cost-benefit analysis can be conducted to determine whether it is worth implementing a solution. On the one hand, the cost of implementing a specific strategy is evaluated. On the other hand, the benefit of implementing such a solution is calculated. If the cost is higher than the benefit, the strategy is not implemented. On the contrary, if the benefit is higher than the cost, the strategy may be considered for implementation. One could also investigate another strategy that would mitigate the risk but would cost less. If the cost is equal to the benefit, the organization gains no advantage in implementing it.

One of the most famous economic approaches is the Annualized Loss Expectancy (ALE) approach. The ALE represents the risk of losing an asset because

Table 2.2: Sample Semi-Qualitative Risk Determination Matrix - Risk Scale: High (from 50 to 100), Moderate (from 10 to 50), Low (from 1 to 10)

| | | Impact | | |
|------------|----------------|------------------------|-----------------------------|------------------------------|
| | | Low (10) | Moderate (50) | High (100) |
| Likelihood | High (1.0) | Low $10 * 1.0 = 10$ | Moderate $50 * 1.0 = 50$ | High $100 * 1.0 = 100$ |
| | Moderate (0.5) | Low $10 * 0.5 = 5$ | Moderate $50 * 0.5 = 25$ | Moderate $100 * 0.5 = 50$ |
| | Low (0.1) | Low $10 * 0.1 = 1$ | Low $50 * 0.1 = 5$ | Low $100 * 0.1 = 10$ |

of a successful threat. For that matter, it is often used for quantitative risk assessments. The ALE is defined as the product of the the Annual Rate of Occurrence (ARO), which is the frequency for losing an asset, by the Single Loss Expectancy (SLE), which is the value in dollars of the loss of the asset:

$$ALE = ARO * SLE \quad (2.1)$$

Gordon and Loeb propose an extension of the ALE approach by defining the expected loss as [57]:

$$E = \lambda * t * \nu \quad (2.2)$$

Where λ is defined as the loss given a successful breach, t as the probability

that a threat occurs, and ν the vulnerability, which is the probability that once a threat occurs, the attack is successful. Gordon and Loeb’s approach aims at determining the optimal monetary amount to invest in security. The authors model the security breach function as being dependent on the amount spent in protecting assets. They show that there is an optimal amount decision makers should invest in security. This theoretical approach does not provide hints on how to decide among security solutions.

Soo Hoo presents a decision-analysis-based, ALE framework that allows to make a decision between several security alternatives [65]. His approach is based on the identification of additional benefit and cost inherent to the implementation of a given policy with respect to a baseline situation. Soo Hoo raises the issue of dearth of data but does not explicitly explain how data can be used in his framework.

Schechter suggests a measure of security strength based on economics [100], where a market price to discover a new vulnerability is introduced as a measure of the security strength for software without known vulnerabilities. This work has the potential to help decision makers in ranking software based on a common security metric. However, the scope of this work is limited to software security. In addition, gathering data to estimate the market price to discover new vulnerabilities requires developers to be involved and so this approach has limited applicability.

Other economic approaches include the Return on Investment (ROI), the Return On Attack (ROA) [37], the Internal Rate on Return (IRR), and the Return On Security Investment (ROSI) [107]. The intuitive ROI is defined as the difference between the ALE before and after the implementation of a security measure divided

by the cost of the measure. Cremonini and Martini believe that this definition lacks to consider the attacker's interests [37]. They suggest the coupled use of the ROA with the ROI. The ROA captures how the attacker's behavior changes with the adoption of a security measure by the organization. It is defined by the ratio of the gain he/she expects from a successful attack and the losses he/she encounters due to the implementation of the security measure.

The Return on Security Investment (ROSI) metric is based on three quantities: the risk exposure RE, which is the dollar amount of losing an asset, the solution cost SC, which is the cost of implementing the solution, and the percentage of mitigated risk PRM, which is the expected mitigation after the implementation of the measure. It is defined as:

$$ROSI = \frac{(RE * PRM) - SC}{SC} \quad (2.3)$$

Gordon and Loeb strongly argue with the use of the ROI and ROSI metrics because of two inherent assumptions that are rarely met in reality: the investment must produce a constant return each year, and accounting profits must coincide with cash profits [58]. They introduce the Internal Rate on Return (IRR), based on the initial cost C_0 , and the cost C_t and benefit B_t in year t :

$$C_0 = \sum_{t=1}^n \left(\frac{B_t - C_t}{(1 + IRR)^t} \right) \quad (2.4)$$

If the IRR is greater than the discount rate or cost of capital k , which is the minimum rate a project needs to earn so that the organization's value is not

reduced, the solution should be implemented whereas it should not be implemented if the IRR is less than k .

These economic approaches are, without doubt, the methods that decision makers are the most familiar with. Their quantitative nature allows a quantifiable comparison among security solutions. Besides, accounting for the cost of a security solution when making decisions is a major concern for managers. However, despite the unquestionable advantages of these measures, the inherent criticism is how to gather data to calculate these measures, and what data to use. As discussed before, calculating the ALE requires that one assesses the monetary value of losing an asset, which is made challenging for intangible assets. The probability of a threat occurring or the losses an attacker sustains are other examples of quantities difficult to evaluate.

2.2.6 Frameworks for Decision Making

Bodin et al. suggest using the Analytical Hierarchy Process to rank security solutions and decide the optimal allocation of budget [22]. First, the organization identifies criteria and sub-criteria they want to take into account when making a decision, and assign weights to each criterion and sub-criterion. These include confidentiality, data integrity, and availability. Then the organization investigates several alternatives. Each alternative is evaluated against each criterion by using an intensity measure that captures how well an alternative accomplishes a criterion. At the end of the process, each alternative is assigned a score between 0 and 1, 1

being the perfect score and therefore the optimal alternative. This approach has the advantage of comparing criteria, sub-criteria and alternatives and can facilitate decision making. However, a decision maker is needed along the entire process to choose criteria and sub-criteria, assign weight, make evaluations to derive a ranking of the alternatives. Providing a composite score hides the fact that this approach heavily relies on the subjectivity of an expert.

Houmb presents a framework for making security decisions. Her work describes a tool that supports decision makers in choosing one or a set of security solutions among alternatives [66]. The approach is called the Aspect-Oriented Risk Driven Development (AORDD) Framework and combines Aspect-Oriented Modeling (AOM) with Risk Driven Development (RDD) techniques. The AORDD Framework is composed of seven components, including the AORDD security solution trade-off analysis and the trust-based information aggregation schema. This work also presents two types of information: observable, empirical, or objective information and subjective or interpreted information through experts. This framework originates from the traditional risk assessment approach and incorporates the ability of qualitative and quantitative assessments. Parameters are derived and scores can be calculated. The issue when using aggregate scores is that information may be hidden behind the unique score. This work focuses on decisions at the low level: for example, a solution considered against Denial-of-Service attacks is to develop a filtering mechanism. This work does not incorporate decisions at a higher level, such as the installation of a new security device on the organization's network. In addition, it is unclear how the framework helps in a real environment for making decisions: Houmb uses

the example of honeypots as empirical data but does not mention how organizations can use her framework and use their own empirical data.

2.2.7 Decision Theory and Game Theory Approaches

Cavusoglu et al. criticize the regular approach of making information security decisions [32]. According to the authors, the fact that decisions made by the organization affect the attitude of an attacker (for instance presence of intrusion detection systems has an effect on preventing the attackers from harming an organization [31]) questions the use of traditional decision making approaches. In this context where the two parties make decisions and each decision may impact the other party's decision, the authors study two approaches: decision theory and game theory. More specifically, they compare three situations: 1) the firm assumes that its decision has no impact on the attacker (decision theory), 2) the firm makes its decision by anticipating the attacker's behavior through a simultaneous game where the firm and the attacker make respectively the investment and the effort simultaneously, and 3) the firm makes its decision by anticipating the attacker's behavior through a sequential game where the firm first makes an investment, then the attacker makes the effort after learning the the firm's decision. Simulations show that the maximum payoff for the firm is obtained in a sequential game. This study remains theoretic as no directions are provided to show how decision theory or game theory can be used to make decisions in practice.

2.2.8 Adversary-Based Evaluations

Qualitative evaluations based on the threat include MITRE-developed cyber preparedness (Cyber Prep) framework [21] and Sandia Threat Analysis Framework [43]. Cyber Prep provides an approach organizations can use to identify their level of preparedness to threats on a scale of five levels. Although the methodology provides sample safeguards, it does not provide guidelines on what measures to implement nor provide a method to compare security solutions. Sandia Threat Analysis Framework presents a threat matrix which identifies eight levels based on measurable quantities, such as intensity, stealth, time, technical personnel, cyber and kinetic knowledge, and access [124]. Both MITRE and Sandia frameworks are qualitative and do not provide guidelines on how to choose the safeguards to implement to protect the organization.

The Mission-Oriented Risk and Design Analysis (MORDA) methodology, by the US National Security Agency and described in [46] and [47], assesses the system's security risk by calculating attack scores based on attack characteristics, adversary preferences, and mission impact. Comparison of security alternatives is possible through the relative change in security, cost, and performance.

The Network Risk Assessment Tool (NRAT) is another adversary-based evaluation [122]: it is a high-level tool to identify attacks against information systems that is based on the likelihood of an adverse event occurring and of the severity of the impact. The likelihood is evaluated based on a series of questions of major attributes of the attacks and the threat actors while the severity is assessed based

on the identification of the impacts of the attacks on security and on services.

LeMay et al. present an ADversary VView Security Evaluation (ADVISE) method to quantitatively evaluate a system’s security [75]. It is based on the characterization of the system through an attack execution graph, characterization of the adversary, and definition of relevant metrics that will be useful for the analyst to make security decisions. A stochastic model that describes how likely an attack happens is generated from these elements, and the execution of the model leads to answers for the analyst on the likelihood that an adversary adopts an attack path.

The aforementioned adversary-based evaluations is labor intensive as it requires the collaboration of several experts to identify attack paths and quantify them. As a result, they are not often used for decision making [123].

Red teaming is another adversary-based approach that is, to some extent, more used than the previous approaches. Red teaming is defined as “a process designed to detect network and system vulnerabilities and test security by taking an attacker-like approach to system/network/data access” [89]. More precisely, red teams are composed of third-party individuals, who have the knowledge, expertise, and resources of hackers, and who are granted authorization by an organization to discover vulnerabilities in their systems and network. Red teams use tools to probe for vulnerabilities and launch attacks against these vulnerabilities. This approach is more in-depth than attacks launched by hackers: most of the time, attackers need to find only one vulnerability in a system to launch an exploit against it whereas red teams identify an exhaustive list of vulnerabilities and try to exploit them. The scope of red teaming depends on the needs of the organization: although red teaming can

be used to identify all vulnerabilities, it can also focus on specific portions of the network. Once vulnerabilities are identified, the organization can make decisions to handle these vulnerabilities. Although an organization may benefit from red teaming, it is challenging to conduct one: the security team in the organization should be aware of the test in order not to stop the red team. While realistic, the test may not be representative of the actual attacks targeting the organization.

2.2.9 Model-based Approaches

Kotulic and Clark try to build a conceptual model for security risk management (SRM) [72]. The authors emphasize the importance of incorporating the human element as they can cause security breaches or make risky decisions that impact an organization's response to threats [64]. The framework identifies several characteristics, including organization characteristics (SRM program posture, IT resource posture, organization posture, contextual factors), management characteristics, executive management support, SRM program effectiveness. Their model focuses on the organization and does not include other components, such as the attacker. The authors do not explain how the model can be practically used to manage security. The authors attempted validating some relationships in their model with surveys sent to 1540 respondents in 23 firms. They reached a response rate of 1.6%. The authors discuss reasons that explain such a low response rate: information security is one of the most intrusive field and there is a mistrust of anyone who tries to understand the actions of security practitioners.

System dynamics has also been used to model organizational security. Rosenfeld et al. suggest a systemic approach to model enterprise security based on archetypes [95]. This intended approach includes not only machines but also human characteristics (security administrators and users). This work is the right approach towards a simple model to reason about security. However, it simplifies influences to two possible impacts: increase or decrease. For example, if factors A and B increase factor C, system dynamics does not allow to decide between factors A and B, the one that is going to have the most influence on factor C.

2.2.10 Perspectives

In the previous subsections, we presented several different approaches for decision making. We acknowledge that managing security is resource demanding, in terms of personnel and time involved. However, we want to compare the ease of use of these techniques with respect to one another. In addition, when managing security, IT security officers provide one or several solutions to managers. Both parties discuss the alternatives and a decision to implement (or not) one (or several) solution(s) is made. Therefore, IT security officers need to communicate appropriately the results of an assessment to highlight a need for a security solution or they need to justify why one solution is better than another one. In this section, we analyze the aforementioned solutions with respect to two questions:

1. *How easy is it to manage security with this technique?* Elements to consider to answer this question include: applicability and feasibility, necessary human

resources, time, involvement of third parties, or required data.

2. *How can decision makers justify implementing a solution?* Assessments can lead to recommendations on improvements. Are the outputs adequate to convince decision makers to invest in the recommended solution?

Among the solutions cited, ad-hoc assessments are the easiest ones to implement when managing security. They do not require as many resources as the other approaches but they do not provide support into deciding among security solutions: it is difficult for IT security officers to use the outputs of these analyses to convince managers to invest in one solution versus other solutions. Self-assessments and standards and regulations are easy to implement as they provide specific questions or guidelines to manage security in organizations. When organizations are looking for certification, they need to have a third party involved in the process. Recommendations on what to do to improve security are derived from these assessments but there is no guideline on how to decide between several solutions and how to convince decision makers. Security risk assessment is probably the most used technique. It is however criticized for being resource demanding. In addition, security risk assessments do not allow justifying the implementation of one solution versus another one. On the contrary, economic approaches allow comparing quantitatively security solutions and managers are familiar with discussions involving dollar values. However, the feasibility of these approaches is questionable as it is unclear where data used in the analysis come from. The same issue with the origins of data stands for the AORDD framework [66]: it is not clear how empirical

data are used for the quantitative analysis. The AHP [22] approach is not easy to implement as it requires the involvement of several experts to identify criteria and assign scores to them. Both the AORDD [66] and AHP approaches [22] have the advantage of comparing solutions and facilitating communication. Game-theory-based and adversary-based techniques, on the contrary, do not facilitate communication as the outputs are low-level and decision makers do not necessarily have an IT security background: for example, both techniques may require the understanding of attack paths. Because of the formalism involved, they are not easy to implement, unless a tool is already provided [75]. Finally, model-based approaches presented above have the significant advantage of showing the interactions between components, hence showing how implementing a solution may affect other factors in the model: this facilitates communication between IT security officers and managers. Their use is however limited as it is unclear how these models can be used in a real organization.

In conclusion, there is a need for a framework for decision making that is *easy to use* for IT security officers and that *facilitates discussion* with managers and the justification of implementing one security solution versus other ones.

2.3 Including the Human Element

Including the human element in security has been an increasing trend ([56] and [102]) as humans can cause security breaches or make risky decisions that impact an organization's security ([64] and [72]). Human elements involved in security are: the attacker, the user, and the organization (through managers, or system

administrators).

2.3.1 The Attacker

The attacker has been a major concern for the security community. More precisely, work has been conducted to identify attributes of the attacker. For example, Arief and Besnard provide insights about the attacker from a human perspective by defining a taxonomy for hackers and discussing hackers' motives [15]. Yuill et al. suggest profile attributes for the attacker [126]. Attackers' attributes include their abilities (such as computer skills or attack skills), their knowledge (their knowledge of the network), and their motives. Also the authors explain that the attacker's decision to attack or not depends on 1) his/her valuation of the network asset, 2) the cost, and 3) the resources.

Quantifying attackers' behavior has been attempted. An example is an informal quantification in which a red team of experts is used to try to compromise a system [78]. An alternative approach has been to probabilistically quantify an attacker's behavior. Littlewood et al. conducted early research in probabilistic modeling of the attacker behavior [77]: the approach is based on the analogy between a system failure and a security breach where the effort of the attacker is introduced as a measure of the security of a system and is assumed to follow an exponential distribution. Besides, Madan et al. model the attacker behavior through a semi-Markov chain and defines the mean effort to security failure to be a good candidate for security quantification [80] while Stevens et al. define two measures [108]: the mean

time to vulnerability discovery and the mean time to exploit a vulnerability. On the other hand, Jonsson and Olovsson study the attacker behavior through empirical data [69]. This work identifies three phases in the attack process: the learning phase, the standard attack phase and the innovative attack phase. The experiment shows that the times between security breaches are exponentially distributed. Ortolano et al. propose modeling known vulnerabilities in a system using a “privilege graph” [88]. By combining a privilege graph with simple assumptions concerning an attacker’s behavior, the authors then obtain an “attack state graph”. Parameter values for such a graph have been obtained experimentally; once obtained, an attack state graph can be analyzed using standard Markov techniques to find several probabilistic measures of security. Dantu et al. suggest a methodology for vulnerability analysis based on attacker behavior [39]. The methodology proposes the use of attack graphs that incorporate attributes related to the attacker such as computer and hacking skills, tenacity, or cost of the attack. A Bayesian approach is used to quantify the attack graph. Goseva-Popstojanova et al. propose a general model of an intrusion-tolerant system to describe security exploits by considering attack impacts where the system state is represented in terms of failure-causing events [59]. Jha and Wing propose a combination of state-level modeling, formal logic, and Bayesian analysis to quantify system survivability [59].

2.3.2 The Organization

The goal of the organization is to protect the organization's assets. Several characteristics related to the organization have been provided in the literature [72] and have their importance when managing security. They include the budget allocated to IT security, information security culture, security awareness [99], resources such as staff, hardware, and software [94].

Martins suggests an information security culture model based on the concepts of organizational behavior [81]. The author identifies information security controls at the individual, group, and organization levels that could influence organizational culture: policy and procedures, risk analysis, budget, benchmarking, trust, management, ethical conduct, and awareness.

Schlienger and Teufel believe that focusing on the organizational culture relies on addressing the human element and understanding its behavior [101]. They propose a framework to analyze security culture of an organization through questions to users in the company. Each user is asked to answer questions such as "The computer and electronic communications systems should be used for the company's business activities only" from his/her own perspective ("Personally I think this is true/false/I don't know"), from the company's perspective ("The company regards this as true/false/I don't know"), and as the best solution ("If I were responsible, I would regard this as true/false/I don't know"). The objective of the questionnaire is to assess whether employees know what security policies state and whether they support them. The results of this analysis are shown as an information security

culture radar. This approach allows assessing how employees perceive security culture and seeing where improvements need to be done. However, this approach may be difficult to apply in some environments, such as universities, where responding to the questionnaire will be up to user's willingness to respond. Quite extensive research exists on the topic of security culture ([38], [60], [81], [99]).

2.3.3 The User

Little work has been done with respect the user in security. However, Schneier stipulated that the user is the weakest link and that security is “as good as its weakest link” [102]. This assertion would place the user at the center of any security system. Attributes of users have been studied in other areas, such as the human-computer interaction area. Examples of characteristics that could be applied to the user in the computer security field are the following: trust ([105] and [111]), knowledge and expertise ([82] and [105]), user acceptance of the technology [40], user perception such as perceived risk ([82] and [106]), or perceived ease of use and perceived usefulness ([40] and [41]), computer-related knowledge and experience [76]. Mitchell mentions that the expertise can improve the perception of risks [82]. With the increasing concern of social engineering [83], the user has become a major interest in the computer security field recently. Indeed, even with the best well-protected network, attackers can get into a system by manipulating the user to get his/her password. Gonzalez et al. use system dynamics to model social engineering [56]. The authors suggest a simple way to recognize social engineering attack patterns by

using feedback and reinforcing loops. The advantage of the suggested model is that the model accounts for both the attack and defense process. There is a common agreement that the best way to prevent social engineering to happen is to educate users [54]. Especially, organizations can raise users' awareness on security issues through communication and users can be educated through the media.

2.4 Model Validation

Validation is defined by Balci as checking that “the model, within its domain of applicability, behaves with satisfactory accuracy consistent with the study objectives” [18]. In other words, validation consists in checking that the model built is the right one ([18] and [87]). There is an extensive literature on validation plans in several fields, including social sciences [29], operations research [52], safety assessment of nuclear waste [115], and information security risk management [49]. Distinction is made between two sources of information to support model validation: experts and data.

First, several validation techniques involve experts. Sargent describes four approaches for the validation of simulation models [98]: 1) asking the development team if the model is valid, 2) asking the users, who have been thoroughly involved in the development process, to check the model validity, 3) asking a third party (also called IV & V: independent verification and validation), and 4) using a scoring model based on subject matter experts who provide a scoring of several indicators [17]. Balci provides a group of informal validation techniques, which rely on human

reasoning [18]. They include:

- Face validity: People, from the model development team, users, or experts, are asked if the model and/or its behavior is reasonable,
- Walkthrough: A team, involving model developers and from four to seven people external to the development, meets to identify faults in the model,
- Inspection: A team of generally six people having precisely defined role meets to identify faults in the model. Differences between a walkthrough and an inspection include the people in the team and the number of steps of each technique (two steps in walkthroughs and five in inspections),
- Reviews: A team, that includes managers, meets to check that the level of quality of the model is attained.

Data may be collected and used to validate a model. Techniques defined in [98] include:

- Sensitivity analysis: The effects of several inputs on the outputs are studied (qualitatively and/or quantitatively),
- Historical data validation: If data are available, part of the data is used to build the model, and the remaining data is used to check that the model behaves as the system does,
- Predictive validation: The model is used to make predictions, which are compared to the real system's behavior.

Although experts and data are two distinct sources of information, they may be combined to validate a model. Hybrid techniques involving experts and data include Turing tests, in which experts are asked to discriminate between the model and system outputs (data). Law describes a 7-step process to build a successful simulation model [74]. The author lists validation techniques that can be applied to one or several steps of the process, including: interviewing experts, using quantitative techniques when possible, walkthroughs, and sensitivity analyses.

Although data may be a strong support to validation, the availability of data and the appropriateness of available data may be a major issue. Kleijen discusses the validation of a simulation model based on the availability of data [71]. Especially, the author concentrates on the use of mathematical statistics. The author identifies three situations: 1) when no data is available, 2) when only output data are available, but no data on the corresponding input or scenario is available, and 3) when inputs and outputs are known. In the first situation, the author suggests the use of knowledgeable experts, whose knowledge is qualitative. Sensitivity analyses are also advised. In the two other situations, the author provides recommendation on statistical tools to validate the simulation model.

As a conclusion, many validation techniques exist, that rely on experts and data. The use of experts provides a subjective and often qualitative model validation. On the contrary, the use of data may allow a quantitative and more objective validation.

2.5 Summary

Several conclusions can be drawn from the previous sections. First, frameworks for IT risk assessments have been developed to assess the level of security of organizations and decide how to invest in security. However, the feasibility of such assessments is questionable and it is often difficult to communicate their results. Therefore, the objective of this work is to provide a model for managing security that is easy to use and that facilitates communication with managers.

Second, the human elements that are involved in security include the attacker, the user, and the organization. Therefore, in the model, we want to identify major components of security. For each of them, the objective is to distinguish characteristics and influences among them. This approach facilitates communication between IT security officers and managers regarding security management: implementing solutions impact characteristics identified in the model and influences in the model depict how the measure impacts security.

Third, developing a model also involves validating it. We described in the third section of this chapter the validation techniques involving data and experts.

Chapter 3

An Approach for the Development and Validation of a Model for Decision Making in IT Security

3.1 Introduction

In this chapter, we describe the process to develop a model for IT security. The objective is to develop a model to manage security that facilitates communication between IT security officers and managers, and includes the human element. The first section of this chapter presents the model representation that was adopted to best achieve these goals.

When developing a model, we should ensure that the developed model is correct. In other words, it should identify correct components, characteristics, and influences between characteristics. Besides, users of the model should be able to believe the outcomes provided by the model. Both objectives are covered by model validation. In the second section of this chapter, we discuss the model development process and the challenges related to model validation, and especially focus on model validation in IT security. We suggest that, although imperfect because of the lack of available data and meaningful metrics, model validation in IT security is possible.

In the third section of this chapter, we describe the carefully thought process to develop and validate a model for managing IT security from a theoretic point

of view. The process relies on four major steps. First, interviews are conducted to obtain models from experts in different organizations. Second, surveys among a larger number of experts are used to determine the characteristics to include in the final model. A model resulting from insights drawn from the interviews and surveys is developed. Third, the model is validated qualitatively through the input of experts. Finally, parts of the model are validated by using case studies in a real environment. Security data before and after the implementation of a security measure are compared to the predictions of the model. This four-step process results in a validated model for security management.

3.2 Model Representation

3.2.1 Motivations

Our objective is to develop a model for IT security officers to manage security that facilitates communication with decision makers. In order to manage security and decide where to invest in security, IT security officers and decision makers want to see the impacts of implementing a security measure on security. As IT security officers and decision makers are often not the same people, the model should allow IT security officers, who have the technical knowledge, to convince decision makers to invest in the most relevant security solution. To do so, IT security officers should show that implementing a solution would impact a set of factors, which would improve the overall security. Furthermore, when making decisions, there may be a need of comparing security solution A versus security solution B. Therefore, the

model should allow a comparison of the effects of both security solutions on other factors, hence on security.

In conclusion, the specifications of the model are the following:

- *A simple visual representation*: This allows reasoning about security and facilitates communication between IT security officers and managers,
- *Factors and influences*: The model should include major factors of security and the causal influences among them so that a security solution can be mapped to a factor or a set of factors in the model, and impacts of implementing this solution on other factors and on the overall security are identified,
- *Comparison of solutions*: The model should allow comparing security solution A versus security solution B. Decision makers should be able, based on the model, to identify which one would have the most impact on security and should be implemented.

3.2.2 Model Constituents

In Chapter 2, we emphasized the relevance of including the human element in security. We identified the user, attacker, and organization as the main stakeholders to consider. The human components interact through the assets. It is then possible to decompose each of them into factors that would impact security. Examples of factors were identified in Section 2.3 and include the user's risk perception and the attacker's motivations. As highlighted in the previous subsection, the objective is to depict these factors in a model and the influences among them so that the model

allows identifying the factors impacted by implementing a security solution.

Therefore, the model is composed of:

- *Components*: Security is decomposed into its major components. An example of a decomposition is user, attacker, organization, and asset,
- *Characteristics*: Each component is then decomposed into attributes that affect security. For example, if “attacker” is a component of security, the attacker’s motivation is an example of its characteristics,
- *Influences*: Causal relationships among characteristics are identified. The objective is to see how changing one characteristic in the model through the implementation of a security measure impacts other characteristics in the model, and the overall security.

The next subsection defines the formalism that includes the aforementioned constituents of the model.

3.2.3 Model Formalism

As we want to provide an effective tool to IT security officers to communicate with decision makers the impacts of one solution versus another one, we believe that an effective way of doing so is to visually represent elements and their relationships with nodes and transitions respectively. Inspired from existing techniques such as influence diagrams [67] and systems dynamics [95], we represent characteristics with nodes and influences among them with arrows. Characteristics can take several

values: in the remainder of the dissertation, we consider at most three values (high, medium, or low). The relationship between two characteristics can be a positive, negative, or neither of them. The third type of relationship implies that there is no simple positive or negative influence of one characteristic on another. We represent these three types of influences by adding to the arrow the sign “+”, “-”, and “?” respectively (Figure 3.1). “A has a positive (respectively negative) influence on B” means that if A is high (respectively low), B is high (respectively low). Moreover, we introduce weights associated with the influences between characteristics to depict the strength of influences. These weights are indicated by the thickness of the arrow. We select a set of three possible weights: a thick arrow, a thin arrow, and a dashed arrow. A thick arrow represents a strong influence, a thin arrow represents a medium influence, and a dashed arrow represents a weak influence. Figure 3.2 depicts an example where characteristic A has a strong influence on C and B a medium influence on C.

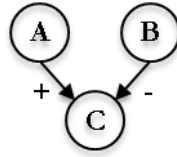


Figure 3.1: Positive and Negative Influences

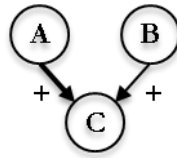


Figure 3.2: Strong and Medium Influences

For the remainder of the dissertation, we say that A is a parent node for B if A influences B (hence arrow from A to B). In the same situation, B is a child node for A.

3.3 Model Development and Validation

3.3.1 Objectives

As previously discussed, the objective is to build a causal model that includes 1) the components of security (for example, attacker, user, organization, and asset), 2) characteristics related to the previously identified components of security, 3) influences among characteristics. Such a model aims at addressing communication issues: with a model that identifies the influences of characteristics of security on one another, security teams will be able to discuss with decision makers the impacts of implementing one security solution versus another one.

The challenges of developing such a model are two-fold. First, the final model should be correct, that is to say it should reflect reality. Secondly, users of the model (IT security officers and decision makers) should be able to believe in the model and believe its results. Both challenges rely on the model validation, which specifically aims at answering the following questions:

- Does the model correctly identify characteristics and influences for security?
Does it include all characteristics? Does it include all relationships?
- Does the model correctly provide results for decision making?

However, validation of a model is challenging, as highlighted in Section 2.4. The next sections presents an ideal validation plan and the challenges of validating a model for IT security decision making.

3.3.2 An Ideal Validation Plan

An ideal validation plan involves the two sources of information previously discussed in Section 2.4: experts and data.

First, experts elicitation can allow the identification of components, characteristics and relationships between two characteristics. Several elicitation approaches are possible: they include interviews (face-to-face or by phone) and surveys (by phone, email, or mail). In the case of interviews, best results are obtained when enough time is allocated to the interview, and several rounds of interviews should be preferred to a single interview. In all cases, we need a sufficient number of experts for the analysis to be relevant. However, there is no agreement on the optimal number of experts needed, although there seems to be a limit beyond which adding more experts does not increase the accuracy of the results. Several studies (including [16], [19], [125], [104]) argue on the number of experts needed. Besides, experts should be from several organizations (in-house and external). Furthermore, if the scope of the model is to develop a generic model, experts should come from different horizons, such as companies, academic environments, or governmental agencies.

In addition to experts, case studies should be derived from data to validate the model. This can be done in several ways, as discussed in Chapter 2:

- Predictive validation: A security solution is implemented and its impacts on the organization's security are later compared to the model predictions,
- Historical data validation: For example, past records show the implementation of a solution. The analysis of security data after the implementation may provide insights on the impacts of the solution on security, which are compared to the model predictions,
- Simulations: If each of the characteristics and relationships in the model can be represented by a mathematical model, a high number of random inputs provides a range of resulting outputs. The outputs should match collected data to validate the model.

In all three approaches, data are compared against results provided by the model. This is depicted in Figure 3.3.

The model should be applied in several organizations as case studies. The major weakness of the case study method is that the results may be specific to the organization and may not be generic. Despite this drawback, insights can still be gained from a case study, and general theories can be generated from practice [51].

Validation of any model can be frustrating because it is not possible to achieve an ideal validation. Experts may not be willing to help, or may not dedicate sufficient time, or data may be unavailable or incomplete. The next section references reasons to explain the difficulty of model validation in IT security.

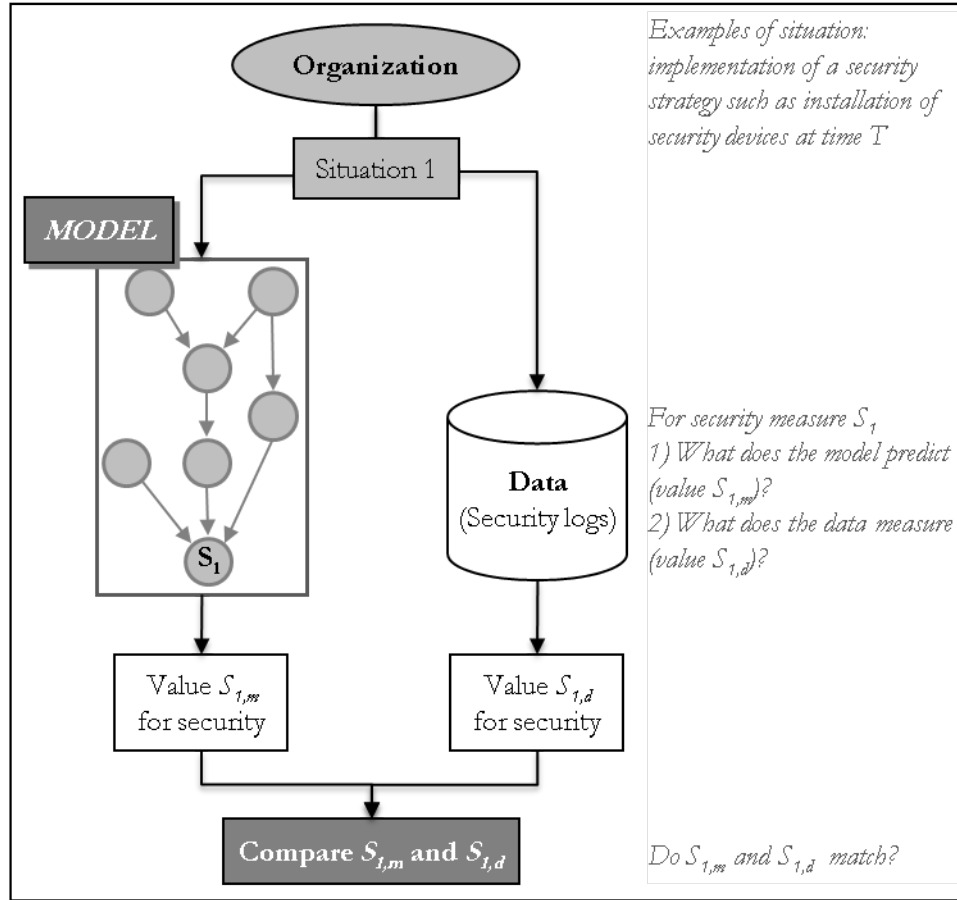


Figure 3.3: Validation through Case Studies

3.3.3 Why is the Validation of an IT Security Decision Model so Challenging?

3.3.3.1 Experts

There is no formal definition of an expert, which is not specific to the IT security field. An expert may be defined by his/her educational background, number of years of experience, recognition by peers, or information he/she has access to. In general, an expert is viewed as a human being who has specific knowledge in a field. Therefore, we define an expert in IT security as a person who has knowledge in IT

security, such as an IT security officer. Security experts have knowledge on security issues and on how to deal with them.

Experts can help during the model development process by providing their insights into what should be and should not be included in the model. In IT security, we face the major issue that experts may not be willing to collaborate. Kotulic and Clark recognize that the research field of IT security is one of the most intrusive domains as there is a mistrust of any outsider who would like to gain any knowledge on how practitioners think and act [72].

If experts accept to help developing the model, we may be limited in the amount of time spent with them. For example, we may need to meet with experts several times and for few hours every time, which experts may not agree on.

3.3.3.2 Data

3.3.3.2.1 Difficulty of Sharing Data

Most organizations collect logs of their network activity. Security data include raw data collected by security devices such as intrusion prevention systems and records of incidents. However, organizations are reluctant to share them. The first reason to explain this is that data contain personal information on users. Through the IP addresses, the user could be tracked and his/her habits could be determined. Second, organizations are hesitant to disclose the types of successful attacks targeting their organizations and their numbers. This gives the image that the organizations' network is unsecure and organizations are not willing to give this image. An

alternative would be to use sanitized data. Sanitized data are data that are deprived from personal information, such as IP addresses. However, sharing sanitized data is still challenging for organizations because organizations are reluctant to share data [68].

To face the issue of obtaining data by ourselves by involving organizations, we investigated existing available sources of information. There are available resources to allow the collection of data, such as the Protected Repository for the Defense of Infrastructure against Cyber Threats (PREDICT). PREDICT is a centralized repository of network operations data for research in IT security [4]. For example, the category Traffic Flow Data regroups datasets on traffic flow information that can be useful for research on denial of services. However, a set of security data is not enough to validate the type of model we are developing. We need additional information, such as specifics on the organization (security culture in the organization, size of the IT security team), details on the users (types of users), or on the data collection (for instance the configuration of the intrusion detection system that collected data).

3.3.3.2.2 Lack of Accepted Security Metrics

Although organizations collect a vast amount of data, data are often raw data and need interpretation. The first issue is that there is no accepted definition of security terms. For instance, vulnerability, threat and risk have different meanings from one person to another [53]. Secondly, although there is no doubt that metrics are needed to understand security and manage it ([20], [27], [53], [85]), the com-

munity has not come to an agreement on the metrics that should be considered for security. Suggested metrics cover a wide spectrum: examples include metrics based on performance, risk ([13] and [45]), financial field ([30] and [57]), and probabilistic approaches ([69], [77], [121]). Despite the wide range, no metric has been widely accepted and issues have been raised regarding IT security metrics [86]. As an example, Wang identifies five of them [120]:

- Metrics are often qualitative rather than quantitative (e.g. TCSEC, ITSEC, Common Criteria),
- Metrics are often subjective rather than objective (for example based on expert opinion),
- Metrics are often defined without formal framework,
- There is no time aspect related to current metrics,
- Traditional two-value logics are not suitable.

Several guidelines have been developed for security practitioners to develop metrics ([35] and [113]), and several required characteristics have been suggested. For example, according to Brothby, metrics should be manageable, meaningful, actionable (what action should be taken), unambiguous, reliable (ability to believe the metrics), accurate, timely, and predictive [27].

Even if there was an agreement on what metrics to use, there is no insurance that there would be a mapping between these metrics and the characteristics of the model.

3.3.3.2.3 Incomplete Information

Without security metrics accepted among the security community, organizations can use their security logs to measure characteristics in the model. However, it would be difficult to know the environment in which events occurred. In the case of a failure in a nuclear power plant, conditions of the environment at the instant of the failure can be investigated and a precise scenario can be built, as in the Three Mile Island accident [23]. In IT security, it is often impossible to trace back the scenario that led to a successful attack. Besides, there may be several causes to explain an event and no evidence to decide which one is indeed the cause of the successful attack. For example, if the number of corrupted computers has increased in an organization, it may be due to an increasing number of attackers, a fault of the user who did not correctly perceive risks, or a breach in a software that was recently discovered. There may be no available evidence to support one of the potential causes.

Although difficult to achieve perfectly, validation can be partially done. In the next section, we describe the process adopted to develop and validate a model for IT security decision making.

3.4 Process

3.4.1 Approach

The objective is to build a causal model that includes 1) the components of security (for example, attacker, user, organization, and asset), 2) characteristics related to the previously identified components of security, 3) relationships (positive, negative, or neither) between characteristics, and 4) strengths of relationships (weak, medium, or strong influence) . The process is based on discussions with experts, that rely on both interviews and surveys. The process is described in Figure 3.4 and relies on the following steps:

- Model development: Two sets of experts are used to develop one unique model through interviews (phase 1) and surveys (phase 2),
- Model validation (phase 3) through experts and case studies: The resulting model is shown to the same experts to obtain their comments, and portions of the final model are validated with case studies.

These items are detailed in the following subsections.

3.4.2 Phase 1: Building a Model through Interviews

3.4.2.1 Objectives

Several possibilities were considered to obtain a model based on the input of several experts and are summarized in Table 3.1:

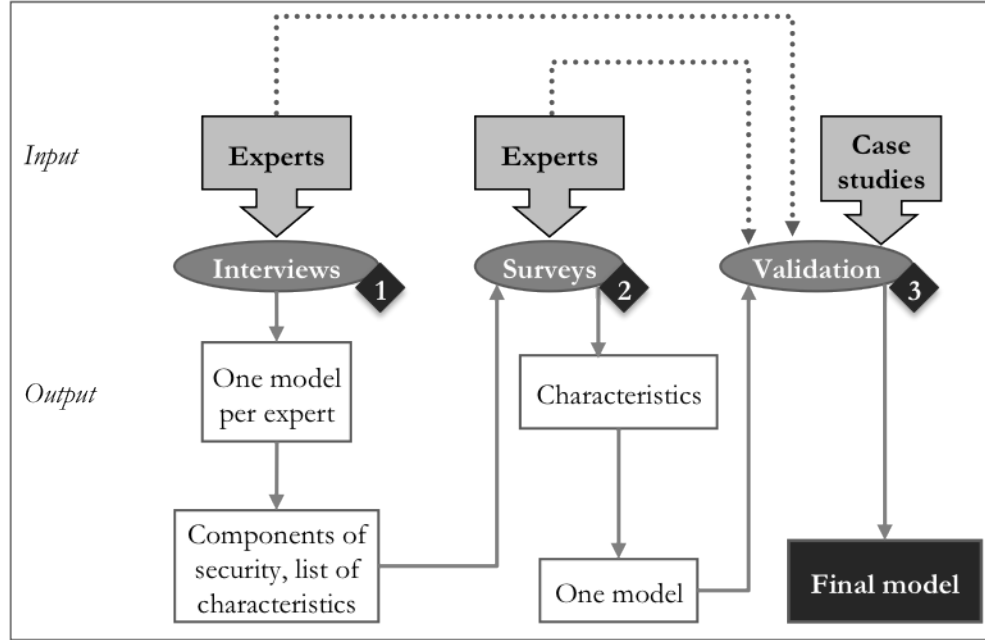


Figure 3.4: Diagram of the Model Development and Validation Processes

- Showing the model: It consists in showing experts a model previously developed (by the research team for instance) and obtaining approval or disapproval, and comments on it. The model can be changed following to these comments and the modified model can be shown to the next expert. It is the easiest solution in terms of analysis but it has the major disadvantage of biasing the interviewees with the original model,
- Aggregation of expert opinion through a Delphi technique ([28], [63], [117]): Experts are asked their opinions independently and have the opportunity to revise their judgment based on the results of all interviews. Ideally, a first round of interview would consist in the identification by each expert of a list of characteristics that influence security. During a second round of interview, the interviewees would be presented with an aggregated list of characteristics

based on the first round and would be asked to depict the influences between them. A third round of interview would lead to present an aggregated model and obtain approval or comments on it. This solution allows the aggregation of expert opinions without bias of experts on one another but has two major drawbacks. It relies on experts willing to be interviewed three times, and the aggregation of models may be difficult to do,

- Consensus among experts [84]: It consists in reaching a consensus among experts through a meeting in which experts discuss together. As opposed to the second solution, there is no difficulty in the aggregation of the model as experts brainstorm together, which results in one unique model. However, it is challenging to manage to have all experts in the same room, at the same time, and less confident experts may be shadowed by more confident personalities.

We consider that the most dominant disadvantages are 1) biasing the experts by showing them a previously developed model, and 2) having all experts in the same location at the same time. Therefore, we opted for the second solution. As experts may not accept three rounds of interviews, we decided first to conduct an interview at the end of which we would obtain one model per expert, with characteristics and influences. The second round of interview would consist in showing an aggregated model based on all interviews and serves as validation for our model.

The objective of the interviews is to develop a complete model per expert. More specifically, the objective is to 1) obtain approval of experts on a suggested decomposition (for example “user, attacker, organization, and asset”), or suggestions

Table 3.1: Alternatives for Interviews

| Solution | Description | Pros | Cons |
|-------------------|--|---|--|
| Showing the model | 1) Show a model previously developed 2) Obtain comments from interviewees on the model | Least time consuming solution for experts Easy to analyze results of interviews and modify model accordingly | Experts are biased by the original model |
| Delphi technique | 1) Round 1: each expert independently identifies a list of characteristics 2) Round 2: each expert is provided with the results of Round 1 and asked to draw a model 3) Round 3: Aggregated model based on all interviews is shown to experts to obtain their comments on it | No bias on the initial model No bias by other experts | Very time consuming for experts Analysis of the results of each round may be difficult: how to merge several opinions? How to account for contradictory opinions? |
| Consensus | Have all experts present in one room at the same time to agree on a unique model | No difficulty for the analyst as one unique model results from the meeting | Have all experts in the same location at the same time Less confident people may be overshadowed by more dominant personalities |

of another decomposition, 2) identify characteristics for each component, 3) and their relationships (type and strength).

We decided to conduct face-to-face interviews. They have the advantage to allow the interviewer to follow the thinking process of each expert. Also, they limit possible misunderstanding or misinterpretation of the questions, as the interviewer is able to reorient the interviewee in his/her thinking process. However, the interviewer needs to ensure that he/she does not bias the answers of the experts.

Building the model based on interviews relies on four steps: 1) designing the interview, 2) selecting interviewees, 3) conducting interviews, and 4) drawing conclusions (Figure 3.5). The following subsections specifically describe the steps of the interviews and their limitations.

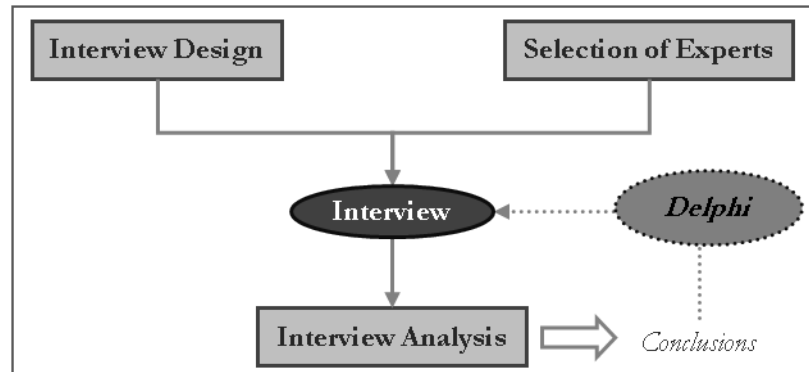


Figure 3.5: Interview Process

3.4.2.2 Interview Design

The interview is designed as a two-part interview. First, general questions should address experts' background, experience, and specifics about their organization (number of computers for instance). Second, their opinion on a model for

security should be asked. The objective is to obtain the following points from each expert:

- The components to be considered in security,
- The list of characteristics for each identified component: for example, the operators fatigue is a characteristic for human error in a power plant,
- A diagram that depicts: 1) characteristics as nodes, 2) relationships between them with arrows, 3) type of relationship (positive, negative, or neither), 4) the strength of relationship through the thickness of the arrow.

3.4.2.3 Selection of Experts

There is no formal definition of what an expert is, hence, no agreement on whether an expert is defined by the number of years of experience, educational background, status among peers, or the amount of information he/she has access to ([28] and [63]). Therefore, the selection of experts is challenging. Monitoring the background of each expert is necessary for further analysis.

Besides, there is no optimum number for the number of experts to interview. However, the number of interviewees may be bounded by two factors: 1) geographic location of the experts as face-to-face interviews require that the interviewers physically go on site, and 2) the number of experts willing to participate in the study.

3.4.2.4 Interview

Although he/she may reorient the interviewee in the thinking process, the interviewer should not bias the responses of the interviewee. Second, results of the interview depend on the time spent with each expert. The goal is to obtain the maximum information within one interview as IT security experts may have very busy schedules that do not allow them to meet with interviewers more than once. The duration of the interview may be bounded by the experts' time constraints. A good time duration is two hours: a shorter time does not allow to gather all the necessary information while it may be difficult for the expert to focus on the interview more than two hours.

3.4.2.5 Analysis

After a number n of interviews, n models are available for analysis. The next step is to conduct surveys among a larger population of experts to gather more opinions in the model.

3.4.3 Phase 2: Conducting Surveys to Gather more Information

3.4.3.1 Objectives

Surveys are intended to gather specific information through a questionnaire given to a large number of people. The major strength of surveys is that they allow a quantitative analysis of the responses. Although a wide literature is available on survey methodology ([14], [24], [62], [110]), designing a survey for our purposes

is challenging. In most surveys, questions target demographics (such as gender or age) or habits of respondents (frequency of computer use for example). On the contrary, our survey aims at gathering opinions of experts on what they think about characteristics of security. More specifically, the objectives of the surveys consist in obtaining experts' opinion on: 1) a decomposition of security (for example user, attacker, organization, and asset), 2) a list of characteristics (based on a merged list from the interviews), 3) and the impact of these characteristics on security.

The following subsections specifically describe the steps of the survey process (Figure 3.6).

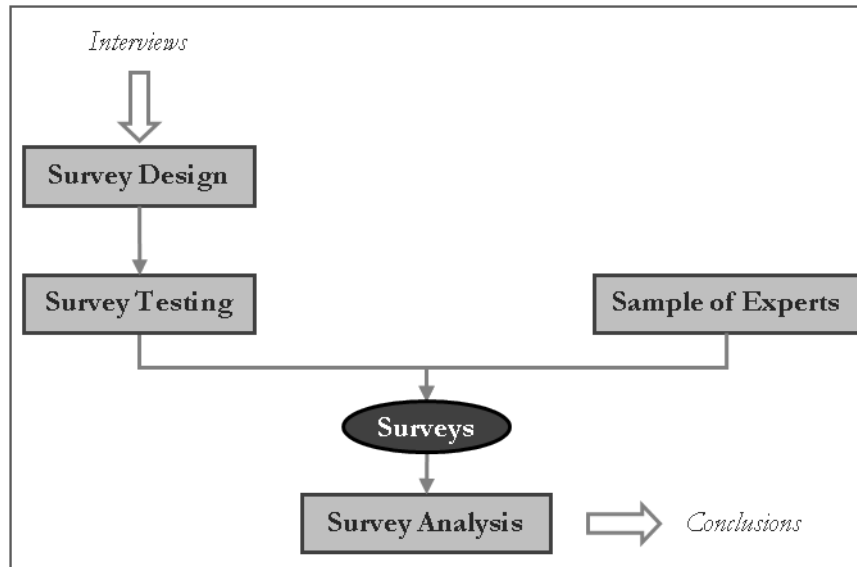


Figure 3.6: Survey Process

3.4.3.2 Survey Design

During the survey design, several decisions need to be made:

- What mean should be used: telephone, online, email, or mail surveys?

- How many questions should be included?
- What type of questions should be used: open or closed-ended, scales?
- What questions should be asked: demographic, biographic, specific questions on characteristic A impacting characteristic B, questions on characteristic A impacting security?

The panel of respondents is a community of IT security experts so an appropriate way to conduct a survey is to create an online questionnaire.

The survey does not allow to gather as much information as interviews. There should not be too complex questions or too many of them, otherwise, respondents may give up answering the survey. Therefore, we decide to focus on some aspects of the models. The format of the questionnaire should be user-friendly and quick to answer: respondents should not spend more than fifteen minutes on the survey. While designing the questions, limitations need to be considered [51]: 1) questions should be asked in the right way and should not bias the answers (as opposed to the interview process, an interviewer is not present to reorient the thinking process), 2) questions may be misunderstood or misinterpreted (no interviewer is present), 3) a sufficient number of responses is necessary for the conclusions to be significant, 4) closed-ended questions are preferred, 5) questions should be asked in a way that the results will be efficiently exploitable, and 6) questions focus on parts of the model as too many questions may prevent respondents from going through the entire questionnaire.

The main components of the survey are (Figure 3.7):

- Introduction: The objectives of the survey should be clearly defined. This part needs to be appealing so that respondents will go further in the survey,
- Questions about the respondents: As IT security people are often reluctant to share personal data, respondents name is not asked. However other details are gathered, such as the name of the organization he/she is working in, the current position, the number of years spent at this position (list of choices), and a list of past experiences. The only required questions are the current position and the number of years spent at this position so that the respondents' background is tracked,
- Questions about the respondents organization: Number of users, people working in the IT department and in the IT security department.
- Questions about the components of security: This section captures the confidence of the respondents in a decomposition such as "Attacker, User, Organization, Asset", and in the definition of each of the components,
- Questions on general influencing characteristics: Because questions about every relationship in the model cannot be asked (in order not to prevent respondents from not answering the entire questionnaire), we decided to ask questions about the impact of characteristics on security. The list of characteristics included in the survey is a result of the previously conducted interviews. Respondents are asked to assess the strength of each characteristic on security,

- Thank you page: On this page, respondents have the possibility to leave their comments and email address for further studies.

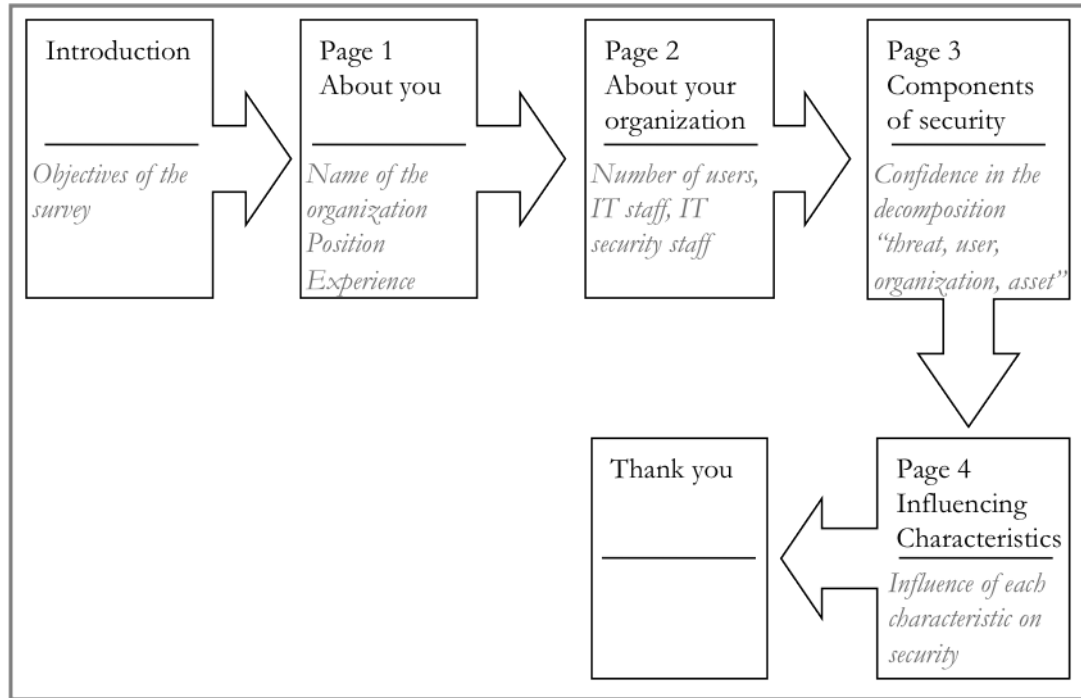


Figure 3.7: Components of the Survey

3.4.3.3 Survey Testing

As sending out the surveys is a one-shot trial, the objective is to obtain a maximum number of usable answers. Therefore, the survey should be extensively reviewed. One possibility is to look for a survey center at the University. Another possibility is to have people take the survey and provide comments. Ideally, they should have a background in IT security so that they are representative of the population of experts who will take the survey. The survey should be modified accordingly to comments before being sent out to experts.

3.4.3.4 Sample of Experts

Parallel to developing the survey and testing it, potential respondents should be investigated. Sending the survey to a listserv of experts is a possibility. As there is a mistrust in the IT security field of anyone who tries to capture how IT security officers think and act, sending the survey through a credible source is recommended. A credible source may be an IT security officer at the University.

3.4.3.5 Survey Implementation and Analysis

In order to maximize the probability of experts taking the survey, the date to send the survey is carefully picked. On the one hand, we ruled out the possibility to send it early in the week because returning from the weekend may result in a high quantity of emails and in the possibility of having our survey directly sent to the trash folder. On the other hand, sending it late in the week would provide the opportunity to potential respondents of delaying answering the survey to the following week and forgetting.

The major objective of the survey analysis is to obtain a list of characteristics to include in the model and the strength of each of these characteristics on security. Further, the results can be analyzed according to the type of positions of respondents, for instance by separating managerial positions from technical positions.

3.4.4 Phase 3: Incremental Validation

3.4.4.1 Objectives

As discussed in Section 3.3, a complete validation of the model is not possible, but partial validation can be achieved. The objectives are to provide a model 1) that correctly identifies characteristics of security and relationships between them, and 2) that users of the model can believe. Two methods are considered:

- Validation through experts: The model is shown to experts who provide comments and accordingly, changes in the model are considered,
- Validation through case studies: Data collected in a real environment are used to validate relationships in the model.

The next two subsections present an overview of both validation approaches.

3.4.4.2 Validation through Experts

The Delphi method ([28] and [117]) recommends to reach a consensus among experts by meeting with them in a second round of interviews. During this second round of interviews, experts are shown the final model and are asked to comment on the model. Questions asked to experts include:

- Do you agree with the structure of the model?
- Do you think all characteristics related to the attacker, user, organization, and asset, that have an impact on security, have been identified?

- Are there any characteristics missing?
- Do you agree with the relationships that were identified?
- Do you agree with the strength of relationships?

The targeted experts for this second round of interviews are the experts who were interviewed during the first round, and experts who took the survey and provided their email address for further communication.

This second round of interviews does not require onsite meetings, as opposed to the first round of interview. There is no need to follow the entire thinking process of experts. Indeed, we need precise approval or disapproval about the structure of the model, which can be obtained through email communication.

3.4.4.3 Validation through Case Studies

Ideally, the model should be applied in several organizations as case studies. The major weakness of the case study method is that the results may be specific to the organization and may not be generic. Despite this drawback, insights can still be gained from a case study, and general theories can still be generated from practice [51]. The idea is to check the conclusions of the model against data collected at organizations, as discussed in Section 3.3 and depicted in Figure 3.3.

3.4.4.4 Use of Indicators

In cases where characteristics cannot be directly quantified with data, we use indicators. Indicators are defined as *metrics or factors that provide an indirect or*

secondary indication of the presence or magnitude of a primary factor or metric for which we do not have a direct metric or method of observation. Examples of indicators in economics are the Gross Domestic Product (GDP) or the unemployment rate. These statistics give a sense of how well the economy is in a country. Here, indicators provide knowledge or information about the value of some characteristics. An example of indicator of the level of security is the number of corrupted computers. If an organization records a high number of corrupted computers, it may mean that its level of security is low. On the contrary, a low number of corrupted computers may reveal a high level of security.

3.5 Summary

In this chapter, we presented the plan for developing and validating a model to help communication during the IT decision making process. We described the formalism used to depict components of security, characteristics of each components, and influences among characteristics. We highlighted the challenges inherent to model development and validation, and specifically, we raised the issues of involving experts and gathering data in the field of IT security.

We suggested in this chapter a carefully thought approach to model development and validation. The approach involves experts and data and can be decomposed into three steps. The first phase consists in interviews of experts in order to obtain a model with components of security, characteristics of components, and influences among characteristics. The list of characteristics is used in the second

phase of the model development: surveys are conducted in order to obtain opinions of experts on the influence of these characteristics on security. A model results from these two phases and is used in the incremental validation phase: first the final model is shown to experts in order to obtain their comments; second, case studies are used to validate portions of the model.

The model development and validation process described in this chapter are generic recommendations on how to build a model for decision making in IT security. The next chapter provides an example of how this approach is developed for universities environment.

Chapter 4

Model Development

4.1 Introduction

The objectives of Chapter 4 are to present the results of the model development for academic environments. We developed a strong collaboration with the Director of Security at UMD over several years, who is present along the entire process of the model development and validation. In the first section of this chapter, we present a preliminary model including components of security, characteristics, and their relationships. This initial model is based on the literature on how to characterize human elements and on a series of discussion with the Director of Security at UMD over several months.

In the second section of this Chapter, we present the results of the interviews. We managed to interview three experts at other academic environments, who are professional contacts of the Director of Security.

In the third section, we discuss the results of the survey. The survey was sent to a mailing listserv of about 600 people and fifteen experts answered the survey.

In the fourth section, we present the main steps to aggregate results from interviews and surveys. The resulting model is presented at the end of this section and is ready for the validation phase.

4.2 Initial Model

4.2.1 A Special Collaboration with the Director of Security

Since the beginning of this project, the Director of Security at UMD accepted to work and weekly meet with us. He has over fifteen years of experience in dealing with IT security issues at a large public university and is, through frequent interactions with his colleagues at other universities nationwide, also very familiar with security issues at other US universities. This special collaboration allowed us to capture his insights along the entire process of the model development and validation and quantification. This relationship is a very valued asset to our research as often, administrators do not trust anyone who tries to capture how they think and act.

The Director of Security at UMD helped developing a first model for managing IT security. Furthermore, through his contacts with IT security officers at other academic organizations, we are able to directly approach experts. We used his connections to select experts for the model development and validation. Interviews were initiated through his professional contacts, and surveys were sent on his behalf. He is mainly in contact with security experts at other universities; hence, the scope of the developed model is limited to academic environments. The model may not be generic and applicable to all environments, such as companies. However, the approach developed in this dissertation is a generic one that can be used to develop a model in another specific environment. Besides his connections, the Director of Security at UMD shared with us highly sensitive data to support the validation through case studies and the measurements of characteristics in the model.

4.2.2 Preliminary Model

4.2.2.1 Model Components

As previously discussed, a first step of the model development consists in identifying the model's major components. Gollman defines computer security to “deal with the prevention and detection of unauthorized actions by users of a computer” [55]. Consequently, this definition of computer security involves two stakeholders: 1) the attacker who attempts “unauthorized actions”, and 2) the organization (managers, system administrators) that aims to prevent and detect actions of attackers. Besides, focus has been especially put on the users (i.e. users of computers). For example, users are the targets of social engineering. Thus, we identified three stakeholders: the attacker, the user, and the organization. These three elements interact through the organization's assets. Therefore, to start with, we identified four components of security to be the user, the attacker, the organization, and the asset, which are defined as follows:

- *User*: We define the user in the computing field as someone who uses a computer. In the case of computer security, a user is also referred as the target of an attack,
- *Attacker*: Gollman defines the attacker to be “an individual who attempts one or more attacks in order to achieve an objective” [55]. This definition involves two concepts: 1) the attacker is a human being and 2) there is a willingness to harm. Even though many attacks are automated, a human being is still

the source of the attacks by developing them and launching the first attack instance,

- *Organization*: Scott defines an organization as “a social arrangement, which pursues collective goals, which controls its own performance, and which has a boundary separating it from its environment” [103]. In the context of information security, the organizational goal is to provide the most secure network to users,
- *Asset*: In business and accounting, assets are often defined as everything owned by a person or company that can be converted into money. We adapt this definition to information security: assets include 1) physical entities such as computers, and 2) data that can be sensitive, such as passwords, credit card numbers, organizational secrets, or intellectual property.

Later, the component “Attacker” is replaced by a more general term “Threat”. This change results from the discussions with experts and is explained in Section 4.3.

4.2.2.2 Model Development at the University of Maryland

The first step of the model development relied on developing a model with the help of the Director of Security at UMD. Based on the four aforementioned components, the objective is to identify characteristics for each of them and specify the interactions between these characteristics. The identification of the characteristics related to the human elements is supported by the literature (Section 2.3). Iden-

tified characteristics include the attacker’s motivations, the user’s risk perception, the value of the organization’s assets, or the IT team’s expertise. We focused on characteristics that can influence security by increasing the level of security (for instance the IT team’s expertise) or by decreasing the level of security (for instance the attacker’s motivations). Age, culture, and gender are characteristics of humans that we could consider in our study. However, we do not believe that any of them sufficiently impacts security to be included in the model. The model is depicted in Figure 4.1.

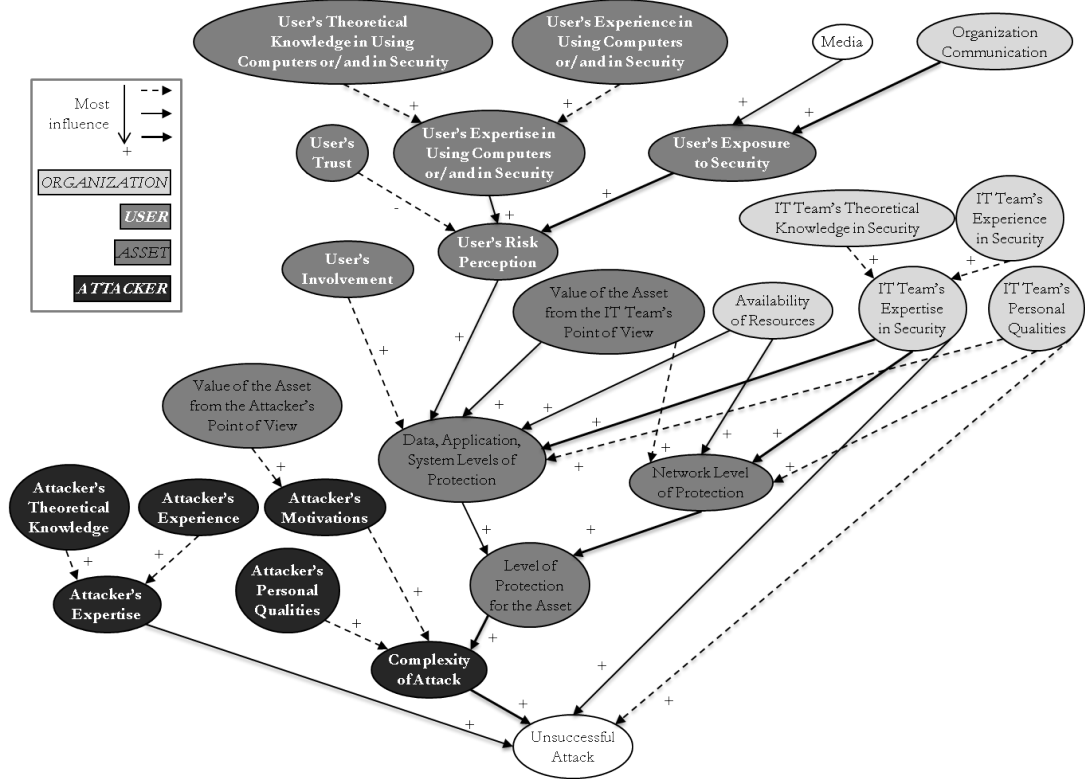


Figure 4.1: Model Developed at the University of Maryland

The end node of the model is the “Unsuccessful Attack”: the objective of the organization is to have a high number of unsuccessful attacks, which would be

representative of high security. We view the “Level of Protection for the Asset” as the different protecting layers that a computer possesses: protection at the network, application, system, and data levels of protection. Users can act on all levels but the network level of protection. This is the reason why the “User’s Risk Perception” impacts the “Data, Application, System Levels of Protection” but doesn’t impact the “Network Level of Protection”.

The characteristics identified in the model almost all have a positive influence. For example, a high value of the user’s theoretical knowledge results in the high value of the user’s expertise, or a high value of the organization’s communication implies a high value of the user’s exposure to security. However, trust has a negative influence on the user’s risk perception. Indeed, the more trust the user has, the more he/she will be inclined to trust the organization to protect the network. Therefore he/she will not have a good perception of risk. On the contrary, if the user has little trust, he/she will rely on himself/herself to protect his/her asset and thus have a better perception of risk.

The fact that an attack is successful (end node) depends especially on the complexity of the attack (high influence), versus the IT team’s expertise (medium influence) and personal qualities (low influence). The better the level of protection for the asset, the more complex the attack needs to be in order to be successful. If the attacker is motivated, he/she will be more inclined to develop a complex attack. The same applies for the attacker’s expertise and attacker’s personal qualities. Therefore, there is a positive influence between the nodes “Attacker Expertise” and “Attacker’s Personal Qualities” and the node “Complexity of Attack”.

4.3 Results of the Interviews

4.3.1 Model Developed at other Academic Environments

Interviews were led according to the discussions in Chapter 3. The questions that were asked to experts are:

- What are the characteristics of each component (attacker, user, organization, asset) that impact security (nodes in the model)?
- What is the influence between one another (arrows from one node to another)?
- What is the type of influence associated to each influence (“+”, “-”, “?” associated to each arrow)?
- What is the strength of each influence (dashed, thin, and thick arrow for weak, medium, and strong influence respectively)?

We succeeded in interviewing three experts at other academic environments, which would not have been possible without the leverage of the Director of Security at UMD. The interviews were taped and conducted by two interviewers together. One of the interviewers is an Associate Professor at the University of Maryland. The other interviewer is a graduate student at the University of Maryland.

The experts’ name and organization remain anonymous. The support sheet for the interviewers and a blank questionnaire are shown in Appendix A. One expert has over 30 years of experience and previously worked in a federal agency and in a company before working in an academic environment. The second expert has 20

years of experience and previously worked as a teacher and as a software engineer. The third expert has 10 years of experience in IT networking. Specifics of each expert's expertise and organization is depicted in Table ??.

Because of time constraints (on average, the interviews lasted two hours), the models developed by these three experts are less detailed than the one developed at UMD. The three models are shown in Figures 4.2, 4.3, and 4.4.

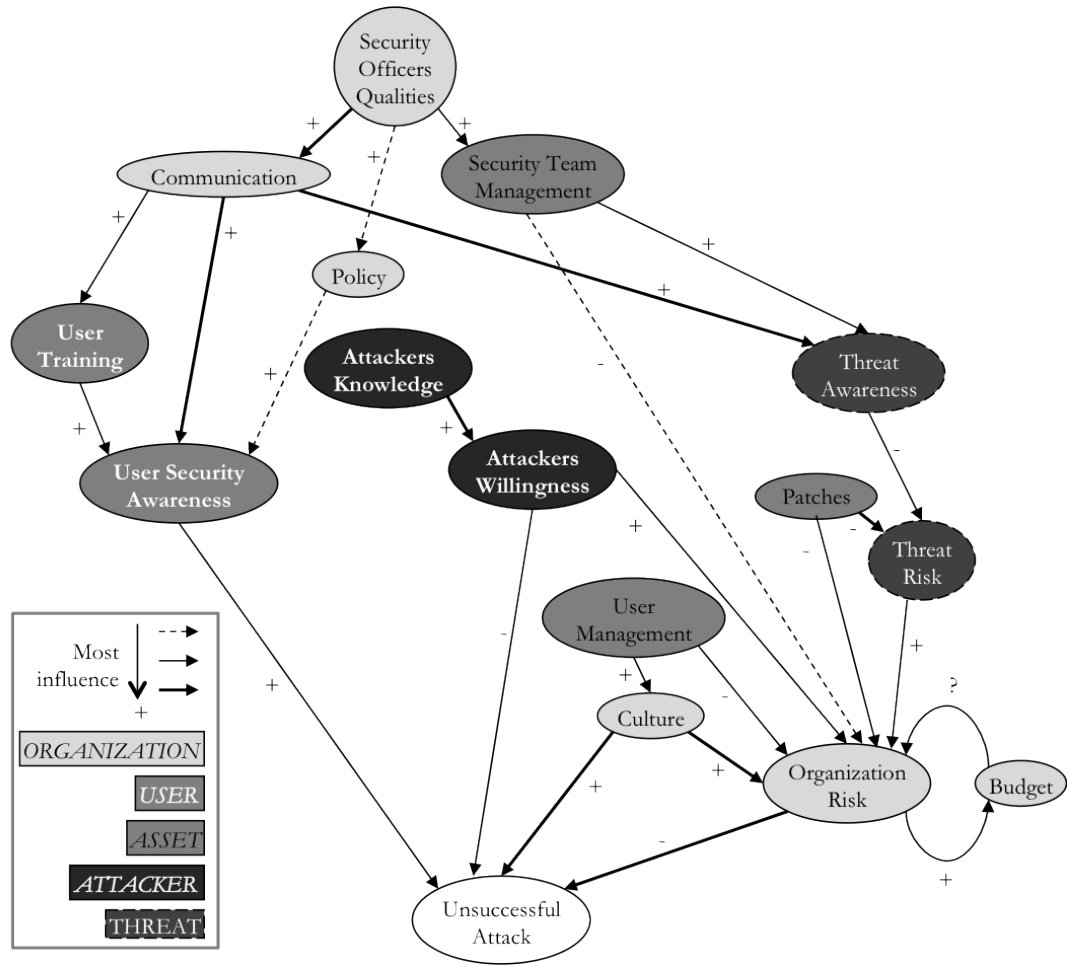


Figure 4.2: Model Developed by Expert 1

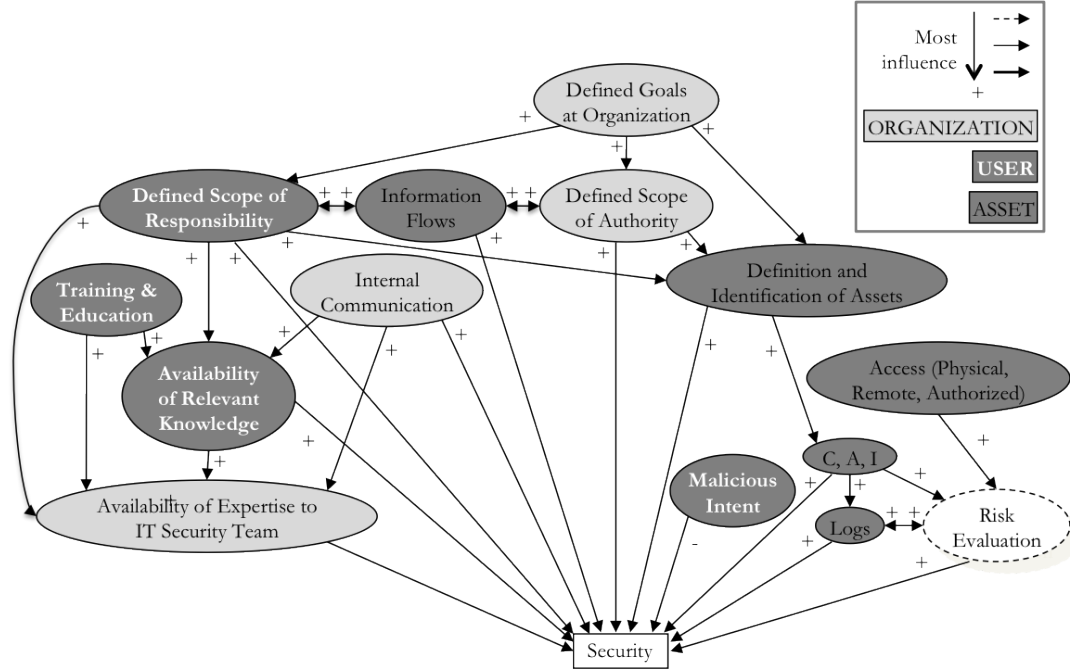


Figure 4.3: Model Developed by Expert 2

4.3.2 General Insights

One of the major insights provided by these interviews is that some characteristics were not mentioned in the initial model, such as policies but we agreed that it is an important characteristic that influences security and needs to be included in the final model.

Even though all four experts did not use the same terminology, they identified some common characteristics, such as the expertise or training of the users or the IT team, the budget, the available software (patches, detection and prevention devices), the attacker’s motivations, the user’s risk perception, the hierarchy of the organization, or policies.

Expert 2 suggested that we transform characteristic “Unsuccessful Attack” to “Security” which is more intuitive as an end goal.

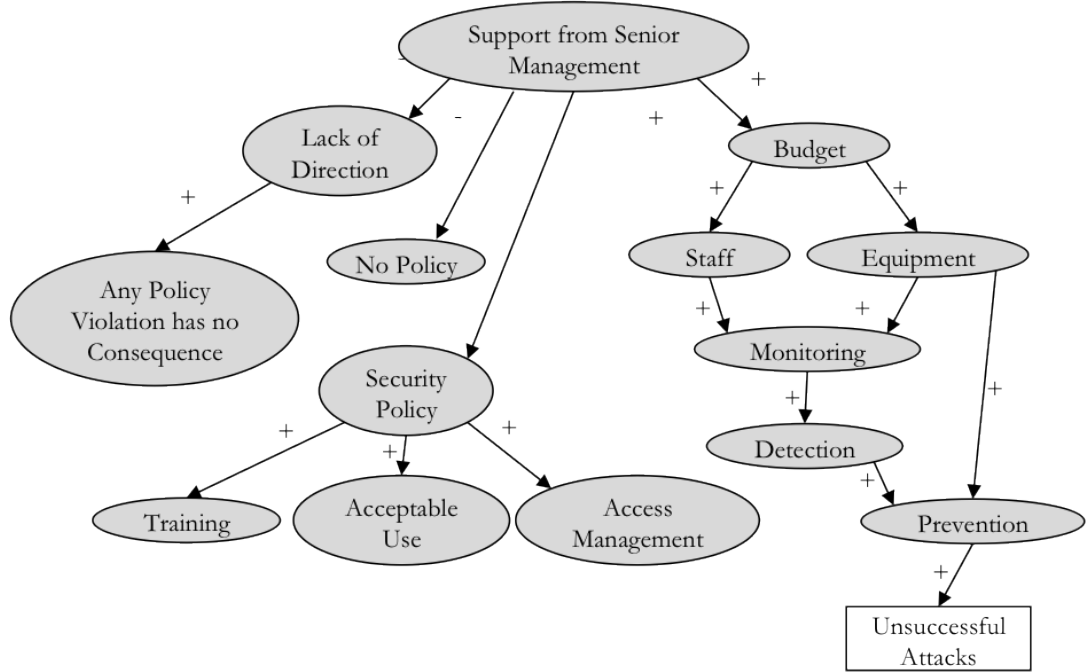


Figure 4.4: Model Developed by Expert 3

The third expert (Figure 4.4) does not provide us with a model that is entirely useful: identified characteristics are partially exploitable but the structure of the model is not. Characteristics of this model can be grouped into three classes: 1) some characteristics correspond to what we are looking for, such as budget, 2) some characteristics need interpretation, such as detection or prevention, which correspond to available software and hardware resources, and 3) other nodes are facts rather than characteristics (for instance, “any policy violation has no consequence”). Regarding the structure of the model, some nodes do not influence the end node “Unsuccessful Attack” while the objective was to identify characteristics that influence security, represented by that node. Despite our efforts, we were not successful in obtaining an exploitable model for the study from Expert 3. This may be explained by his role in his organization, which was more operationally focused than

the other experts. Therefore, this model is dropped for further analysis.

Expert 1 suggested the threat as a fifth component of security. After discussions with the expert, we understood that the term Attacker implies the concept of a human being as the source of the attack. Although an attacker is always at the source of malicious attacks, automated attacks, such as worms, can spread by themselves. Therefore, we decided to label the component “Threat” as being anything that can do harm and that includes the attacker.

Furthermore, it was suggested to use a more meaningful term for the end node of our model. Therefore, we replaced “Unsuccessful Attacks” by “Security”.

4.3.3 Outputs

The interviews will be used for two purposes:

- From the three models developed by the Director of Security at UMD, Expert 1 and Expert 2, we extracted a list of characteristics. This list is used in the surveys to gather opinions of experts on the strength of the influence of each characteristic on security,
- Once the surveys are conducted, the structure of the models developed by the Director of Security at UMD, Expert 1, and Expert 2, are used to develop the final model.

4.4 Results of the Surveys

This section describes the results of the survey at several levels: population of respondents, opinion on the decomposition “User, Organization, Threat, and Asset”,

and opinion of the influence on security of each characteristic previously identified.

4.4.1 Survey Implementation

4.4.1.1 Survey Design

As discussed in Chapter 3, the survey is administrated online. Two choices within free software were considered: Survey Monkey and the online Google Documents Forms. The free version of Survey Monkey is limited in the number of questions; hence we opted for the second solution.

Besides, the first page of the survey is located on a UMD URL and a UMD template to increase the credibility of the study. When clicking on “Start the survey”, the respondent is redirected towards the first page of the questionnaire. Snapshots of the survey and the complete list of questions are provided in Appendix B.

4.4.1.2 Survey Testing

Before sending it out, we considered having the survey reviewed by the survey methodology department at UMD and by an organization at UMD that deals with surveys. First, a mass email was sent to students in the survey department methodology, in which students were asked to review the survey on a voluntary basis. Second, an email was sent to a person from the Research Population Center, who is accustomed to designing surveys. Unfortunately, we did not receive the expected feedback and the reasons are the following: 1) both centers are not providing services for reviewing surveys, 2) people are asked to respond on a voluntary basis, with no reward, and 3) the type of survey is different from surveys where demographics or habits are usually investigated. The person from the Research Population Center

was unable to review the survey, mainly because of the field of study.

Besides, a testing phase was launched. The Director of Security, three security officers, three computer security graduate students, and three undergraduate students who are members of the UMD Computer Security Club took the survey, monitored the time to take the survey, and provided feedback. The survey was modified accordingly.

4.4.1.3 Survey Administration

The Director of Security at UMD is a member of the EDUCAUSE community. EDUCAUSE is “nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology” [2]. The survey was sent to an EDUCAUSE listserv. This listserv targets about 600 individuals who are responsible of IT security within a community college or university at the enterprise-wide level (no individual responsible of IT security at the department level in a university for example) from about 300 academic environments in the USA mostly but also in Canada and New Zealand. These individuals include day-to-day IT security practitioners (later called technical positions) but also IT security managers (later called managerial positions). The Director of Security provides credibility to the project and sent the survey under his name to this listserv.

4.4.2 General Insights

4.4.2.1 Visit and Response Rates

The Google Document Forms structure allows us to collect the answers only if experts indeed go through all the pages and click on the button “submit my answers”

on the last page of the survey. We decided to monitor the number of experts who visited the first page of the survey.

Out of 600 experts, 33 visited the first page of the survey and 15 answered the survey, which makes a visit rate of 5.5% and a response rate of 2.5% of the emails sent. 15 out of 33 experts who visited the first page answered the questionnaire: in this context, the response rate is 45.5%. We are not able to track the exact number of organizations (out of 300) that responded to the survey as the organization name was not a required field. However, 10 respondents out of 15 provided us with their organization name and all 10 are different organizations. Based on this number, the response rate regarding the responding organizations is at least 3.3% (10 distinct organizations out of 300) and at most 5% (16 organizations out of 300). Figure 4.5 shows the number of visits and answers to the survey per day.

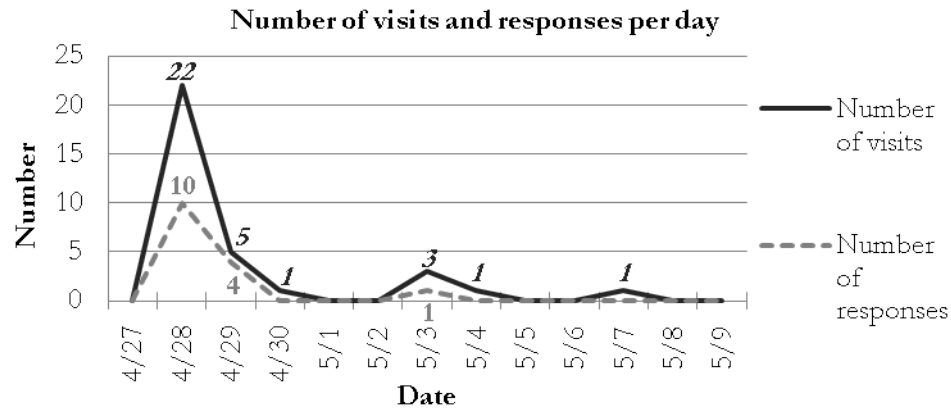


Figure 4.5: Visit and Response Rates

Visit and response rates are low, and taken out of their context, would be critiqued by many survey analysts. By replacing the survey in its context, we came up with a set of explanations for such low response rates:

- A sensitive field: The IT security field is not open on sharing information. We are not the first researchers to realize it. The authors of [72] recognize that the research field of IT security is one of the most intrusive domains as there is a mistrust of any outsider who would like to gain any knowledge on how practitioners think and act. They attempted to gather information from IT security officers and managers in firms through mail surveys and 23 firms out of 1,500 surveyed firms (response rate of 1.6%) responded. In our research, even if we sent the survey through a legitimate source, the Director of Security at UMD, IT security officers may still be reluctant to share their opinions,
- Type of questions: The survey does not ask for habits but for opinions, therefore requires time and energy from respondents. It is easier to answer questions such as “how many hours per week do you spend in front of a computer?” than “how would you rate the strength of the influence of the user’s expertise on security?”,
- Survey instrument, emails: IT security officers receive many emails per day. Although, we sent the survey out during the week, in order to avoid the flood of emails at the beginning of the week and early weekends, our survey was certainly in the middle of other emails that would end up in the trash folder.

4.4.2.2 Technical versus Managerial Positions

In the analysis process, we decided to differentiate answers from respondents working in technical positions and managerial positions. The motivations behind this action are to see if answers are clustered by experts’ position: by aggregating all

answers together, we may miss insights that could be gained if answers were grouped by experts' position for instance. It is expected that technical people have a better understanding of the protections of the assets, whereas managerial people have a better knowledge of the policies implemented in the organization. The weakness of differentiating between the two groups resides in the small available sample: the small number of respondents in each group may not be representative but we may be able to draw insights, although imperfect, from the responses.

Out of 15 respondents, 8 people have technical positions (such as security analyst positions) whereas 7 people have managerial positions (such as Chief Information Security Officer). Figure 4.6 represents the number of years of experience at the current position and the total number of years of experience respectively, for respondents working at a technical position (labeled [T]), a managerial position (labeled [M]) and all respondents together (labeled "All"). The majority of respondents spent less than 5 years at their current position (8 respondents, which represents 53% of all respondents¹, including 63% of technical respondents and 43% of managerial people). Only one respondent (7%) has less than 10 years of total experience; in other words, respondents, both at technical and managerial positions, are experienced IT officers.

Figure 4.7 provides statistics about the organizations: number of users, IT officers and IT security officers. At UMD, there are about 40,000 users, about 260 IT officers and 7 IT security officers. Most organizations (60%) are of medium size

¹According to Figure 4.6, $13\% + 13\% + 13\% + 13\% = 52\%$ of all respondents have less than 5 years of experience at their current position while in reality, 8 out of 15 respondents represent 53%. This is due to the rounding error encountered when summing up rounded percentages. For more accurate approximations, the reader should refer to Appendix C.

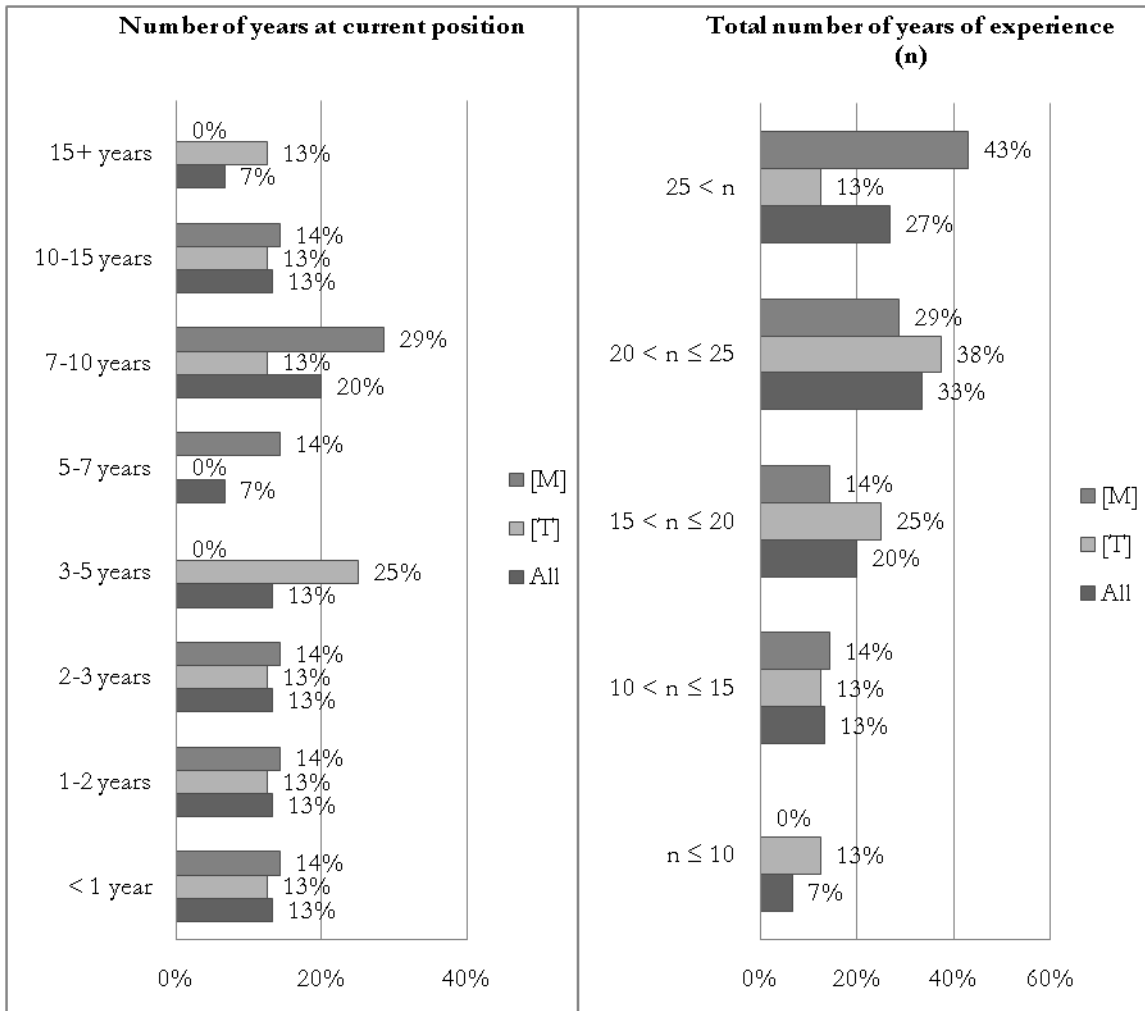


Figure 4.6: Total Number of Years of Experience: Managerial [M] versus Technical [T] Positions of Respondents

(between 10,001 and 25,000 users). The number of IT officers per organization seems fairly distributed among organizations. On the contrary, most respondents (57% of managerial positions, 88% of technical positions and 73% total) assessed the number of IT security officer to be less than 4 in their organization. These numbers allow capturing an idea on the size of the organization, the IT and IT security departments but these numbers should be considered with care. They rely on the respondents' assessment of these numbers, but it may be difficult, for instance, for an IT security

officer to assess the exact number of IT officers in one's organization.

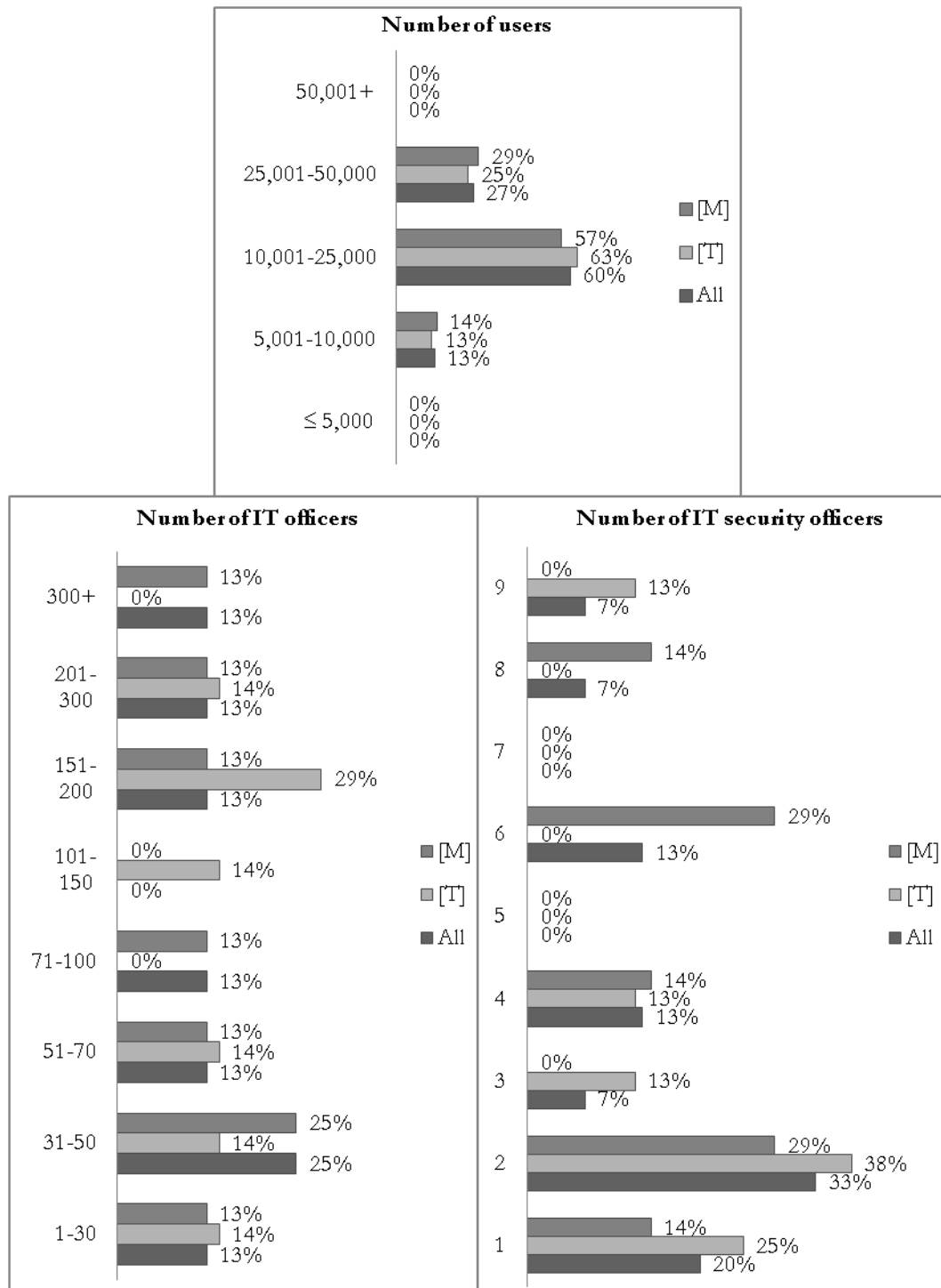


Figure 4.7: Organizations of Respondents: Managerial [M] versus Technical [T] Positions

4.4.3 Components of Security

Respondents were first asked to assess their confidence in the decomposition “threat, user, organization, assets”, and in the description of each of them as:

- Threat: Anything that had the potential to do harm and contains attackers,
- User: Anyone who uses a computer,
- Organization: Includes security team and managers,
- Assets: Include computers and data.

Experts had the choice between not believing or agreeing on the decomposition or description, somewhat confident, confident, and very confident. Results are provided in Figure 4.8. The majority of respondents (73%) are confident or very confident in the previous decomposition and 60% of respondents are confident or very confident in the description of the components. Comments received on these two questions included a suggestion of a decomposition that is similar to the risk analysis decomposition with the threat, vulnerabilities, risks, and controls.

4.4.4 Characteristics of Security

From the interviews, we identified a list of characteristics for each of the four components of security. This list was enhanced with some characteristics that we expect not to have an influence on security, such as the user’s place of birth. For each characteristic, respondents are asked to assess the strength of the influence of each of them on security: no influence, weak influence, medium influence and strong

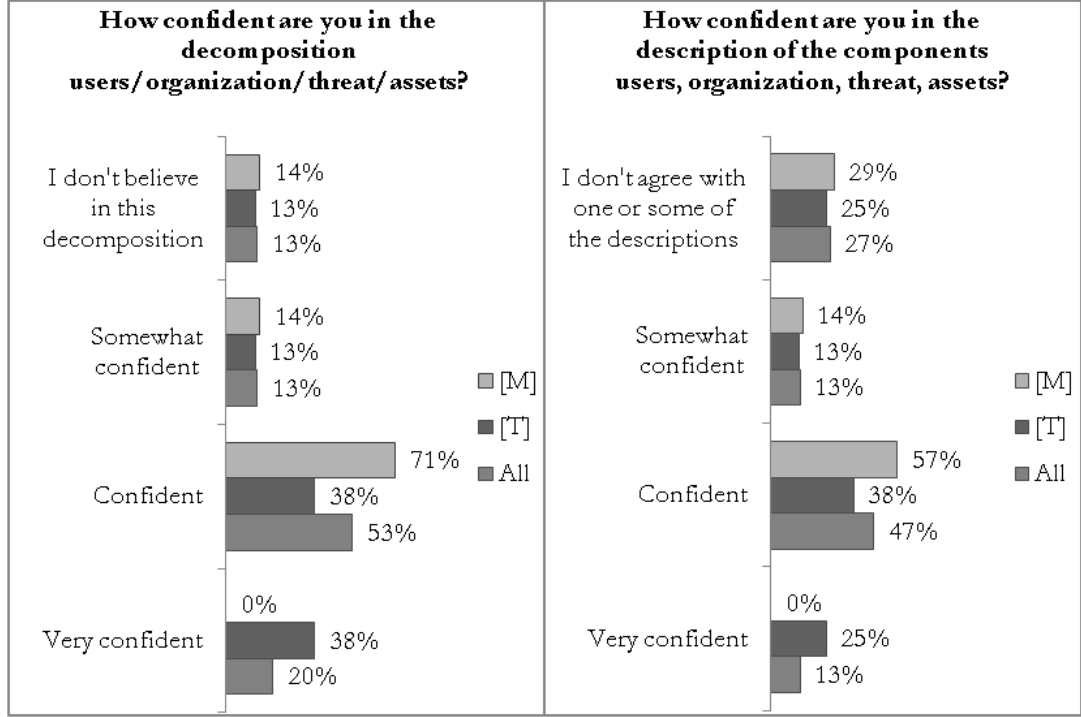


Figure 4.8: Confidence of Experts in the Decomposition and Description Users, Organization, Threat and Assets

influence. The list of characteristic per component is provided in Table 4.1. The list was reviewed and modified by the Director of Security in order to use terms that would be familiar to IT security officers. When needed, a description was added to the characteristic.

For the purpose of visualizing the results of this part of the survey, we use the following equation to calculate a coefficient assigned to a particular characteristic:

$$c_{x,y} = \frac{\sum_{i=0}^3 (w_i * n_i)}{n_T} \quad (4.1)$$

Where $c_{x,y}$ is the coefficient for characteristic x and group of respondents y (managerial, technical positions, or all positions), i is the strength of the influence (no influence, weak, medium, strong influence), n_i is the number of experts answer-

Table 4.1: List of Characteristics Included in the Survey

| Component | Characteristic |
|--------------|--|
| User | User's Risk Perception User's Trust User's Exposure to Security (for example through media) User's Theoretical Knowledge in Using Computers or/and in Security User's Experience in Using Computers or/and in Security User's Gender User's Age User's Place of Birth User's Role (if the user is an undergraduate/graduate student, a faculty, a staff, an intern, etc...) |
| Organization | Security Awareness Communication to Users Management Understanding of Security Needs Security Team Talent Security Team Qualities (for example withstanding stress) Financial Resources Available for Security Available Security Hardware (for example security devices such as intrusion prevention systems) Available Security Software (for example patches, signatures) Risk Assessment Program Security Policies Organizational Attitude Towards Security Threat Awareness |
| Threat | Attacker's Motivations Attacker's Expertise Attacker's Qualities (for example perseverance) |
| Asset | Value of the Asset from the Attacker's Point of View Value of the Asset from the Organization's Point of View Depth of Protection of the Asset (includes all protections of an asset - passwords, firewalls...) |

ing influence i for characteristic x , n_T is the total number of respondents, w_i is the weight assigned to the influence of strength i (0, 1, 2, and 3 for no influence, weak, medium, and strong influence respectively).

Let us illustrate this equation through the results for characteristic "User's Risk Perception" for all respondents. Table 4.2 provides the number of respondents

per influence. The calculated coefficient is 2.6.

Table 4.2: Example to Find the Coefficient Associated to the User’s Risk Perception for All Respondents

| Influence i | Number of respondents n_i | Weight for influence i | $w_i * n_i$ |
|------------------|--------------------------------|--------------------------|--------------------|
| No influence | 0 | 0 | 0 |
| Weak influence | 1 | 1 | 1 |
| Medium influence | 4 | 2 | 8 |
| Strong influence | 10 | 3 | 30 |
| | $n_T = 15$ | | $c_{UR,all} = 2.6$ |

Based on its definition, $c_{x,y}$, ranges from 0 to 3. If all experts answer that characteristic x has no influence on security, then the coefficient will be 0. On the contrary, if all experts answer that a characteristic has a strong influence on security, then the coefficient will be 3. For a given characteristic x , a coefficient is calculated for each group of respondents (managerial and technical positions, all positions), leading to three numbers for each characteristic. This is done for all characteristics included in the survey. The results are shown in Figure 4.9. All three numbers are represented on a unique vertical line. If all three numbers are stacked (for example for characteristic “User’s Experience in Using Computers or/and in Security”, respondents from managerial positions and from technical positions agree. On the contrary, if the three points are spread (characteristic “User’s Exposure to Security”), there is a disagreement between experts.

The results do not show a strong disagreement between groups of experts. At one end of the spectrum, the characteristics for which there is the strongest agreement are: “Organizational Attitude towards Security”, “User’s Theoretical

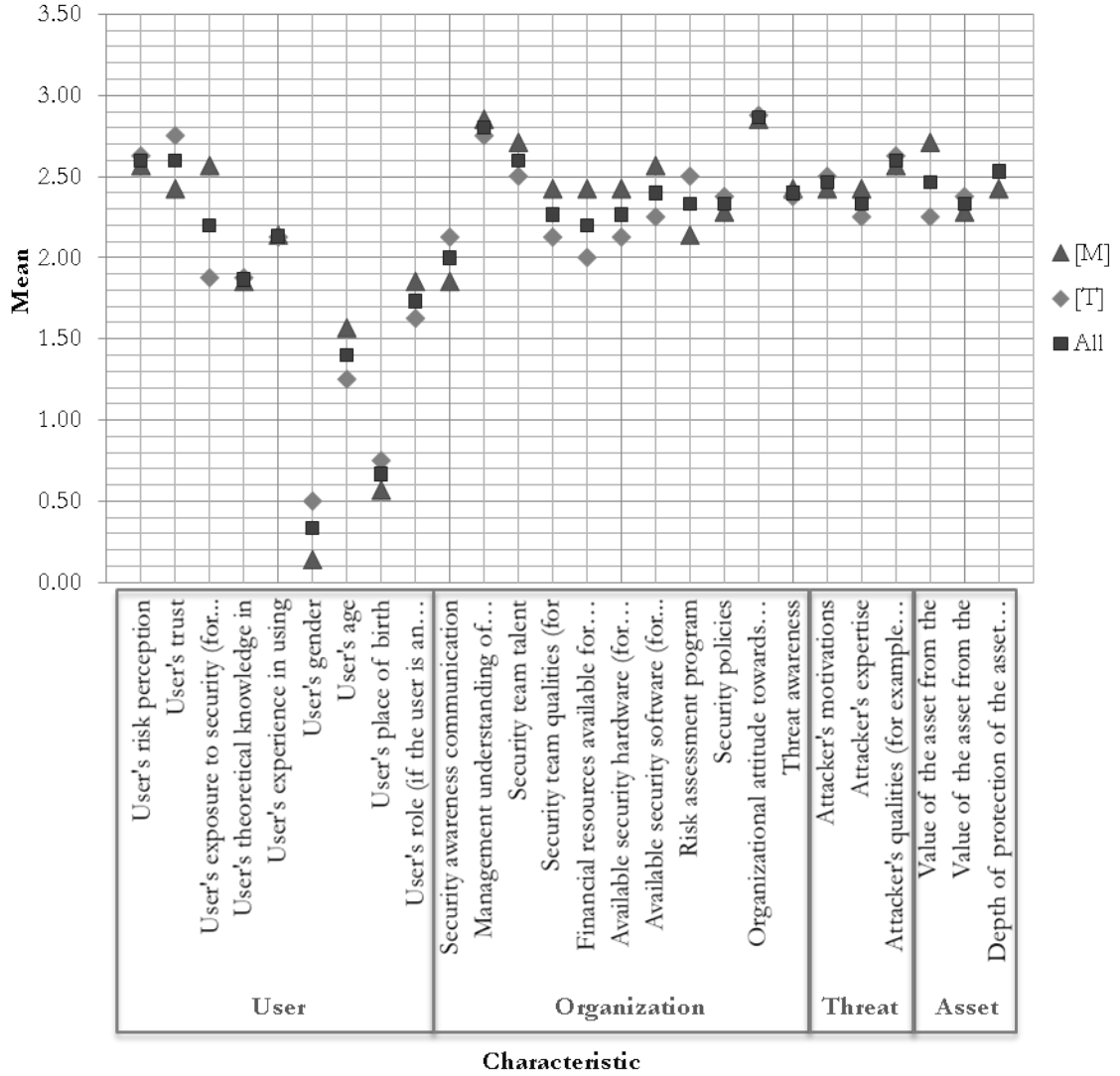


Figure 4.9: Influence of Each Characteristic on Security

Knowledge and Experience in Using Computers or/and in Security”. At the other end of the spectrum, the strongest disagreement is on the “User’s Exposure to Security”. However, if we look more closely at the raw numbers on the “User’s exposure”, we see that 63% of technical positions think that there is a medium influence on security, whereas 71% of managerial people think that it is a strong influence. In summary, both groups do not strongly disagree as they believe there

is a relatively important influence (medium or strong).

We can draw two conclusions from the analysis of Figure 4.9. First, there is no characteristic for which there is a big difference between technical and managerial positions (for example, for a given characteristic, coefficients of 0.5 and 2.5 for technical and managerial positions): thus, there is a consensus between the two groups. Second, when we look more closely at the characteristics where there would be a difference, even small, such as the “User’s Exposure”, the gap is not due to a strong disagreement between respondents (for example one group saying low influence, the other strong influence). Therefore, we do not lose much insight by only looking at the aggregated number (all positions), as it is depicted in Figure 4.10.

In Figure 4.10, lines show the limits between strong, medium, low and no influence. Table 4.3 supported the choice of these limits: characteristics are ordered by decreasing coefficient. The third column depicts the difference in coefficient with the previous characteristic. This table supported discussions with the Director of Security at UMD to determine the limits between strong, medium, low, and no influence.

4.4.5 Outputs

First, the results of these surveys allowed us to have an overview of the characteristics to include in the model. Those for which no influence was identified were discarded: “User’s Age”, “User’s Gender” and “User’s Place of Birth”. Second, we identified the strength of remaining characteristics on security (Table 4.4).

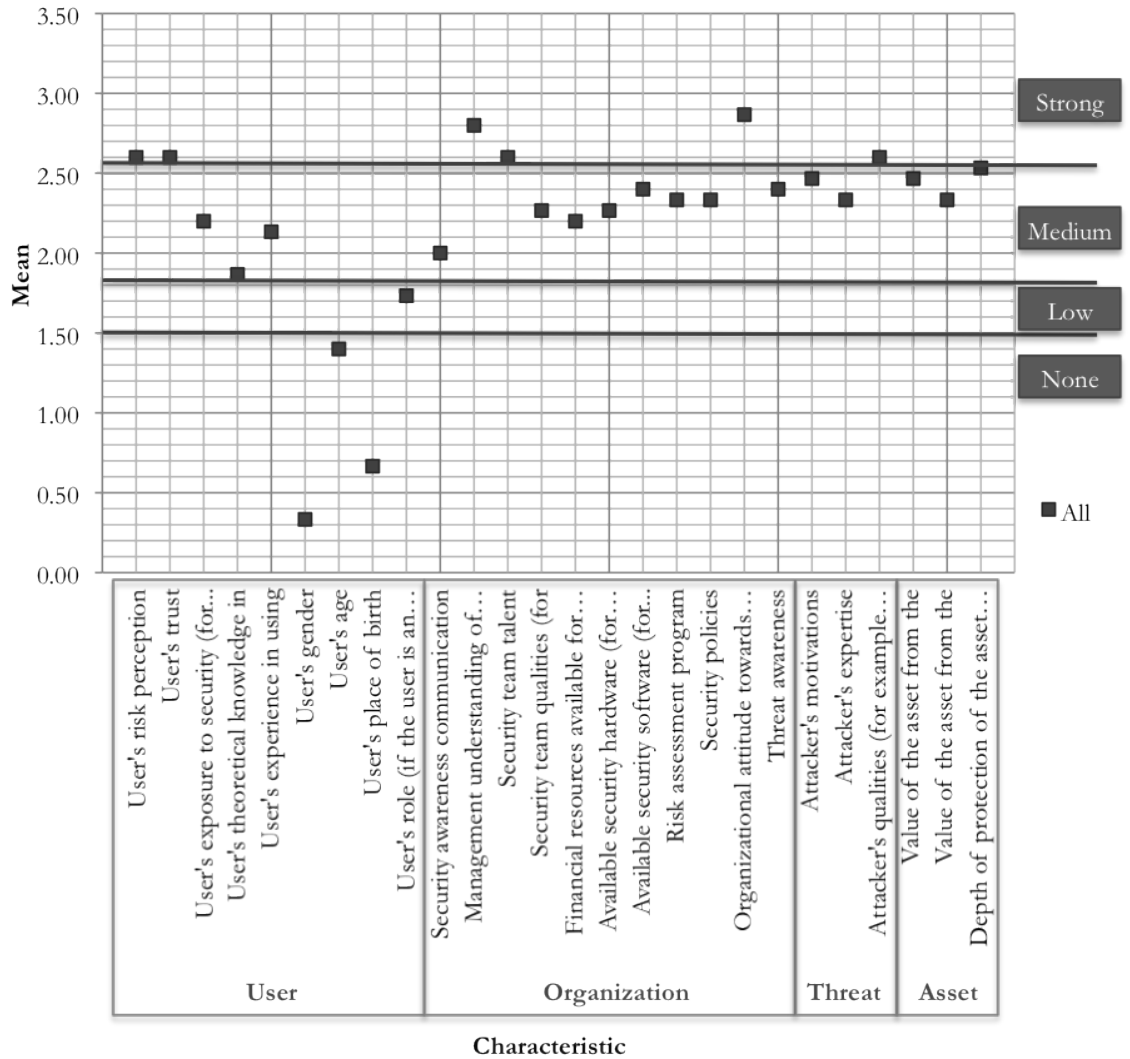


Figure 4.10: Limits between Strong, Medium, Low and No Influence

Deciding on which characteristic to include in strong, medium, low or no influence, is based on our interpretation. We do not expect all readers to agree with the thresholds set in this dissertation but we provide the methodology and the results of the surveys so that people can reproduce this analysis with their own thresholds. More detailed results on the survey are provided in Appendix C.

Table 4.3: Ranked Coefficients

| Characteristic | Coefficient | Difference |
|---|-------------|------------|
| Organizational attitude towards security | 2.87 | - |
| Management understanding of security needs | 2.80 | 0.07 |
| User's risk perception | 2.60 | 0.2 |
| User's trust | 2.60 | 0 |
| Security team talent | 2.60 | 0 |
| Attacker's qualities (for example perseverance) | 2.60 | 0 |
| Depth of protection of the asset (includes all protections of an asset - passwords, firewalls...) | 2.53 | 0.07 |
| Attacker's motivations | 2.47 | 0.07 |
| Value of the asset from the attacker's point of view | 2.47 | 0 |
| Available security software (for example patches, signatures) | 2.40 | 0.07 |
| Threat awareness | 2.40 | 0 |
| Risk assessment program | 2.33 | 0.07 |
| Security policies | 2.33 | 0 |
| Attacker's expertise | 2.33 | 0 |
| Value of the asset from the organization's point of view | 2.33 | 0 |
| Security team qualities (for example withstanding stress) | 2.27 | 0.07 |
| Available security hardware (for example security devices such as intrusion prevention systems) | 2.27 | 0 |
| User's exposure to security (for example through media) | 2.20 | 0.07 |
| Financial resources available for security | 2.20 | 0 |
| User's experience in using computers or/and in security | 2.13 | 0.07 |
| Security awareness communication to users | 2.00 | 0.13 |
| User's theoretical knowledge in using computers or/and in security | 1.87 | 0.13 |
| User's role (if the user is an undergraduate/graduate student, a faculty, a staff, an intern, etc...) | 1.73 | 0.13 |
| User's age | 1.40 | 0.33 |
| User's place of birth | 0.67 | 0.73 |
| User's gender | 0.33 | 0.33 |

Table 4.4: Characteristics and their Strength on Security

| Component | Characteristic | Strength on Security |
|--------------|---|----------------------|
| User | User's Risk Perception | Strong |
| | User's Trust | Strong |
| | User's Exposure to Security (for example through media) | Medium |
| | User's Theoretical Knowledge in Using Computers or/and in Security | Weak |
| | User's Experience in Using Computers or/and in Security | Medium |
| | User's Role (if the user is an undergraduate/graduate student, a faculty, a staff, an intern, etc...) | Weak |
| Organization | Security Awareness Communication to Users | Weak |
| | Management Understanding of Security Needs | Strong |
| | Security Team Talent | Strong |
| | Security Team Qualities (for example withstanding stress) | Medium |
| | Financial Resources Available for Security | Medium |
| | Available Security Hardware (for example security devices such as intrusion prevention systems) | Medium |
| | Available Security Software (for example patches, signatures) | Medium |
| | Risk Assessment Program | Medium |
| | Security Policies | Medium |
| | Organizational Attitude Towards Security | Strong |
| | Threat Awareness | Medium |
| Attacker | Attacker's Motivations | Medium |
| | Attacker's Expertise | Medium |
| | Attacker's Qualities (for example perseverance) | Strong |
| Asset | Value of the Asset from the Attacker's Point of View | Medium |
| | Value of the Asset from the Organization's Point of View | Medium |
| | Depth of Protection of the Asset (includes all protections of an asset - passwords, firewalls...) | Medium |

4.5 Developing the Final Model

4.5.1 Objective: Aggregating the Results of the Interviews and Surveys

At this point, we have two models from the interviews, one extended model developed at UMD, and insights from the surveys. These three sources of information will be used to develop an aggregated model, which will be shown to experts for validation (Figure 4.11). On the one hand, surveys will be used to identify the characteristics to include in the model and give an idea of the strength of their influence on security. On the other hand, the resulting models from the interviews and from our discussions with the Director of Security at UMD will serve through the structure. The idea is to merge insights from the three models into one model.

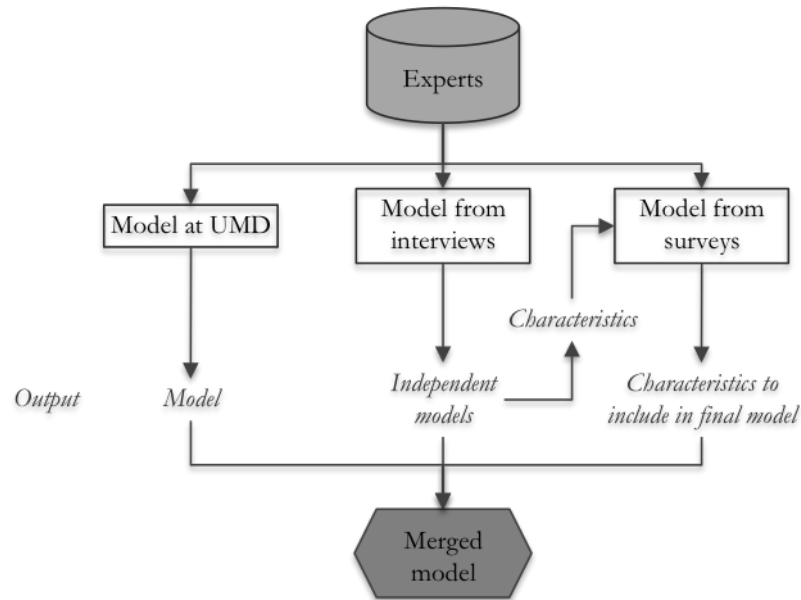


Figure 4.11: Flowchart of the Model Development Process

An issue that was raised when trying to merge these models is: how can we aggregate several influential models? As opposed to reaching a consensus between

experts present at the same time in the same location, independent interviews that led to independent models require that the analyst develops a process to aggregate all models. This step necessarily contains some subjectivity. The final model, based on interviews and surveys (surveys will be discussed in the next section), is based on the interpretation of the analyst. However, we provide in this dissertation all the results so that analysts who disagree can reuse the results of this study. The process is described in Figure 4.12 and identifies three steps that are described in the next subsections.

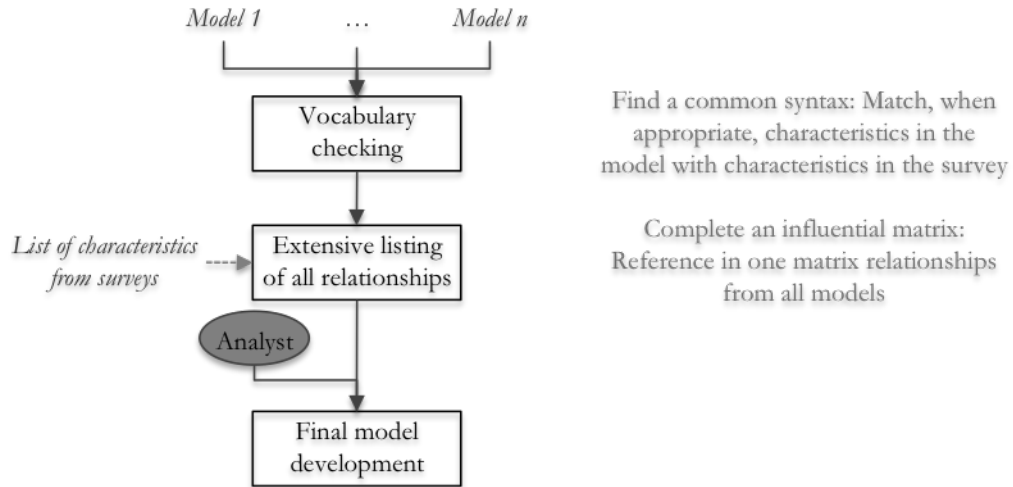


Figure 4.12: Process to Aggregate Several Influential Models?

4.5.2 Step 1: Vocabulary Checking

In this first step, the objective is to match characteristics identified by interviewees with characteristics in the survey. The objective is to obtain a common syntax between all models and the survey. For example, Expert 1 identifies “User Security Awareness”. We are confident in the mapping between that characteristic and the “User’s Risk Perception” identified in the surveys. However, mapping

between characteristics may not be obvious. On the one hand, characteristics identified by interviewees may be too broad: the Director of Security at UMD identifies the availability of resources, which includes characteristics such as “Financial Resources Available for Security”, “Available Security Hardware” and Available Security Software. On the other hand, experts may be too specific: Expert 2 identifies characteristics “C, A, I”, “Access (Physical, Remote, Authorized)”, “Logs”; they are included in characteristic “Depth of Protection of the Asset” in the survey. The mapping shown in Table 4.5 was reviewed and confirmed by the Director of Security at UMD. Table 4.5 also provides abbreviations for each characteristic that will be used in the next subsection.

4.5.3 Step 2: Extensive Listing of all Relationships

Once all characteristics identified by interviewees have been mapped with characteristics selected in the survey, the next step consists in identifying all relationships. In order to have a user-friendly overview of these relationships, we will use a matrix, shown in Figure 4.13:

- If characteristic A influences characteristic B, we find A in the first column and B in the first line. The intersection between the row of A and the column of B contains the relationships identified by interviewees (Director of Security at UMD, Expert 1, and Expert 2),
- In each cell, direct influences (for instance A directly influences B) are depicted by a number. 1, 2, and 3 represent a weak, medium, and strong influence in the model drawn by the expert respectively. Indirect influences (for instance A

Table 4.5: Characteristics and their Influences in Experts' Models

| Survey | | UMD | Expert 1 | Expert 2 |
|--|----|--|-----------------------------|---|
| User's Risk Perception | UP | User's Risk Perception | User Security Awareness | - |
| User's Trust | UT | User's Trust | - | - |
| User's Exposure to Security | UE | User's Exposure to Security | - | - |
| User's Theoretical Knowledge in Using Computers or/and in Security | UK | User's Theoretical Knowledge in Using Computers or/and in Security | Training | - |
| User's Experience in Using Computers or/and in Security | UX | User's Experience in Using Computers or/and in Security | | - |
| User's Role | UR | User's Involvement | - | - |
| Security Awareness Communication to Users | OC | Organization Communication | Communication | - |
| Management Understanding of Security Needs | OU | - | - | Internal Communication |
| Security Team Talent | OT | IT Team's Expertise in Security | Security Officers Qualities | Availability of Expertise to IT Security Team |
| | | | | Training, Education |
| | | | | Availability of Relevant Knowledge |
| Security Team Qualities | OQ | IT Team's Personal Qualities | | - |
| Financial Resources Available for Security | OF | Availability of Resources | Budget | - |
| Available Security Hardware | OH | | - | - |
| Available Security Software | OS | | Patches | - |
| Risk Assessment Program | OR | - | - | Risk Evaluation |
| Security policies | OP | - | Policy | - |
| Organizational Attitude Towards Security | OA | - | Culture | Defined Scope of Authority |
| | | | | Defined Scope of Responsibility |
| | | | | Defined Goals at Organization |
| Threat Awareness | OW | - | Threat Awareness | - |
| Attacker's Motivations | AM | Attacker's Motivations | Attackers Willingness | Malicious Intent |
| Attacker's Expertise | AE | Attacker's Expertise | Attackers Knowledge | - |
| Attacker's Qualities | AQ | Attacker's Personal Qualities | - | - |
| Value of the Asset from the Attacker's Point of View | AA | Value of the Asset from the Attacker's Point of View | - | - |
| Value of the Asset from the Organization's Point of View | VA | Value of the Asset from the IT Team's Point of View | - | Definition and Identification of Assets |
| Depth of Protection of the Asset | PA | Level of Protection for the Asset | Security Team Management | C, A, I |
| | | | User Management | Access (Physical, Remote, Authorized) |
| | | | | Logs |

influences B through characteristic C) are depicted by a star “*”. No influence is depicted by a dash “-”,

- In each cell, all three models are represented. For instance if for statement “A influences B”, the Director of Security at UMD identifies a strong direct influence, Expert 1 an indirect influence and Expert 2 no influence, we have “3*-”,
- All 24 characteristics that were identified in the survey are represented in the matrix through an abbreviation that is referenced in Table 4.5. For instance, the depth of protection of the asset is represented in the matrix as PA. A column security is added to represent the influences on security. As it is the final node in the model, security does not have child nodes and do not need to be represented as a line in the matrix,
- The last column summarizes the strength of the influence of each characteristic on security identified through the survey. 1, 2, and 3 represent a weak, medium and strong influence respectively,
- The last line represents the number of parents for each characteristic depicted in the column,
- The diagonal is shaded for ease of reading. If numbers or stars are in the diagonal, it means that experts depicted loops in their model.

| 🏠 | UT | UA | UR | UE | UP | UK | UX | OF | OH | OS | OT | OQ | OP | OU | OA | OR | OC | OW | PA | AA | VA | AM | AQ | AE | Sec | Surv |
|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|------|
| UT | --- | --- | --- | 1-- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 3 |
| UA | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 1 |
| UR | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| UE | --- | --- | --- | 3-- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| UP | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 3 |
| UK | --- | --- | --- | --- | 2-- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| UX | --- | --- | --- | --- | 2-- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| OF | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| OH | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| OS | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| OT | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 3 |
| OQ | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| OP | --- | --- | --- | --- | 1- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| OU | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 3 |
| OA | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 3 |
| OR | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| OC | --- | --- | --- | 3-- | 2- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| OW | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| PA | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 3 |
| AA | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| VA | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| AM | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| AQ | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 3 |
| AE | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | 2 |
| | 0 | 0 | 0 | 1 | 8 | 3 | 3 | 10 | 0 | 0 | 3 | 0 | 3 | 0 | 1 | 5 | 2 | 4 | 17 | 0 | 2 | 2 | 0 | 0 | 23 | |

Figure 4.13: Influential Matrix

4.5.4 Step 3: Final Model Development

The final step consists in developing a unique model based on the interviews and the survey. The final model is based on our interpretation of the results but we reduce the subjectivity involved in the process by taking the following control steps:

- We pushed the analysis to be as formal as possible, with the definitions of the coefficient and matrix for instance,
- The Director of Security at UMD was involved along the entire process and gave his acknowledgement at each milestone, such as the interview and survey designs, or the merging process. This ensures the credibility of the model.

The objective of this subsection is not to exhaustively describe how the model was built but to provide general guidelines that allowed us to develop such a model. We try to reference our justifications on the building process but despite our efforts, the reader may disagree with these guidelines. Therefore, we provide in this dissertation the results of the interviews and survey so that analysts who disagree can develop their own model.

The following list provides with a set of guidelines to develop the final model:

- An initial step (Step 0) aims at rearranging the previously presented matrix (Figure 4.14). The matrix should be rearranged so that columns are ranked in the order of increasing number of parents p_i and the lines are in the same order (labeled “1” and “2” in Figure 4.14). Ranking the columns by increasing p_i enables building the nodes at the top of the model first (with few parents), then

progressing towards deeper layers in the model (nodes with many parents),

- The first step (Step 1) allows building the primary structure of the model, based on direct influences only (depicted by numbers in the matrix, versus “*” and “-”), without taking care of the strength of the influences,
- Through Step 2, we add indirect influences to the primary model if they are not already there. At this point, the relationships are built. The next steps consist in adding the strength of these relationships,
- In Step 3 of the process, the model is enhanced with the strengths of direct relationships. Numbers 1, 2, and 3 for weak, medium, and strong influence in the matrix allow adding the strength of these direct relationships in the model,
- Step 4 is less formal than the previous steps. Strengths of relationships that have not been added through Step 3 are determined based on the judgment of the analyst. This task is supported by the last column of the matrix that references the impact of each characteristic on security from the analysis of the surveys,
- By definition, the characteristics we have selected and included in the matrix all have an influence on security, which was demonstrated through the surveys. Therefore, Step 5 consists in linking all nodes to security, directly or indirectly.

We had several discussions with the Director of Security at UMD. He followed the entire development process and agreed that the model we obtained after the five

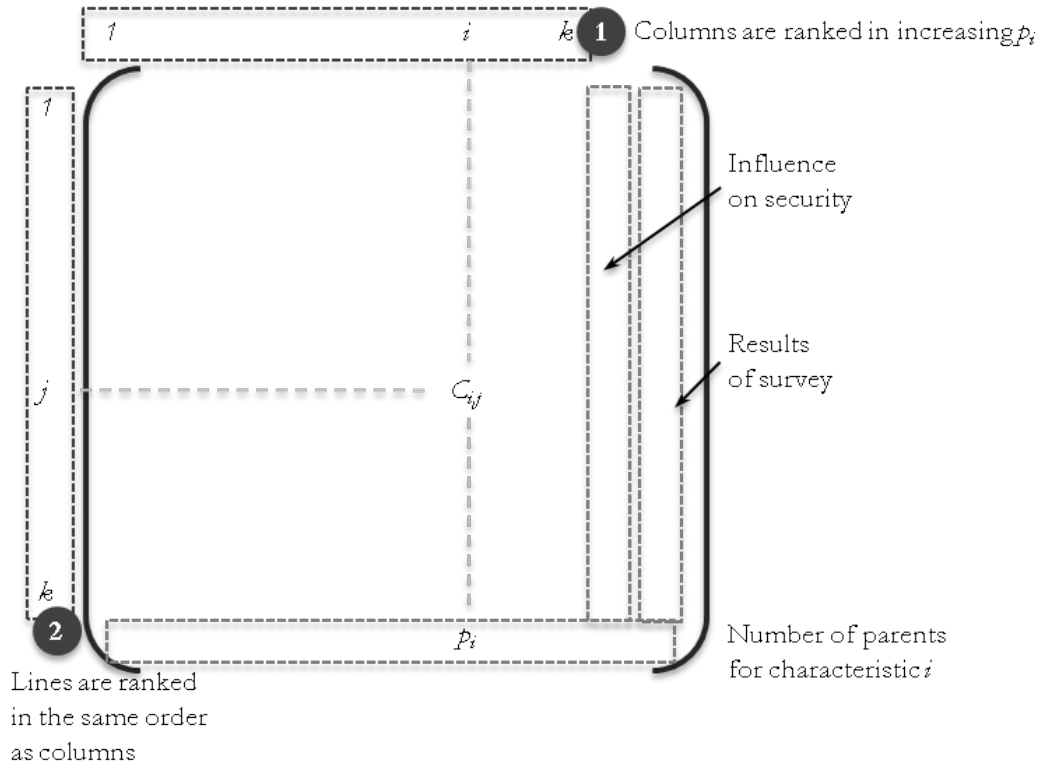


Figure 4.14: Initial step (Step 0) of the Final Model Development

steps described above led to a too complicated model. The Director of Security did not agree on everything that was in the model. We modified the model accordingly. Finally, we decided to merge few characteristics because separating them did not bring a additional refinement to the model. For example, available security hardware and additional software were combined together. The resulting model is presented in Figure 4.15. Validation of this model is presented in Chapter 5.

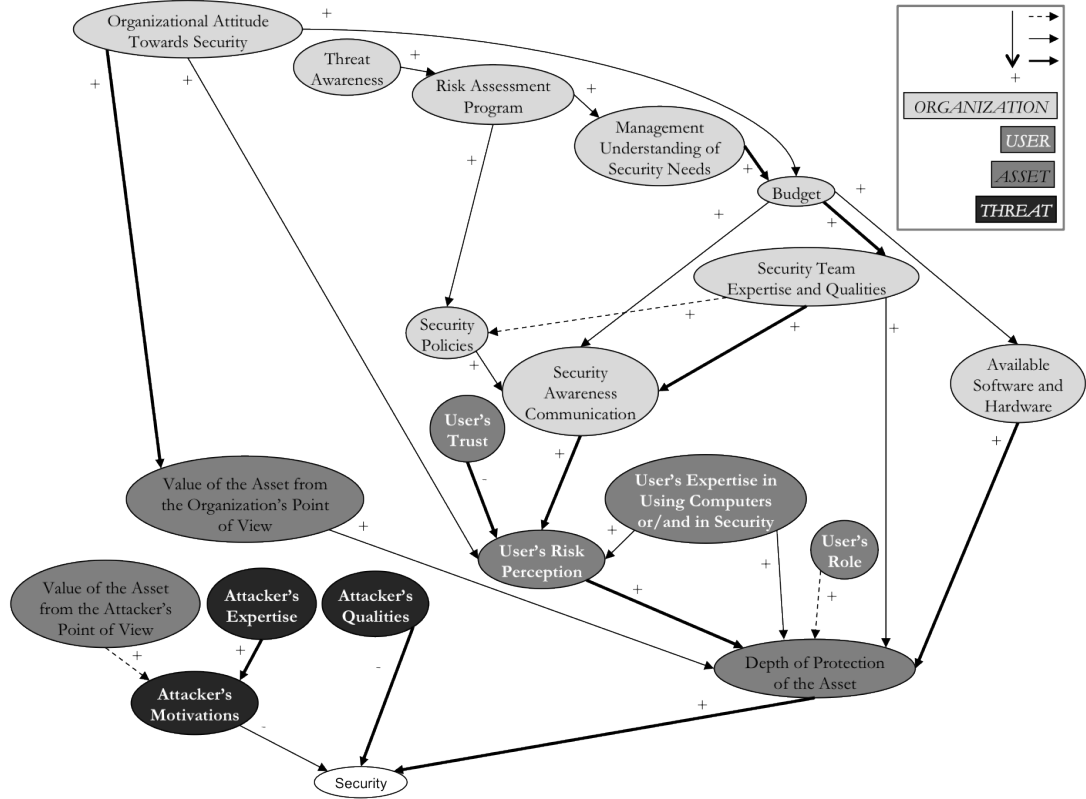


Figure 4.15: Model before Validation

4.6 Summary

In Chapter 4, we presented the results of the development of a model for universities environments. A model based on the literature and on insights from the Director of Security at UMD led to the development of an extensive model. Two other models were developed through interviews with experts in other academic environments. Surveys were conducted to gather opinions of a larger population of experts: the survey was sent to a listserv of 600 IT security officers and fifteen experts accepted to answer the survey. We presented the method to merge all sources of information to develop a unique model. The resulting model can be submitted for the validation process.

Chapter 5

Model Validation

5.1 Introduction

In this chapter, we present the approach for model validation, which relies on two steps:

- Validation by experts,
- Validation with case studies.

We contacted experts from interviews and surveys, who provided us with their email address. The objective was to obtain their agreement or comments on the model presented in Figure 4.15. A model resulting from these insights and from discussions with the Director of Security at UMD was developed and ready for the second step of validation. This first step of model validation is described in the first section of this chapter.

In the second section, we present an approach to validate the model through case studies. We collected a list of implemented security measures at UMD since 1996. Two additional datasets are available and consist in the number of accounts corrupted by phishing attacks and the number of incidents. The objective is to study the trend of these data after the implementation of a measure through the Laplace trend test. The measure is mapped to a path in the model and when the outcomes of the analysis match the consequences expected after the implementation of the measure, we have more confidence in the identified path. We present the results of

the validation of parts of the model through case studies and list the limitations inherent to this analysis.

5.2 Validation by Experts

5.2.1 Objectives

The model presented in Figure 4.15 was sent by email to interviewed experts (Expert 1 and Expert 2) and to the three experts who took the survey and provided their email address. The email also included a description of the project, of the model components, and the following questions:

- What do you think of the decomposition user/organization/threat/asset and the descriptions?
- Do you think we included all characteristics that influence security in the model or would you add or delete some characteristics?
- Would you modify the strengths of some influences in the model (meaning: change the thickness of the arrow)?
- What are your general thoughts on the model?
- How could this model help you in your work?

5.2.2 Results of the Validation by Experts

We received feedback from two experts: Expert 1 and one expert who took the survey, named Expert 4 for the remainder of the dissertation.

Expert 1 agreed with the presented components' description and model. No changes were recommended. Expert 1 believes that this model can be useful in communicating with “directors and managers of OTS” (Office of Information Technology) and in the risk assessment process as the model allows listing all aspects that should be considered in the risk assessment process.

Expert 4 sent a detailed modified model presented in Figure 5.1. He believes that this type of model is “a good exercise in attempting to understand some of the key components of communications and their relationship”. We appreciated the effort of the expert, who spent a significant amount of time to send us a new version of the model. He highlighted that he could spend much more time on it before he would be fully satisfied. Although he kept the four components when building a model, he suggested decomposing security into more layers than the four we mentioned. Although we agree with his comments, as the model could be more detailed and could include more layers of decomposition, our primary objective is to develop a model useful for communication purposes. In that sense, the model should not be too detailed and complex.

5.2.3 Resulting Model

The model was modified according to comments provided by experts and discussions with the Director of Security. Modifications include:

- Including a more general component “Attacker’s Resources”: Expert 4 identified several components of the attacker, that we decided to include under a single component “Attacker’s Resources”. The justification is that we cannot

managers, there should be a risk assessment program in place,

- Adding an influence from the “Security Awareness Communication” to the “User’s Expertise in Using Computers or/and in Security”: Awareness campaigns towards users help educating users on security issues, hence impact their expertise.

The modified model is presented in Figure 5.2. The next step is to validate parts of the model with case studies.

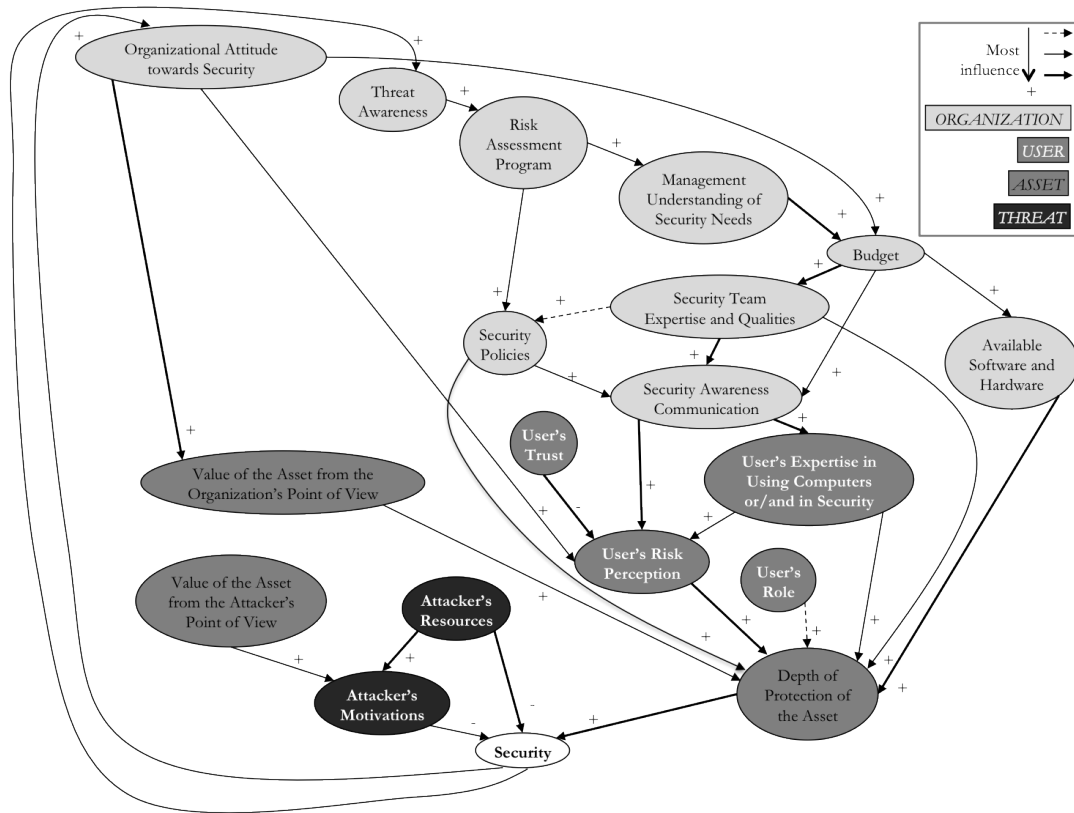


Figure 5.2: Model Validated by Experts

5.3 Validation with Case Studies

5.3.1 Objectives

Specific case studies at UMD for which data are available are used to validate the model.

The measurement of characteristics in the model can be direct or indirect. Direct measurements, or metrics, are values that directly quantify characteristics. For example, the carbon footprint is a metric of one’s impact on the environment. Indirect measurements, or indicators, indirectly quantify characteristics. The Gross Domestic Product (GDP) is an indicator of a country’s economy and reveals how well the economy is in a country. Indicators were introduced in Section 3.4.4.4.

This dissertation does not include a quantitative framework of the model. In other words, if we manage to measure characteristics in the model based on data, we cannot propagate these measures in the model in order to obtain a numerical value for characteristic “Security”.

Furthermore, we are not able to measure all characteristics in the model because we may not know how to quantify them (for example, characteristic “Organizational Attitude towards Security”), or because we cannot quantify them (attackers characteristics may be difficult to quantify as it may be difficult to gather information on attackers). However sensitivity analyses can be performed: by changing one factor, one sees how the change affects the model, hence security.

The objective of the validation with case studies consists in validating the influences between characteristics. Data support the measurements of characteristics

in the model. The outcomes of the model are compared against data. For example, let us consider a case study that consists in implementing security solution S. This solution was implemented in the organization and data on the number of corrupted computers per day are available. The first step of the validation consists in relating measure S to one or several characteristics in the model. Other available data may provide information on other characteristics. All pieces of data, associated to characteristics in the model, translate into a low, medium, or high value characteristics. By propagating them into the model, we can determine a low, medium, or high value of our node of concern “Security”, or an increasing or decreasing level of security. Let us assume that solution S can be mapped to characteristic A in the model, which has a positive influence on security. In other words, according to the model, implementing solution S should improve the overall security. The second step of the validation consists in analyzing the rate of corrupted computers and determining the trend after the implementation of measure A. Under the assumption that the number of corrupted computers is an indicator of security, the trend after measure S is implemented is compared to the outcome of the first step. If they match, we have more confidence in the positive influence of characteristic A on characteristic “Security”. If they don’t match, the model may need to be modified accordingly.

We present the results of several case studies at UMD. In addition to the security measures implemented at UMD, three types of data are considered to support these case studies: Intrusion Prevention System (IPS) data, incidents, and accounts corrupted by phishing.

5.3.2 The University of Maryland

The environment under study and available for the validation through case studies is the University of Maryland, College Park, which is a public research university. The average enrollment over the last ten years is 35,754 students and the average campus population is 43,613 people. The campus population includes undergraduate and graduate students, faculty members, instructors and lecturers, and staff. The number of people included in each category from 2001 to 2010 is shown in Table 5.1. The total campus population is a good approximation of the number of users at UMD.

5.3.3 Available Data

5.3.3.1 List of Security Measures

In order to investigate the impact of security measures, the Director of Security at UMD provided us with the list of measures implemented at UMD since 1996. The list of measures are provided in Table 5.2. It was challenging to obtain the exact dates of these measures, this is the reason why for some of them, only the year is available. This is especially the case for events that occurred before 2001. In addition, we do not need all exact dates: this will later be explained in the chapter.

Table 5.1: Campus Population between 2001 and 2010 - Data show statistics for academic years starting in Fall

| Category | 2001 | 2002 | 2003 | 2004 | 2005 | 2006 | 2007 | 2008 | 2009 | 2010 |
|---------------------------|--------|--------|--------|--------|--------|--------|--------|--------|--------|--------|
| Undergraduate students | 25,099 | 25,240 | 25,446 | 25,140 | 25,442 | 25,154 | 25,857 | 26,475 | 26,542 | 26,922 |
| Graduate student | 9,061 | 9,561 | 9,883 | 9,793 | 9,927 | 9,948 | 10,157 | 10,525 | 10,653 | 10,719 |
| Student enrollment | 34,160 | 34,801 | 35,329 | 34,933 | 35,369 | 35,102 | 36,014 | 37,000 | 37,195 | 37,641 |
| Professor | 695 | 702 | 697 | 695 | 687 | 698 | 680 | 673 | 674 | 681 |
| Associate Professor | 472 | 474 | 460 | 470 | 478 | 466 | 467 | 466 | 455 | 447 |
| Assistant Professor | 325 | 308 | 306 | 274 | 268 | 304 | 325 | 346 | 343 | 335 |
| Other Faculty | 1,370 | 1,430 | 1,474 | 1,424 | 1,503 | 1,460 | 1,476 | 1,475 | 1,593 | 1,687 |
| Faculty | 2,862 | 2,914 | 2,937 | 2,863 | 2,936 | 2,928 | 2,948 | 2,960 | 3,065 | 3,150 |
| Instructors and lecturers | 729 | 742 | 724 | 700 | 738 | 824 | 837 | 907 | 932 | 973 |
| Staff | 4,995 | 5,003 | 4,675 | 4,581 | 4,682 | 4,829 | 4,974 | 5,171 | 5,129 | 4,988 |
| Total campus population | 42,017 | 42,718 | 42,941 | 42,377 | 42,987 | 42,859 | 43,936 | 45,131 | 45,389 | 45,779 |

Table 5.2: List of Security Measures Implemented at UMD

| Date | Security measure |
|-----------|---|
| 1996 | Creation of the project NETHics to promote acceptable use and prosecute IT related student violations |
| 1999 | Creation of the virus notification program to distribute free anti-virus software and to keep users informed on virus outbreaks |
| 2000 | Creation of a security engineer position within the Networking group |
| 2001 | Deployment of Snort Intrusion Detection System (IDS) |
| 2001 | Launch of virtual private network service to provide secure network paths into the campus network |
| 6/17/2002 | Creation of IT Security Officer position within OIT and of one intern position to monitor security events |
| 6/28/2002 | Blocking of routing of Microsoft protocols from outside campus |
| 2003 | Creation of a full-time analyst position reporting to the IT Security Officer |
| 7/2003 | Project NETHics merged with the IT Security Office |
| 7/2003 | Introduction of packetshaping to limit resource consumption by file sharing |
| 5/2004 | Creation of the Security Office as an OIT department reporting directly to VP (Vice President)/CIO |
| 8/2004 | Addition of audit compliance to Security department duties |
| 1/3/2005 | Creation of a second full-time analyst position reporting to the IT Security Officer |
| 1/23/2006 | Creation of a third full-time analyst position reporting to the IT Security Officer |
| 8/2006 | Implementation of a campus password policy with 180 days on password life |
| 8/2006 | Approval of Acceptable Use Policy by Campus Senate |
| 9/01/2006 | Installation of IPSs |
| 2/2007 | Creation of a compliance position |
| 2007 | Launch of Forensics Lab |
| 6/28/2007 | Wireless network put behind IPSs |
| 1/2008 | Protection of OIT Data Centers by firewalls |
| 2008 | Launch of an awareness communication campaign |
| 2009 | Protection of OIT Data Centers by IPS |
| 7/2010 | Addition of Data Policy and Administration to Security Department |
| 9/2010 | Introduction of IronPort anti-spam/anti-malware system to protect campus email |

Some measures are expected to have campus-wide consequences, that is to

say they focus on a large proportion of assets in the organization, such as the hire of analysts to deal with IT security in the university. On the other hand, some measures focus on specific assets such as the OIT data centers.

Before 2002, security was part of the networking group in the OIT department. In 2002, an IT security pole was developed at UMD within the OIT department. This action was accompanied by the advancement of a security engineer in the networking group to the newly created security pole. The engineer was previously in charge of networking duties and incidents monitoring. After his advancement, he focused on security tasks, versus networking tasks. Since then, he directly reports to the deputy Chief Information Officer (CIO). His hire was accompanied by the hire of an intern to support the IT security officer's monitoring duties. Since 2002, several analysts were hired to support IT security at UMD at several levels: prevention, protection, and mitigation. In the next subsections, we present the datasets that could support our analyses.

5.3.3.2 Intrusion Prevention System Data

An Intrusion Prevention System (IPS) is a security device that monitors malicious activity and reacts in real-time by blocking a potential attack. An IPS is considered as an extension of an intrusion detection system (IDS). An IDS is a passive device that monitors activity whereas an IPS is an active device that blocks potential malicious activity. In 2006, signature-based IPSs were installed at the border of the University: the IPS blocking decision relies on a set of signatures that are regularly released by the vendor as attacks are newly discovered on the Internet.

IT security officers choose to enable or disable them. When characteristics of an attack match the ones of a defined signature, the attack is blocked and an alert is recorded in the IPS logs ([33] and [34]).

An alert provides several pieces of information, including the date and time, signature, source IP address, source port, destination IP address, destination port, or the IPS device name that blocked the communication. Organizations use IPSs to monitor their traffic. The monitored activity provides insights into an organization's security and may help identifying potentially corrupted computers. While in some organizations the quantity of monitored traffic is manageable, it becomes a hassle to analyze security data for large organizations. For example, IPSs could record thousands of alerts per day and the security team cannot investigate every alert. Moreover, although IPSs are aimed at detecting and blocking malicious activity, they also raise false alarms. Due to this limitation, we cannot derive indicators of security based on IPS alerts but can be used to support further analyses. This will be shown later in this chapter.

5.3.3.3 Incidents Data

Incidents are daily recorded at UMD, based on three sources of information: 1) intrusion detection system alerts, 2) reports from users, 3) and reports from other system administrators [36]. Each incident is reviewed by security officers and leads to the blocking of the suspicious computer's IP address. As a result, there is no false positive in the incidents data, as opposed to IPS data. It is the reason why the rate of incidents is a relevant indicator of security. Depending on the context,

an increasing or decreasing rate of incidents may provide insights into the level of security of an organization. The incidents are collected at UMD since June 2001.

The objective is to use the incidents data to validate the model. More specifically, we aim at investigating the impact of security measures (such as hiring analysts or installing security devices) on the number of incidents per day. As we are interested in the rate of compromised machines on campus, we use a subset of the incidents data and look at the incidents related to computers on campus. The increasing or decreasing rate of incidents after the implementation of the measure should match the expected outcomes provided by the model for the model to be partly validated.

When proceeding in the analysis of these security measures, we faced several limitations:

- All measures do not have an impact on incident detection. On the one hand, the rate of incidents is expected to be impacted by the hire of analysts, who work on identifying incidents. On the other hand, password policies are not expected to have a consequence on the incidents. In addition, some measures are implemented to solve a problem, such as the blocking of the Microsoft protocols routing, whereas others are implemented in prevention of future attacks. For example, it was decided to protect data centers by putting them behind firewalls in 2008 and behind IPSs in 2009. No incident on the OIT data centers was previously recorded but the measure was implemented to prevent a harmful loss of the data centers. These reasons also explain why we did not

try to gather exact dates for all security measures, as all measures are not expected to impact the rate of incidents,

- We should account for a delay after which the measure becomes effective. For example, when analysts are hired, they go through a training phase. Therefore, the expected decrease in the rate of incidents may appear several weeks after they were hired. This delay is indeed difficult to assess accurately but the Director of Security at UMD gave us, when possible, orders of magnitude for these periods,
- As each suspicious IP address is reviewed by a security officer, we are sure that it is corrupted, but the number of incidents per day may be bounded by the number of available IT security staff, as each IT security officer may be able to handle only a few incidents per day. The number of incidents per day may also depend on the type of incident. Indeed, if there is a fast spreading worm, users may be reactive to report it and analysts learn to detect the same type of incident, which would lead in a high number of incidents per day,
- Although the incidents data do not include false positives, we are concerned by not having all pieces of information. Indeed, if the analysis reveals that the measure decreases the rate of incidents, several reasons other than the implementation of the measure may explain it. For example, reasons include the campus population (less populated during summer and winter breaks), the IT security team size (if analysts are on vacation, therefore fewer employees to deal with incidents), or the attack pattern (campus not being targeted at

that period) may explain it.

5.3.3.4 Number of Corrupted Accounts by Phishing Attacks

In 2008, there was a significant number of successful phishing attacks targeting UMD accounts. Phishers sent emails to UMD users that appeared to be sent by OIT, requiring users to reset their usernames and passwords through a webpage that was very similar to one OIT could have designed. Once accounts are corrupted, they are used to send mass phishing emails. Due to the noise these phishing emails make on the network, IT security officers manage to shut down the account within hours. The number of accounts corrupted by phishing attacks (or the number of successful phishing attacks) indicates how well users perceive risks related to phishing attacks. The dates and user accounts are saved in a database.

When using this dataset, we consider the following:

- We want to emphasize that this dataset only includes accounts corrupted by masquerading the University entity. For example, they do not include phishing attacks that aim at stealing bank or Yahoo email credentials,
- Because of the method of identification of corrupted accounts, there is no false positive in the dataset,
- Data does not include cases where the phisher steals a user's credentials without using them.

5.3.4 Laplace Trend Values

As previously mentioned, the objective is to identify trends in the datasets after the implementation of a security measure. The Laplace trend test allows identifying trends in a dataset based on the Laplace trend value $u(k)$ for period $[0, k]$ and is defined as:

$$u(k) = \frac{\frac{\sum_{i=1}^k ((i-1)*n_i)}{N(k)} - \frac{k-1}{2}}{\sqrt{\frac{k^2-1}{12*N(k)}}} \quad (5.1)$$

where,

- k is the day number
- n_i is the number of incidents or successful phishing attacks during day i ,
- $N(k)$ is the cumulative number of successful attacks until day k .

The practical interpretation of the Laplace trend analysis can be done at two levels [70]:

- Globally: If the Laplace trend values are positive (respectively negative), there is a global increase (respectively decrease) in the rate of successful phishing attacks. Values between -2 and $+2$ indicate stability,
- Locally: Increasing (respectively decreasing) values indicate a local increase (respectively decrease) of the rate of successful phishing attacks.

5.3.5 Approach

In subsection 5.3.1, we presented the objectives of the validation through case studies. More specifically, the approach consists in looking at trends of indicators: the number of incidents is considered an indicator of “Security” whereas the number of successful phishing attacks (or number of corrupted accounts by phishing attacks) is considered an indicator of the “User’s Risk Perception”. In other words, we want to study their Laplace trend values to study the impact of the implementation of a security measure. If the trend observed after the implementation of a measure matches its expected consequences, the confidence in the portion of the model concerned with the measure is increased.

When calculating the Laplace trend values, we should select an appropriate starting date. The trade-off consists in choosing a starting date so that we have enough data before the implementation but not too much, as a too long history may interfere in the interpretation of the results. We decided to start the analysis one month before the implementation of the measure, when possible. On the other hand, the choice of the end date is more flexible. If we want to observe effects on the long term, the analysis may be done over several months, six for example. If we want to focus on the short term, we may only need one or two months of Laplace trend values.

We will show Laplace trend values over a period of several months to be able to investigate impact on a longer term. As the environment quickly changes, with the change in campus population but also to the attack profiles, there is a limit beyond

which trying to observe the effects of the implementation of a measure is useless. We will show the Laplace trend values over a period of eight months, although we might make our observations on a shorter time window. For most measures, we do not think that the consequences are observable beyond eight months. However, if we need a longer time window, we can lengthen it for specific case studies.

Several discussions with the Director of Security at UMD were conducted in order to identify expected consequences of the implementation of a measure. For example, if an analyst is hired, his/her duties may focus on incidents detection, or on prevention. If his/her focus is on incidents detection, we expect to see an increase in the rate of incidents on the short term because there are more resources to deal with incidents. If the analyst is also expected to work on prevention, the effects may be noticeable on the long term by an overall decrease in the rate of incidents. Besides, discussions with the Director of Security also allow mapping the security measure to the model. For example, we need to understand why the hire of an analyst occurred. An analyst may be hired for at least two reasons: 1) budget becomes available, or 2) there is a need for hiring an IT security officer. In the first case, the measure is mapped to characteristic “Budget” in the model, while in the second case, it is mapped to “Security Team’s Expertise and Qualities”. Besides, we need to capture the exact tasks of the analyst in order to identify the path under validation in the model. In the second example mentioned above, if the analyst is mainly in charge of awareness or policies, the path under validation is different. Therefore, discussions with the Director of Security are necessary to capture the expected outcomes of the implementation of a security measure but also to select the path under validation

in the model.

Three conclusions are possible from the analysis of the Laplace trend values. In the first scenario, the analysis may be inconclusive: this is the case when the Laplace trend values are evolving in the $[-2, +2]$ interval. Another example is when external factors may explain the observed trend: an increasing trend at the beginning of the Fall or Spring semester may be explained by the increasing number of users, as students come back on campus. When coming back, students may plug their infected machines to the network and trigger more incidents. If we reach an inconclusive conclusion, the model is unchanged. In the second scenario, we may observe that the conclusions of the analysis (increasing or decreasing trend) match the expected outcomes. In this case, we have more confidence in the path under validation, and the model is unchanged. In the third scenario, the conclusions of the analysis do not match the expected outcomes. In this case, the path under study may be incorrect and the model may need to be modified accordingly. For example, the modification of the model may consist in changing one type of influence (positive or negative). We want to emphasize that in the second and third scenario, the conclusions drawn from the Laplace trends are not always obvious. We may need to investigate additional information, such as the number of users per period (Summer versus Fall semester).

In conclusion, the steps of the validation through case studies are the following:

1. Select a security measure to analyze and the appropriate dataset: All measures listed previously may not have observable effects on the available data, such

as password policies,

2. Identify with the help of the Director of Security at UMD the expected outcomes of the implementation of the measure,
3. Calculate the Laplace trend values for the selected data: We decide to start the analysis one month before the implementation of the measure and to cover a period of several months (typically eight months),
4. Map the measure to a node and a path in the model, which is possible through discussions with the Director of Security at UMD,
5. Draw conclusions: If the Laplace trend values are between -2 and $+2$, the trends are not significant and the analysis is inconclusive. If the outcomes of the analysis match the expected consequences, we have more confidence in the path of the model related to the security measure under study. In both previous cases, we do not modify the model. On the contrary, if the conclusions of the analysis and the expected outcomes do not match, we may need to modify the model accordingly. Conclusions of the analysis should be handled with care as, due to the lack of information, it is possible that the observed consequences are the result of other factors, such as the change in campus population.

In the next subsection, we apply this process to validate parts of the model.

5.3.6 Results

5.3.6.1 Impact of the Hire of an Analyst

Measures and dataset

According to Table 5.2, four hires occurred since 2001:

1. Hire of an IT security officer and of an intern on June 17, 2002,
2. Hire of an analyst in 2003: the intern who was working in IT security since June 2002 was hired as a full-time analyst,
3. Hire of an analyst on January 3, 2005,
4. Hire of an analyst on January 23, 2006.

All officers, when they were hired, were assigned the task of incidents identification and response. Therefore, the hires should have an impact on the rate of incidents.

Expected outcomes

For the first measure, the hired IT security officer was previously working at UMD as a security engineer within the Networking group. His advancement is the result of the will of the organization to build a Security department, as security became a priority for OIT. The security engineer was handling networking duties and security incidents identification. When he became a security officer in 2002, he was relieved from his networking duties and could focus on security tasks. Therefore, the expected outcomes of his hire and the hire of an intern to support his tasks are an immediate increase in the rate of incidents. On the longer term, the rate of

incidents is expected to decrease as their tasks towards prevention would lead to fewer incidents on campus.

The intern who started working for the Security department in 2002 was gradually assigned incidents detection between 2002 and 2003. Therefore, when he was hired as a full-time analyst in 2003, his tasks were unchanged and his new hire is not supposed to have an effect on the rate of incidents. Therefore, this measure is not included in the analysis.

Both analysts hired in 2005 and 2006 (third and fourth measure), are expected to work on incidents mitigation. On the short term, we are expected to observe an increase of the rate of incidents shortly after both measures are implemented. On the longer term, analysts earn more responsibilities and work on prevention, which is expected to result in a decrease in the rate of incidents.

The Director of Security estimates the short term to be two months after the measure is implemented.

Laplace trend values

The Laplace trend values of incidents for measures 1, 3, and 4 are calculated. Their analyses are explained in the following paragraphs.

From Figure 5.3, we observe a slight increase in the rate of incidents over the first two months. However, the increase mostly occurs within the $[-2, +2]$ interval, which indicates that the trend is not significant. On the long term, we observe an increasing rate followed by an overall decreasing rate. The first observation matches the beginning of the Spring semester: students come back to campus with their potentially infected machines and plug them to the network, resulting in an

increasing incidents rate. The decreasing rate that follows matches the expected outcomes. Therefore the analysis for the hire of the IT security officer in 2002 is inconclusive on the short term but matches the expectations on the long term, if we do not account for the increase probably due to the beginning of the Fall semester.

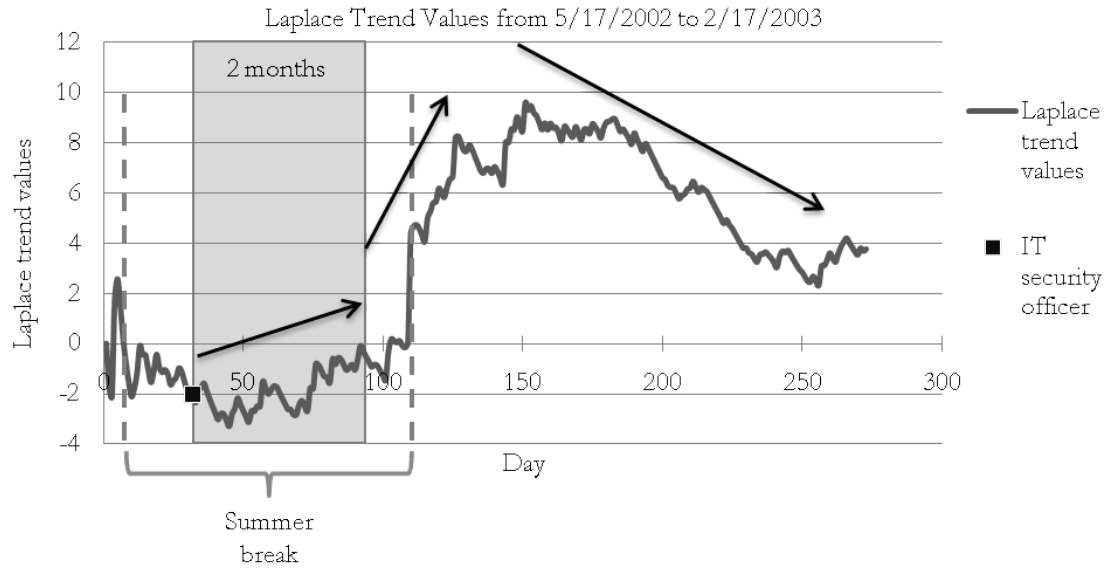


Figure 5.3: Laplace Trend Values for the Hire of the IT Security Officer in 2002

We observe an increasing trend for more than one month and a half after the hire of an analyst in 2005 (Figure 5.4). This increase spans over a period that includes the beginning of the Spring semester. Before the semester begins, the increasing trend is inconclusive as it happens in the interval $[-2, +2]$. The increasing trend continues after the semester has begun. Therefore, the increase in the Laplace trend values after the beginning of the semester may be explained by the hire of the analyst, by the beginning of the Spring semester, or by a combination of the two effects. In order to study the effects of the beginning of the semester, we compare the cumulative number of incidents for years from 2002 to 2007, as shown in Figure

5.5. We compared the beginning of the Fall semesters over these years but it is fair to assume that the conclusions also hold for the beginning of the Spring semesters. A vertical line at day 32 in Figure 5.5 shows the day the Fall semester begins for each year. Figures 5.6 and 5.7 zoom on a time window around the beginning of the Fall semester and show that the effects of the beginning of the semester occur on a short period of time around the date the semester begins. For example, according to Figure 5.6, in 2002, there was a significant increase in the number of incidents on the day the semester begins (Day 32). In 2004, the peak seems to occur the day after the semester begins. Similarly, in 2003 (Figure 5.7), the increase occurs from the day before the classes begin (Day 31) until two days after the semester has begun (Day 33). We believe that the increase in the number of incidents due to students coming back on campus is roughly limited to a time window of few days before and after the semester actually starts. Data show that the increase of the number of incidents during the five-day time window around the beginning of the semester (two days before and two days after classes start) with respect to the preceding five-day time window ranges between 30% and 1,800% for the years under study. When comparing that time window with the following five-day time frame, there is a decrease for all years but 2003, ranging between 25% and 79%. 2003 is an outlier, as we can see from Figure 5.5, and may not be representative of the incidents data. To conclude, this analysis shows that when the semester begins, the rate of incidents increases. This observation, made for the beginning of the Fall semester, also holds for the beginning of the Spring semester. As previously highlighted, the increase occurs on a period of time of few days. Therefore, the increasing trend that

takes place for one month and a half after the analyst is hired in Figure 5.4 may be explained by the beginning of the Spring semester but the effects of the beginning of the semester only act for few days. For the other days, we can reasonably assume that the hire of the analyst contributed to the increasing trend, which matches our expectations on the short term. On the long term, we observe a significant decrease in the rate of incidents, as expected.

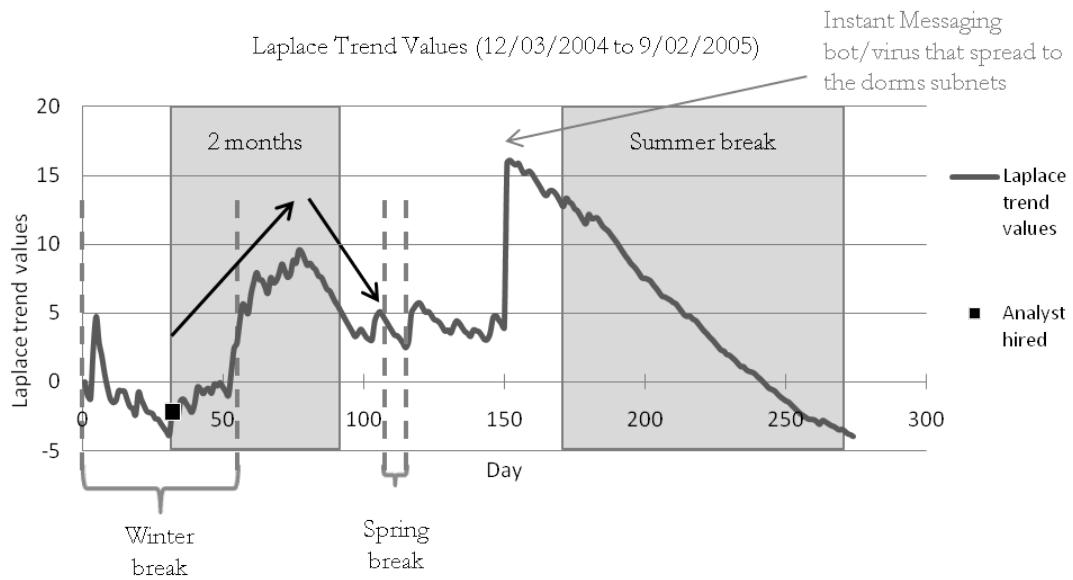


Figure 5.4: Laplace Trend Values for the Hire of an Analyst in 2005

For the last measure (Figure 5.8), we observe an increasing rate of incidents on a period of one month and a half, followed by a decrease. The same discussions on the beginning of the semester and on the $[-2, +2]$ interval apply here. Indeed, the increase that occurs over the first two weeks that follow the hire happens in the $[-2, +2]$ interval. In addition, the hire of the analyst coincides with the beginning of the semester and the increase on the short term may be explained by the change in campus population. However, there is a significant increase until one month and

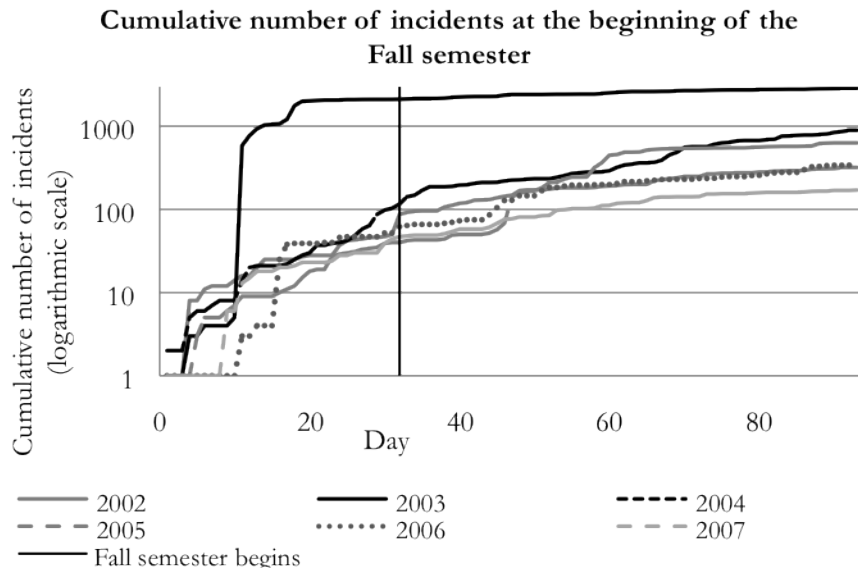


Figure 5.5: Cumulative Number of Incidents for Years from 2002 to 2007

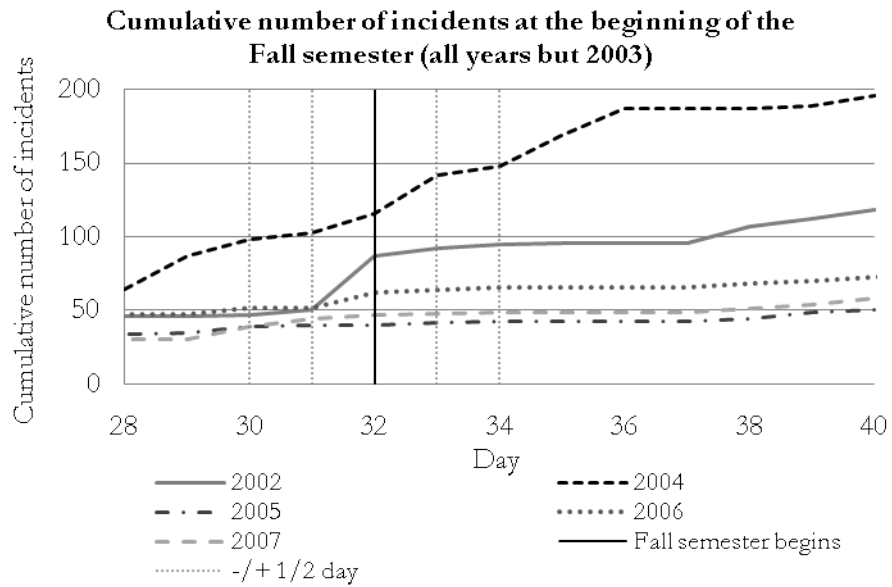


Figure 5.6: Cumulative Number of Incidents for Years 2002, 2004, 2005, 2006, and 2007

a half after the beginning of the semester. It is unlikely that the change in campus population has effects over such a long period, as previously discussed. Therefore,

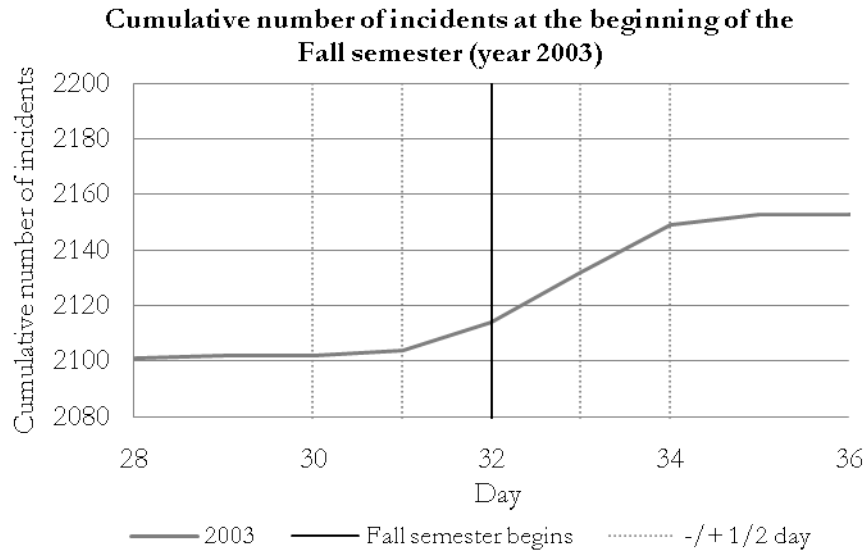


Figure 5.7: Cumulative number of incidents for year 2003

we have confidence that on the short term, the hire of the analyst contributed to the increase in the rate of incidents, which matches our expectations. On the long term, we observe a decreasing rate of incidents until the end of April (around Day 126), as expected. Therefore the results of the analysis of the hire of an analyst in 2006 match the expected outcomes.

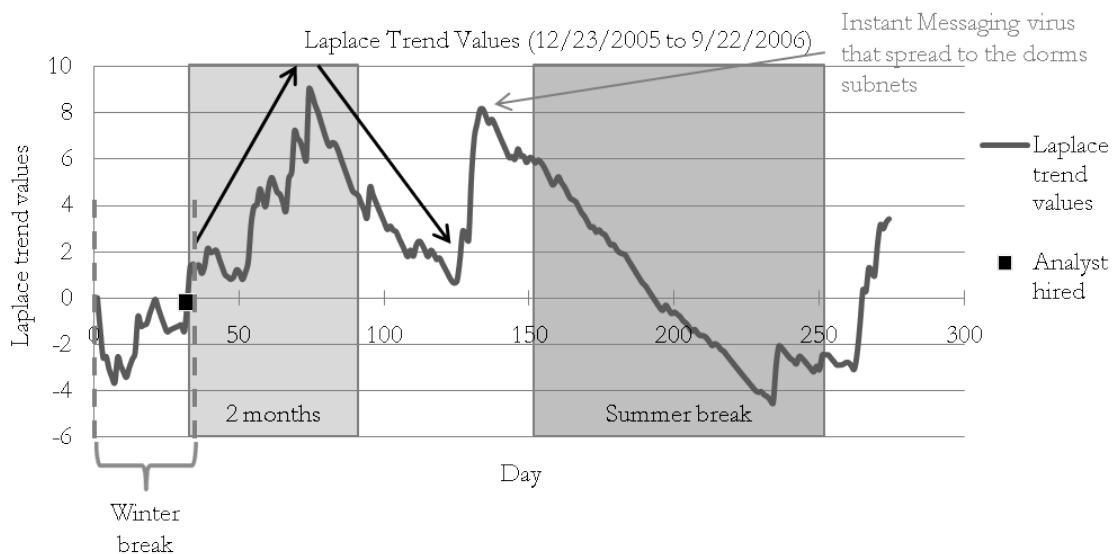


Figure 5.8: Laplace Trend Values for the Hire of an Analyst in 2006

Insights on the model validation

On the one hand, we studied the effects of the measure on the rate of incidents, considered as an indicator of security. On the other hand, we need to relate the measure to a node in the model, and more precisely to a path in the model.

The hire of the security officer in 2002 results from a change of culture within the organization: managers identified a need of differentiating security duties from networking ones. Therefore, a Security Department was launched, resulting in the hire of the security officer and the intern. This measure relates to the node labeled “Organizational Attitude towards Security”. Fourteen paths are possible from this node to node “Security”, which are depicted in Figure 5.9: they are labeled 1, 2, 3.1.1.1, 3.1.1.2.1, 3.1.1.2.2, 3.1.1.2.3, 3.1.2.1, 3.1.2.2, 3.1.2.3, 3.2.1, 3.2.2, 3.2.3, 3.1.3, and 3.3. Because the change in culture (mapped to node “Organizational Attitude towards Security”) resulted in budget allocation for hiring the security officer, the path under validation should go through nodes “Budget” and “Security Team Expertise and Qualities”. Thus, paths 1, 2, 3.2, and 3.3 in Figure 5.9 are not the ones concerned with the implementation of the measure. During the first eight months of his hire, the security officer was working on detection and reaction, which relates to the “Depth of Protection of the Asset” in the model. At this point, his tasks do not focus on “Security Policy” and “Security Awareness Communication”. Therefore, the path under validation in the model is the one labeled 3.1.3 in Figure 5.9 .

The analysis of the Laplace trend values for the hire of the Security officer and hire of an intern to support him was inconclusive on the short term but matched

the expected outcomes on the long term. Therefore, we have more confidence in the influence of the “Organizational Attitude towards Security” on security. More precisely, the analysis increases our confidence in the path through “Budget”, “Security Team Expertise and Qualities”, and “Depth of Protection of the Asset”.

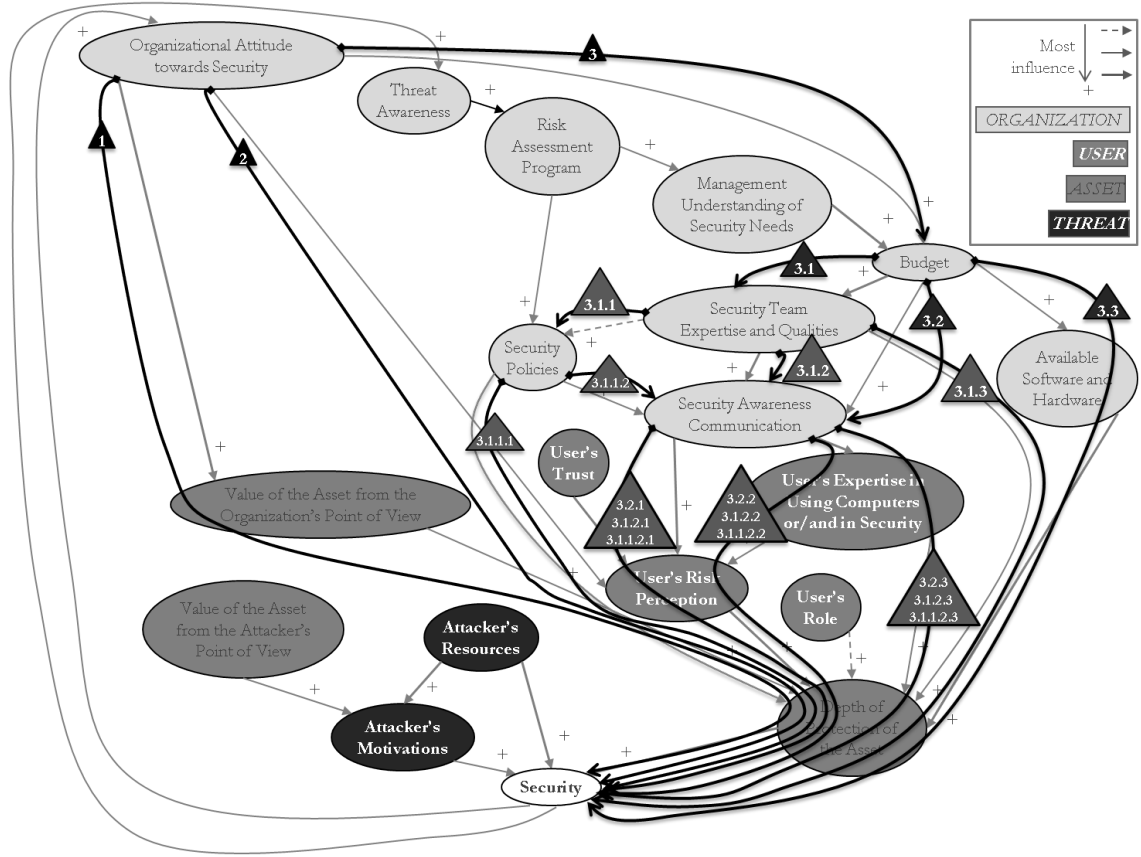


Figure 5.9: Mapping of the Hire of the Security Officer in 2002 to the Model

Both analysts in 2005 and 2006 were hired because there was a need of analysts to support the security officer’s duties. Therefore, both measures are mapped to characteristic “Security Team Expertise and Qualities” in the model. If these measures were the results of available budget allocated to IT security and a decision was made to use it to hire an analyst, then the measures would have been mapped to node “Budget”. It is important to understand the reasons why measures are

implemented in order to best map the measures to the model.

Figure 5.10 shows the eight possible paths from characteristic “Security Team Expertise and Qualities” to characteristic “Security”. Analysts’ primary tasks did not concern policies or communication to users but consisted in incidents detection. Therefore, the path under validation with these measures is path 3, which goes from “Security Team Expertise and Qualities” to “Depth of Protection of the Asset”. The analysis of Laplace trend values for the hire in 2005 is inconclusive on the short and long term whereas it matches the expected outcomes on the short and long term for the hire of an analyst in 2006. Consequently, through this analysis, we are more confident in the path that goes from “Security Team Expertise and Qualities” to “Security” through the “Depth of Protection of the Asset”.

Summary

In this subsection, we analyzed the effects of hiring personnel to deal with security. Three of these hires are expected to impact security through incidents identification: on the short term, officers are expected to work on their mitigation, resulting in an increasing detection rate; on the long term, officers learn how to incorporate tools in their work to prevent successful compromises, resulting in a decreasing detection rate of incidents. In 2003, the hire concerned an intern who was already working in the newly formed Security Department. His advancement as a full-time analyst did not change his day-to-day tasks, thus no effect on the rate of incidents is expected to result from this measure.

Discussion with the Director of Security at UMD allows understanding the motivations behind these hires. This major step enables the mapping of the mea-

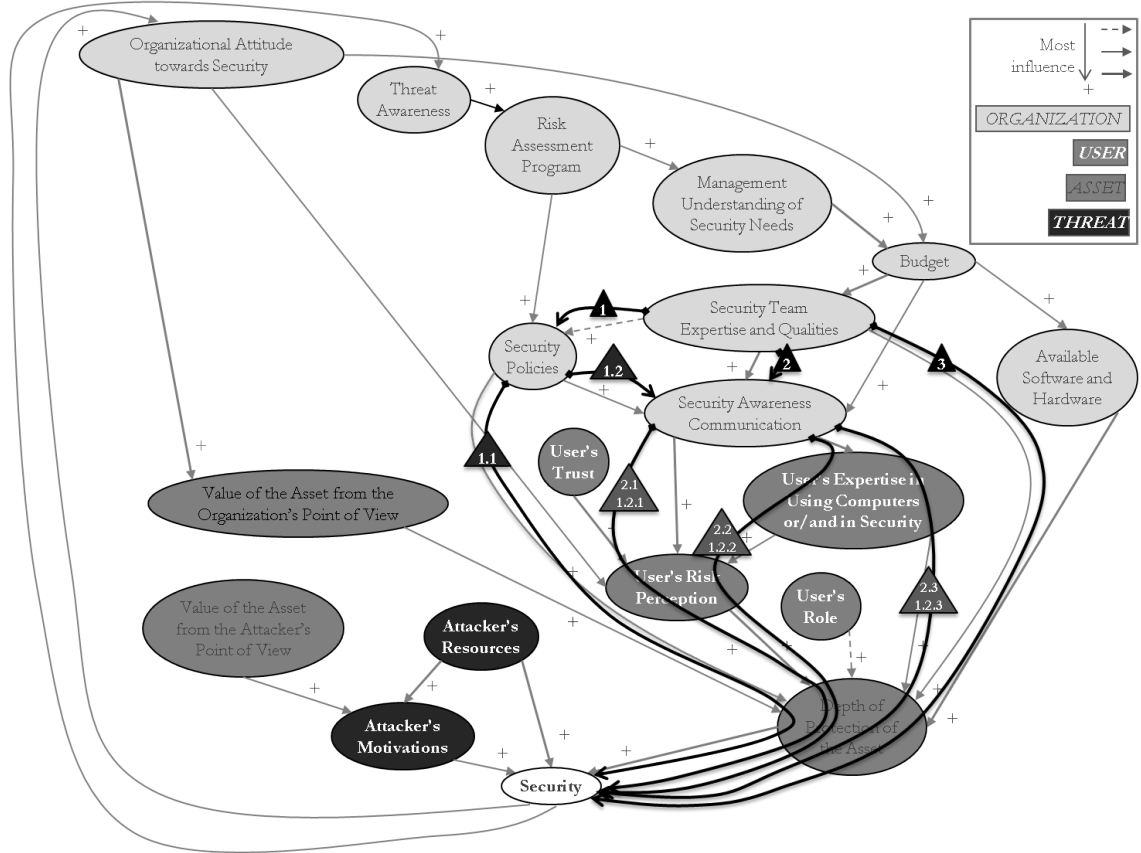


Figure 5.10: Mapping of the Hire of the Security Officer in 2006 to the Model

asures in the model. The hire of the security officer in 2002 relates to the node “Organizational Attitude towards Security” whereas the hires of analysts in 2005 and 2006 map to the “Security Team Expertise and Qualities”. More specifically, we identified the path under validation from these nodes to node “Security”.

The analysis of the first measure on the long term, and the analysis of the hire in 2006 on the short and long term increase our confidence in the identified paths in the model. The analyses of the first measure on the very short term and of the hire in 2005 were inconclusive: we observed the expected outcomes but they were either non-significant (occurring between -2 and $+2$) or they can be explained by the change in campus population.

Discussion

These conclusions need to be handled with care. We are aware that other factors may have had an effect on the rate of incidents, which could also explain the outcomes. For example, the beginning of the semester results in an increase in the number of incidents. By investigating the beginning of the semester, we showed that this effect occurs on few days only. If an increase occurs on more than few days, we can fairly assume that the implemented measure contributed to the increase. Other factors that could have affected the trends are the attack profiles. However we cannot gather data on the attacks that target the organization. Considering the information available, we can however increase our confidence in the identified paths in the model.

5.3.6.2 Blocking of the Routing of Microsoft Protocols from Outside Campus

In 2001, highly critical vulnerabilities related to NetBIOS ports were discovered on Microsoft operating systems [3]. NetBIOS ports are used for Microsoft file sharing and contain security issues that attackers were able to exploit to get remote access to computers [6]. For example, attackers could access sensitive information on computers or create self-propagating malware. Besides, the fact that Windows XP firewalls were disabled by default led to a large number of corrupted machines. In order to prevent external scanners from exploiting vulnerable machines inside the network, the routing of packets sent to Microsoft ports was blocked at the border of the campus on September 2, 2002. Therefore, the implementation of this mea-

sure should reduce the number of infected machines and have a direct effect on the incidents. It is expected that the rate of incidents immediately decreases after the implementation of the measure.

The Laplace trend values from one month before the measure is implemented (August 2, 2002) to eight months after (May 1, 2003) are depicted in Figure 5.11. Overall, we observe a decreasing rate of incidents. Immediately after the implementation of the measure, there is a peak, that is explained by the change in campus population: students come back to campus, bring their potentially corrupted machines, and plug them on the University network. This results in an increasing number of incidents at the beginning of the semester. Although we observe a quick decrease after the peak, and an overall decrease of the rate of incidents, we cannot conclude with confidence that the implemented measure led to the expected outcomes. Therefore, this analysis is inconclusive because of the bias due to the beginning of the semester.

In order to remove the effect of the beginning of the semester and draw better conclusions, the campus population before and after the beginning of the semester could have been investigated. For example, we could normalize the incidents by the campus population, as there are more users after the beginning of the semester. However, this type of data is not available: although we have access to the campus population for each academic year (Table 5.1), we cannot obtain the number of users on campus during Summer. Therefore, it is challenging to analyze the immediate effects of measures that are implemented at the same time as the beginning of the semester.

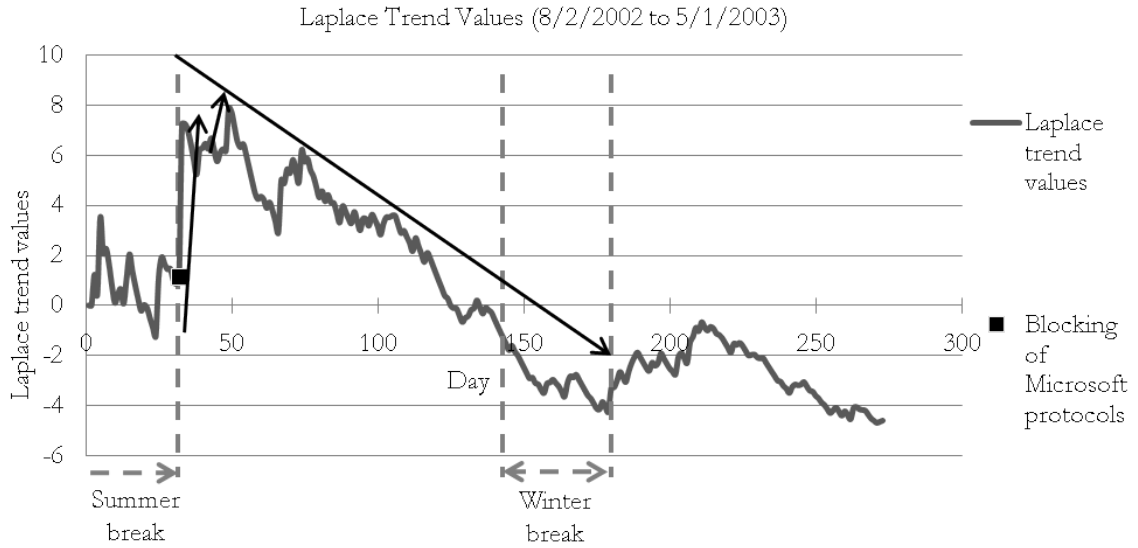


Figure 5.11: Laplace Trend Values for the Routing of Microsoft Protocols from Outside Campus in 2002

5.3.6.3 Installation of IPSs at the Border of the University

Measures and dataset

On September 1, 2006, signature-based IPSs are installed at the border of the campus. These IPSs are active devices that block traffic based on triggered signatures. IT security officers can choose the signatures to enable or disable.

When the IPSs were installed on the network, they immediately collected alerts, that may be viewed by IT security officers. The average number of alerts during the first week of the implementation is 3,545. In other words, the IPSs collected a vast amount of alerts: the security team needed to understand what alerts mean. This corresponds to a learning phase for IT security officers to understand and use IPS alerts in their work of mitigation and prevention. Once they assimilate this, they gain visibility into machines that are already compromised, thus, IPS alerts are used to detect and report incidents. Then, the IPS becomes an integrated

tool for the protection of the network.

Expected outcomes

The implementation is expected to have consequences on the rate of incidents:

- Learning phase: IT security officers try to understand the meaning of alerts.

No effect on incidents is expected immediately after the installation of IPSs,

- IPS alerts used for incidents detection: IT security officers gain visibility into already compromised computers on campus and this results in an increasing rate of incidents on the short term,

- IPSs are integrated to the existing solution for protection of the network and help preventing the corruption of machines in the network. On the long term, the rate of incidents is expected to decrease.

Laplace trend values

Figure 5.12 depicts the Laplace trend values before and after the implementation of the measure. We observe an increasing rate of incidents from Day 42, ten days after the IPSs are installed on the network. This increase continues until Day 52 where an overall decreasing trend follows over the next months. The three phases, also depicted in Figure 5.12, from the implementation of the IPSs to Day 42 (labeled “Learning phase”), from Day 42 to Day 52 (labeled “Detection”), and after Day 52 (labeled “Prevention/Protection”), correspond to the expected time windows: learning phase, IPS alerts used for incidents detection, and IPS alerts used for protection of the network.

Insights on the model validation

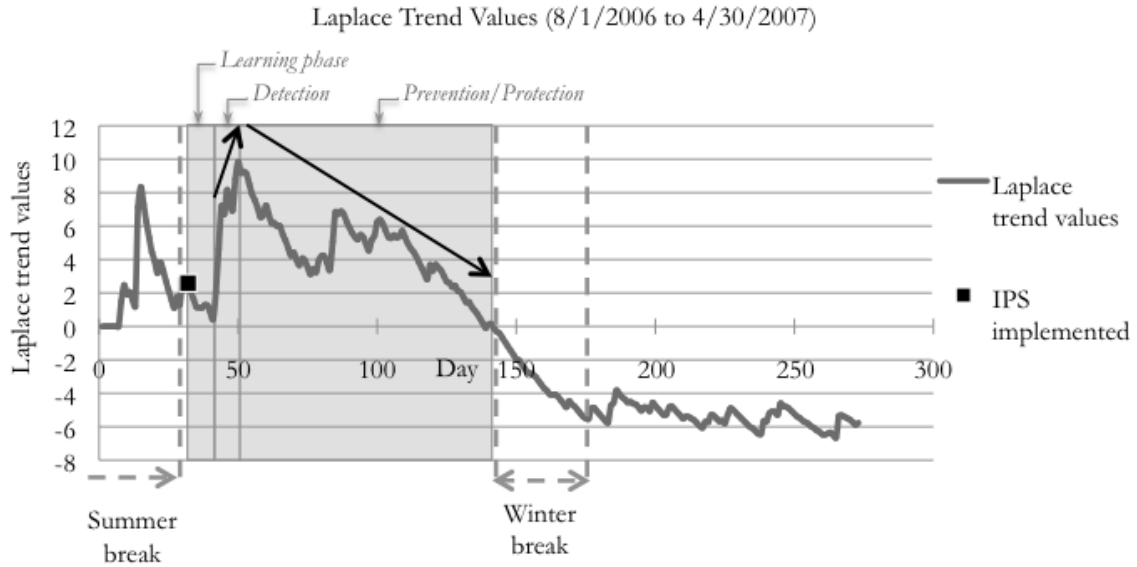


Figure 5.12: Laplace Trend Values for the Installation of IPSs in 2006

The installation of IPS devices involves a better protection of machines inside the network at the network level. Therefore, this measure is directly related to the node “Depth of Protection of the Asset” in the model. As incidents are an indicator of security, the path under validation is the path from “Depth of Protection of the Asset” to “Security”.

The expected outcomes consisted in three different phases, as listed above. The analysis of the incidents rate shows that the expected outcomes are met. Therefore, we have more confidence in the path from “Depth of Protection of the Asset” to “Security”.

Summary

In this subsection, we analyzed the effects of installing IPS devices at the border of the University to block incoming or outgoing potentially malicious activity. The analysis of the Laplace trend values of the number of incidents matches the

expected outcomes: after a learning phase, the IT security team gained visibility into compromised machines, which led to an increasing rate of incidents. On the long term, the IPSs become part of the solution for protection and prevention, resulting in a decreasing rate of incidents.

Discussion

In addition, the Fall semester started on August 30, two days before the IPSs were installed. According to our discussion in the previous subsection, we would expect a significant increase in the rate of incidents few days before or after the beginning of the semester, due to the change in campus population. Although we cannot ensure it, it is possible that the installation of IPSs reduced the effect of students coming back on campus and that it explains why there is no significant increase at the beginning of the Fall semester.

In order to increase our confidence in the effects of the IPSs on security for UMD, we wanted to compare the speed of detection of incidents after the beginning of the semester over several years. To do so, we investigated the percentage of the normalized detected incidents per day over the total number of incidents normalized discovered during the month of September. For a period starting the day before the Fall semester begins and spanning over one month, the percentage per day k is given by the following formula:

$$p(k) = \frac{\frac{\sum_{i=1}^k n_i}{n_U}}{\frac{n_T}{n_U}}$$

$$p(k) = \frac{\sum_{i=1}^k n_i}{n_T} \tag{5.2}$$

Where n_i is the number of incidents for day i , n_T is the total number of incidents for the period under study, n_U is the number of users for the period under study.

The number of users is estimated to be the campus population provided by Table 5.1. To be more accurate, we would need to find an approximation of the campus population the first day of the time window, which corresponds to the day before the semester actually begins. For example, it would be ideal to have the number of users during the Summer semester but we cannot obtain this number, as previously discussed. Besides, we believe that students come back the day before the semester begins to move in the dorms. Thus, we think that using the campus population for the academic year is an appropriate estimation. Table 5.3 provides the beginning and ending dates of each period, and the campus population.

Table 5.3: Data to Support the Comparison of the Speed of Incidents Detection over Four Years - The time window for the analysis starts one day before the semester begins and spans over one month

| Period | Year | Start date | End date | Number of users |
|--------|------|------------|-----------|-----------------|
| 1 | 2004 | 8/29/2004 | 9/28/2004 | 42,377 |
| 2 | 2005 | 8/30/2005 | 9/29/2005 | 42,987 |
| 3 | 2006 | 8/29/2006 | 9/28/2006 | 42,859 |
| 4 | 2007 | 9/28/2007 | 9/27/2007 | 43,936 |

The comparisons between years 2004, 2005, 2006, and 2007 are depicted in Figure 5.13. It is expected that once the IPSs are installed, IPS alerts provide visibility into corrupted machines that are plugged on the network after the beginning of the semester. In other words, in 2006, the detection of corrupted machines should occur earlier in the period than in 2004 and 2005. This trend should be even more

noticeable in 2007, as the IPS is entirely integrated to the overall security solution. Therefore, it is expected that the curves representing 2006 and 2007 are above the ones for 2004 and 2005. From Figure 5.13, the curve representing 2004 is above the other curves for half of the period under study. We would have expected this curve to be lower than the curve for 2006 and 2007, when the IPS is implemented. However, from one year to another, many factors can impact the number of incidents. Few reasons include:

- Awareness of users: from one year to another, users learn about potential attacks and learn how to better protect their assets,
- Attack profile: attacks targeting UMD can be very different from one year to another, which would affect the number of incidents

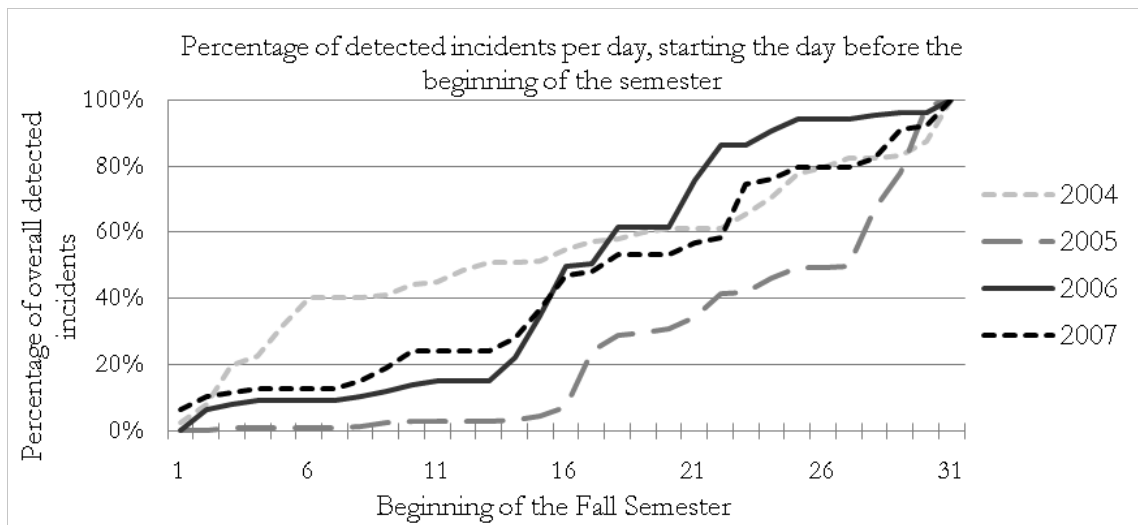


Figure 5.13: Comparison of the Percentage of Detected Incidents for the Month of September

In conclusion, the comparison of the incidents over several years does not allow us to improve our confidence in the conclusions already drawn: the installation of

IPSs at the border of the University led to three phases (learning, detection, and protection/prevention), which matches the expectations.

5.3.6.4 Wireless Networks Put Behind IPSs

Wireless networks are a major concern for UMD because it is difficult to track wireless computers. When users plug in their computers to the wireless network, they are asked to enter their username and password to be given access to the Internet. These computers are allocated dynamic IP addresses that may change every time users log off and log in. From UMD's point of view, each wireless computer is recognized by the username used to connect to the network, an internal wireless IP address, and a routable IP address. The latter is the IP address that can be viewed from outside the network. However, one routable IP address hides several dynamic private IP addresses, which are not visible from the outside world. Figure 5.14 provides a graphical representation of this network address allocation.

When corrupted wireless computers are plugged on the network, they may infect other computers inside the organization. This is especially true at the beginning of the Spring and Fall semester, when students come back to campus and connect their potentially corrupted machines to the network. Therefore, on June 28, 2007, IPSs were put between the wireless network and the rest of the organization. The motivation is to provide IT security officers with visibility into compromised wireless computers that are plugged on the University network (Figure 5.15).

According to this discussion, one would expect to observe an immediate increasing rate of incidents as the measure helps detecting already compromised com-

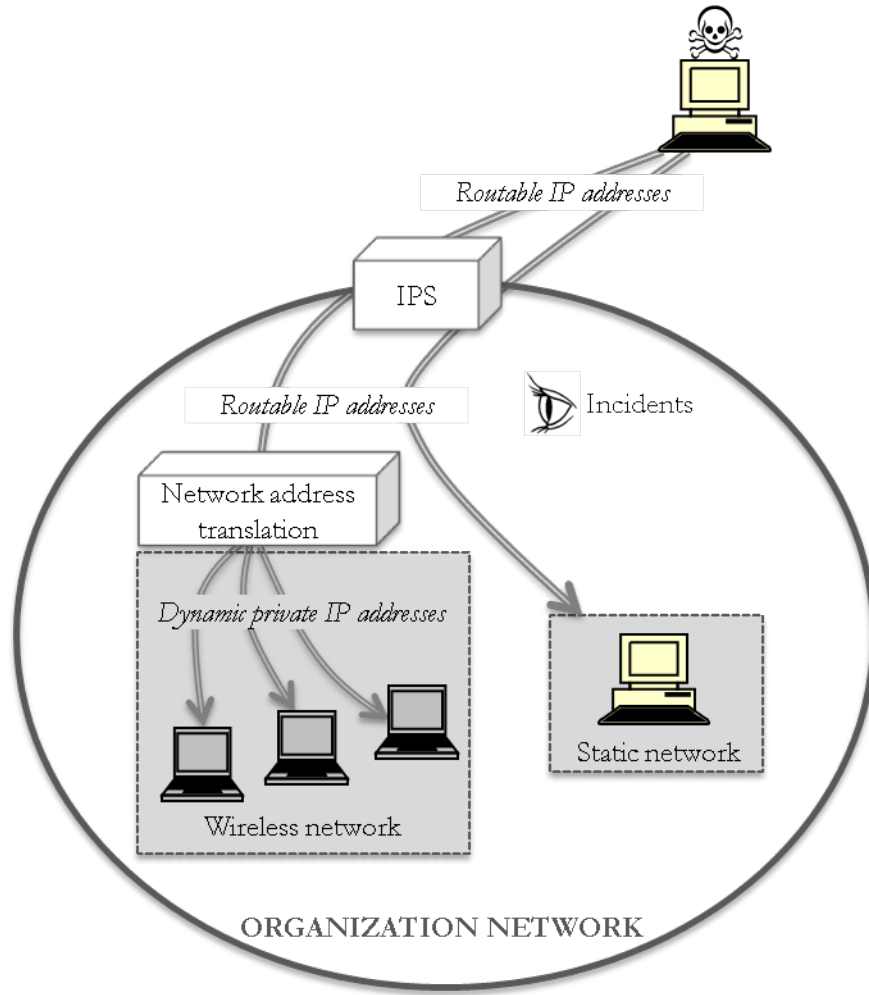


Figure 5.14: Graphical Representation of the Network Address Allocation - A wireless device inside the organization is provided with a dynamic private IP address that can only be seen from inside the organization network. Attackers from outside the network can only see routable IP addresses, behind which several dynamic private IP addresses can be hidden. Incidents focus on routable IP addresses and do not concern dynamic private IP addresses.

puters. On the long term, the measure should help decrease the number of incidents.

However, the incidents dataset available does not contain dynamic IP addresses.

Two reasons explain it:

1. There is no point of blocking a dynamic IP address as the IP address is relocated to another computer when a user needs to connect to the network, and

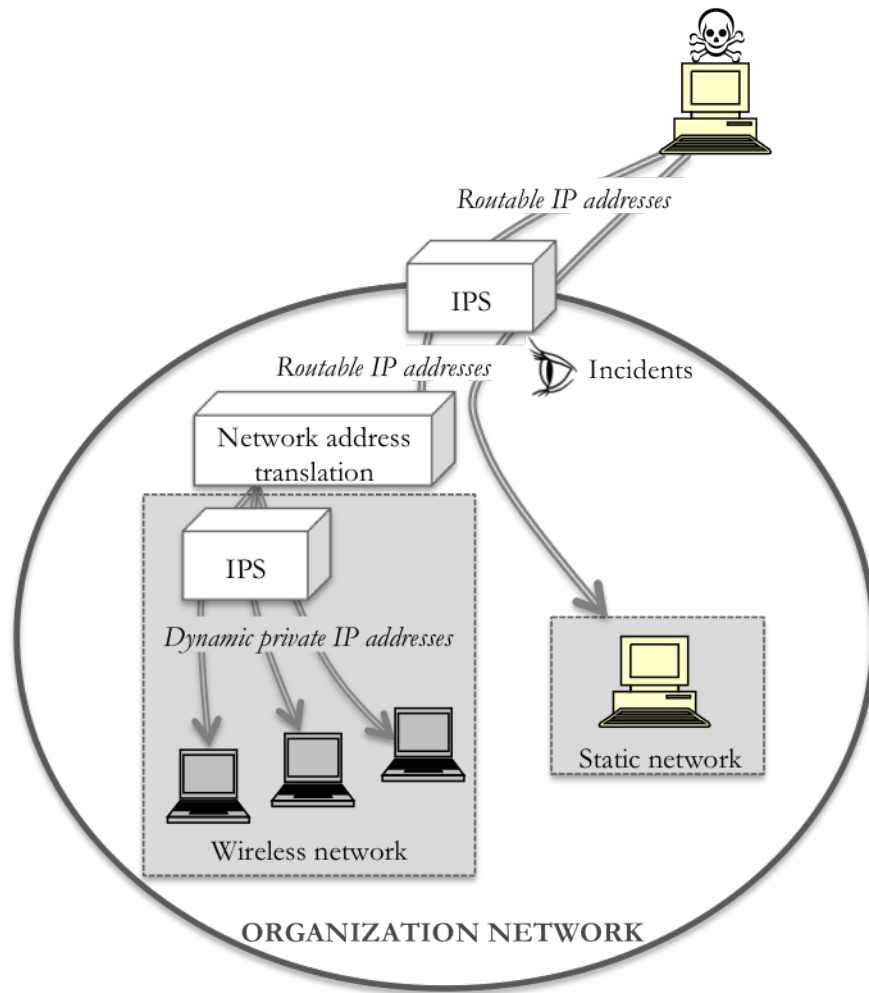


Figure 5.15: Graphical Representation of the Network Address Allocation after the Wireless Networks are put behind IPSs - After the measure, IPSs can trigger alerts related to the internal wireless network.

it does not prevent the corrupted wireless computer to connect to the network from another dynamic IP address,

2. Keeping track of these IP addresses in the dataset are meaningless as they are relocated to other computers later on.

Consequently, we cannot observe direct consequences of the implementation of the measure on the short term, as compromised wireless computers are not recorded in the incidents dataset. However, the indirect effect resulting from the identification

of these corrupted machines and the prevention of having other machines in the network corrupted by them can still be observed in the rate of incidents. This indirect effect is expected to be observed on the long term.

The Laplace trend values from May 28, 2007 to February 27, 2008 are shown in Figure 5.16. We observe a decreasing incident rate after day 137, which matches our expectations. This measure is related to the path from the “Depth of Protection of the Asset” to “Security”.

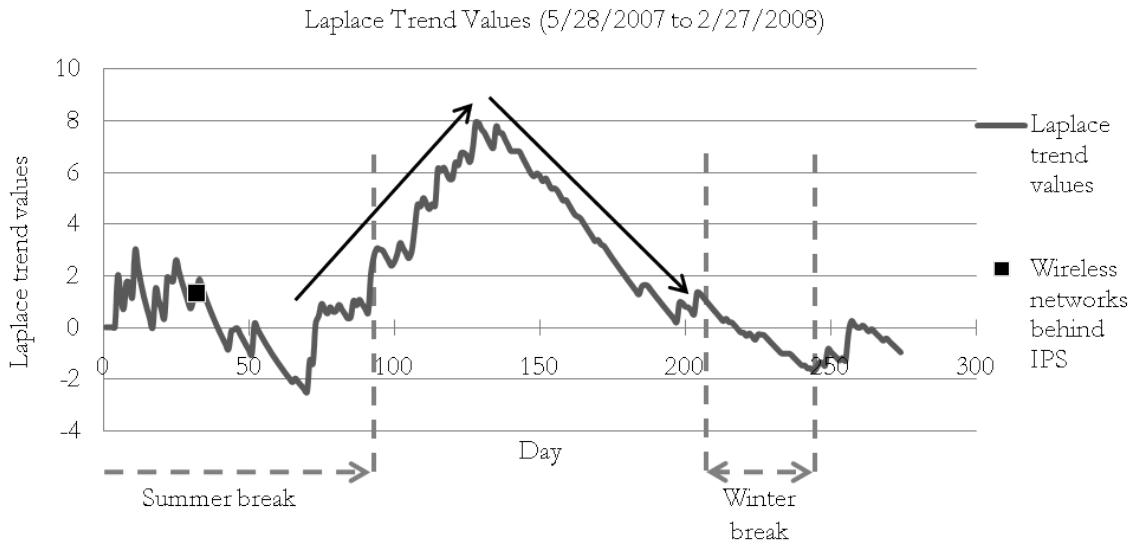


Figure 5.16: Laplace Trend Values for the Installation of Wireless Networks behind IPSs in 2007

Although the results match the expectations, they should be handled with care. Unlike previous case studies, the decreasing rate of incidents is an indirect consequence of the measure. One could look into IPS alerts concerned with dynamic IP addresses, keeping in mind that IPS alerts may contain a high number of false positives. Keeping this in mind, we observe that on the period from June 28, 2008 to February 27, 2009, on average per day, 45% of alerts originating from inside the

University (static and dynamic IP addresses) are from internal wireless machines. This represents on average per day 44% of source IP addresses within the network.

5.3.6.5 Impact of a Communication Campaign

Measures and dataset

In 2008, in order to tackle the issue of phishing attacks at UMD, an anti-phishing awareness campaign was launched. The campaign aimed at making users sensitive to phishing attacks through four measures:

- First mass email sent on April 11,
- Second mass email on May 12,
- Message on login page on June 15,
- Message on webmail page on July 28.

The first and second mass emails were sent to make users sensitive to ongoing fraudulent emails that appeared to be sent by OIT and that required users to provide their University username and password. The new message that was displayed on the login and webmail pages was the following “*OIT will never ask you to put your password into an e-mail message, but scammers will. Do not share your password with others!*”. The decision on the last two measures was made at the same time but it was more challenging to change the webmail page than the login page, resulting in the delay between the two measures.

These measures implemented in the scope of an awareness campaign communication are expected to impact the number of corrupted accounts by phishing.

Expected outcomes

Once a measure of the anti-phishing awareness campaign is implemented, there is a delay between the implementation and the effectiveness. For example, when a mass email is sent, there is a delay before users read the email, and another delay before users indeed take the advice into consideration. The Director of Security at UMD expects a decreasing rate of corrupted accounts within days of the implementation of the measure.

Insights on the model validation

Implementing an anti-phishing awareness campaign implies a high value for characteristic “Security Awareness Communication” in the model, therefore the campaign can be mapped to that node in the model. The number of successful phishing attacks is an indicator of the “User’s Risk Perception”: the higher (respectively lower) the number of successful attacks, the less (respectively more) users perceive risks related to phishing attacks. The objective of this case study consists in studying the impact of the awareness campaign on the number of successful phishing attacks. If after the implementation of the campaign, the number of successful attacks decreases (hence user’s risk perception increases), then there is a positive influence of the awareness communication on “User’s Risk Perception and we have more confidence in the positive influence of the “Security Awareness Communication” on the “User’s Risk Perception”. On the contrary, if data show that the awareness communication does not decrease the number of successful phishing attacks, there is no validation of the positive influence of node “Security Awareness Communication” on node “User’s Risk Perception” in the model.

Laplace trend values

The Laplace trend values for the period from April 10, 2008 to September 12, 2008 are shown in Figure 5.17. During the first nineteen days following the mass email on April 11, the Laplace trend values fluctuate between -2 and $+2$, which makes the analysis on the impact of sending the first mass email inconclusive. Unfortunately, we do not have data for dates before April 10, which prevents us from building a history for the Laplace trend values. After the second measure (second mass email), there is a significant decrease of the rate of incidents that starts three days after the mass email is sent, as expected.

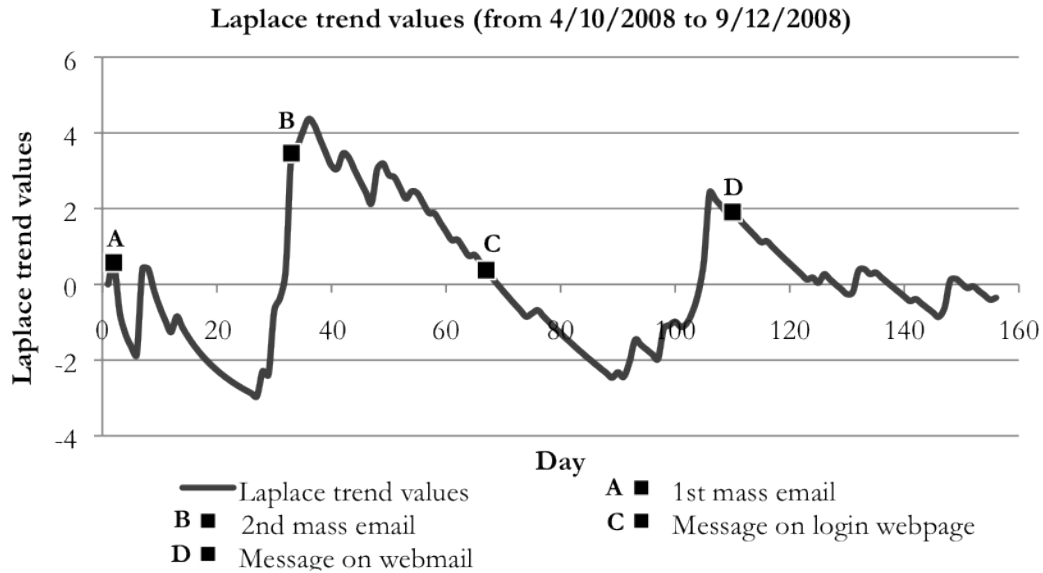


Figure 5.17: Laplace Trend Values for the Number of Successful Phishing Attacks at UMD from April 10, 2008 to September 12, 2008

A decrease follows immediately the implementation of the third measure but the decrease only becomes significant ten days after the measure is implemented. The measure was implemented while the trend was already decreasing. The same observation is made for the fourth measure: we observe a decreasing rate before the

measure is implemented and the trend continues afterwards. For both measures, it is difficult to draw conclusion, and the reason may be due to a bias inherent to the starting date for the Laplace trend values. In order not to keep too much history, Figures 5.18 and 5.19 show the Laplace trend values for each measure starting one month before the implementation of the measure.

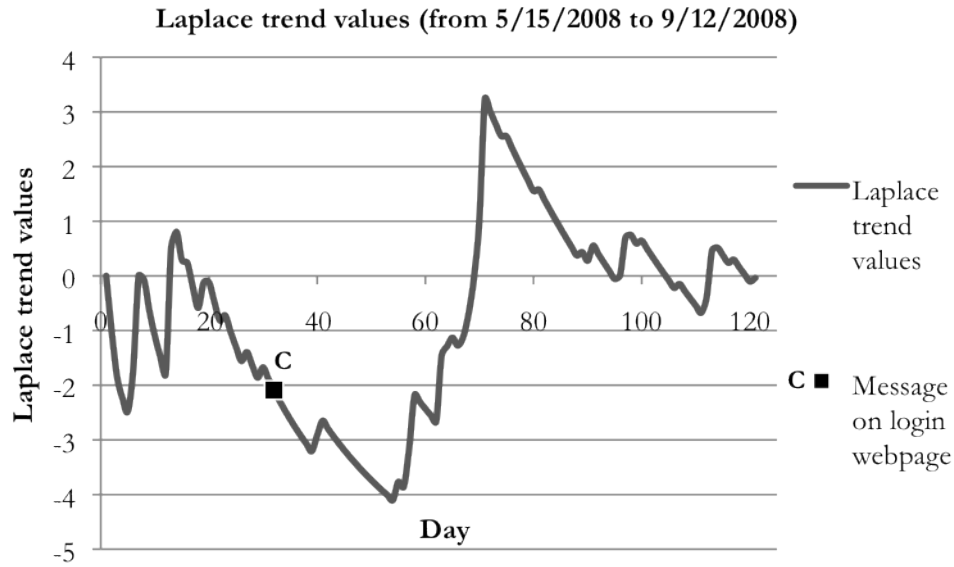


Figure 5.18: Laplace Trend Values for the Number of Successful Phishing Attacks at UMD from May 15, 2008 to September 12, 2008

From Figure 5.18, we observe that the message on the login webpage was released while the rate of successful phishing attacks was decreasing. We observe that a significant decrease follows the measure. Two conclusions are possible: either the measure did not contribute to the decrease and without it, the trend would have kept decreasing, or the measure helped continuing the decrease. A conservative conclusion would be that the outcomes do not contradict the expectations (decrease after the measure is implemented).

The same observations can be made from Figure 5.19. The warning message

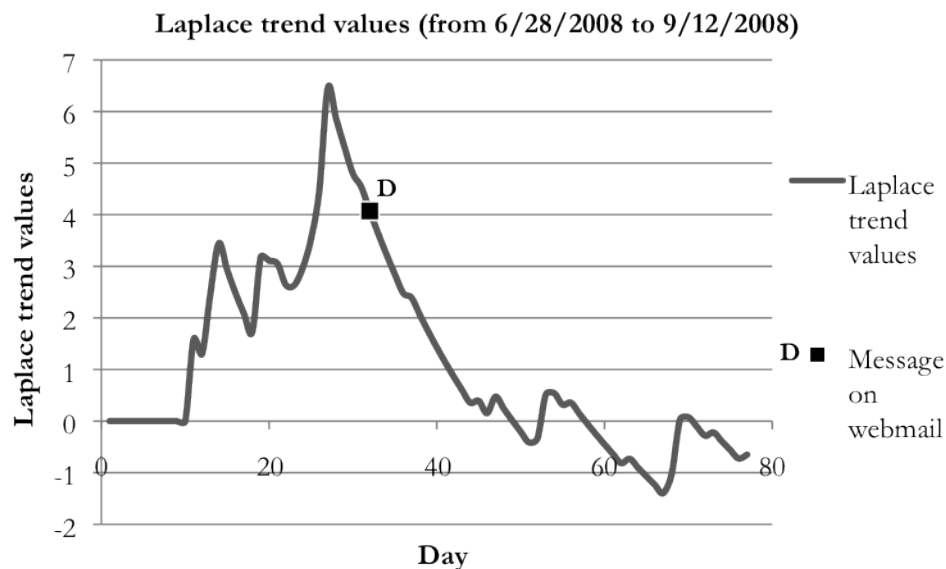


Figure 5.19: Laplace Trend Values for the Number of Successful Phishing Attacks at UMD from June 28, 2008 to September 12, 2008

was displayed on the webmail page while the rate of successful phishing attacks was decreasing. If we look at data after August 2008, we see that the rate keeps decreasing, as fewer and fewer accounts are corrupted. No corrupted accounts are registered for the first half of 2009. Several reasons could explain this trend. First, users may have become aware of phishing attacks, thanks to the four implemented measures. Second, the change in campus population from Spring to Summer may have an effect, although, there is no clear correlation between observed trends and the end or beginning of the semester. Third, there may be fewer phishing attacks. In conclusion, even though we cannot conclude that the measure acted upon decreasing the rate of successful phishing attacks, we can fairly say that the analysis does not contradict the expected outcomes, which were a decrease after the implementation of the measure.

Summary

In conclusion, on the one hand, the analyses of the second, third, and fourth measures match the expected outcomes and increase our confidence in the path from “Security Awareness Communication” to “User’s Risk Perception”. Indeed, the implementation of the second measure is followed by a significant decrease three days after the measure is implemented, which matches our expectations. The interval of three days includes the time for users to notice the new message on the login page and take it into account when they receive an email asking for their credentials. Besides, the third and fourth measures were implemented while there was already a decreasing trend. Although we cannot conclude if the measure participated in the decreasing trend, we can still conclude that the measure did not contradict the expected outcomes.

On the other hand, the first measure is inconclusive: it is difficult to draw conclusions as we do not have more than one day of data before the implementation of the measure.

5.4 Summary

The validation process described in this chapter relies on two initiatives: we first provide experts with the model resulting from the model development (Chapter 4) and then, we use data collected at UMD to validate several nodes and paths in the model.

We managed to have feedback from two experts. We also led several discussions with the Director of Security at UMD. A resulting model is derived and ready for validation through case studies.

In this second step, we used a list of measures implemented at UMD and two datasets: corrupted accounts by phishing attacks, and incidents. We derived a method to study the consequences of implemented measures on security, which relies on the following steps:

1. *Selection a measure and a dataset*: For example, we investigated the effects of hiring analysts, who work on incidents detection. Therefore, this measure should impact the rate of incidents,
2. *Elicitation of the expected outcomes*: We identify, with the help of the Director of Security, the expectations after the implementation of the measure in terms of increasing or decreasing trend of incidents for example, on the short and long term,
3. *Calculation of the Laplace trend values*: The Laplace trend test is used to investigate increasing or decreasing trends in the data,
4. *Drawn insights on the model validation*: Discussions with the Director of Security at UMD enables us to understand how the measure can be mapped to a node in the model, and more precisely to a path in the model,
5. *Conclusions*: The analysis of the Laplace trends are compared to the expected outcomes. If they match, we have more confidence in the path under validation. If they do not match, the model may need to be changed accordingly.

We analyzed the implementation of several measures since 2001. A summary of the measures, their expected outcomes, the results of the analysis of the Laplace

trend values, and the validated paths in the model are shown in Table 5.4.

In our analysis, we faced several limitations, due to the nature of the available data and to the lack of data:

- We cannot validate the entire model: Measures and data available to us limit the analysis to some nodes and paths in the model,
- We cannot validate the strengths of relationships,
- The lack of data does not enable us to conclude with full confidence that the measure actually matches the outcomes: Other factors, that we cannot quantify or identify, may come into account. These factors include the change in campus population, or in the attack profiles.

Despite encountered limitations, we provided a carefully thought method to analyze available data to validate parts of the model. The analysis allows gaining insights into model validation. Several attempts were made to remove the uncertainty on the campus population or attack profiles and were discussed in this chapter. The method described here can further be used to validate other nodes and paths in the model when other security measures are implemented, or when other types of datasets are available.

Table 5.4: Summary of the Validation with Case Studies

| Security measure | Expected outcomes | Conclusion (inconclusive or validated path) |
|---|---------------------|---|
| Hire of security officer and intern (2002) | Short-term increase | Inconclusive |
| | Long-term decrease | “Organizational Attitude towards Security”; “Budget”; “Security Team Expertise and Qualities”; “Depth of Protection of the Asset”; “Security” |
| Hire of analyst (2005) | Short-term increase | Inconclusive |
| | Long-term decrease | “Security Team Expertise and Qualities”; “Depth of Protection of the Asset”; “Security” |
| Hire of analyst (2006) | Short-term increase | “Security Team Expertise and Qualities”; “Depth of Protection of the Asset”; “Security” |
| | Long-term decrease | “Security Team Expertise and Qualities”; “Depth of Protection of the Asset”; “Security” |
| Blocking of routing of Microsoft protocols | Immediate decrease | Inconclusive |
| Installation of IPSs | Short-term increase | “Depth of Protection of the Asset”; “Security” |
| | Long-term decrease | “Depth of Protection of the Asset”; “Security” |
| Wireless networks put behind IPSs | Long-term decrease | “Depth of Protection of the Asset”; “Security” |
| Communication awareness campaign (1st mass email) | Decrease | Inconclusive |
| Communication awareness campaign (2nd mass email) | Decrease | “Security Awareness Communication”; “User’s Risk Perception” |
| Communication awareness campaign (message on login webpage) | Decrease | “Security Awareness Communication”; “User’s Risk Perception” |
| Communication awareness campaign (message on webmail) | Decrease | “Security Awareness Communication”; “User’s Risk Perception” |

Chapter 6

Model Description

6.1 Introduction

Chapter 6 presents the model resulting from 1) the literature, 2) interviews with experts, 3) surveys, 4) validation with experts, and 5) validation with case studies at UMD. In the first section of this chapter, we define the model components: user, threat, organization, and asset. In the second section, we focus on characteristics for each component and present the model resulting from our study.

In the last section, we illustrate the use of the model through two examples. We first show that the model can be used by IT security officers to start the discussion with managers on security solutions. We compare three solutions for which the objective is to increase the level of security of the organization: sending frequent emails to make users sensitive to security issues, implement new policies, and investing in security devices to protect assets in the organization. In the second example, we show how the model can be used to reason about security. We take the example of an organization where data show that users are not aware of social engineering techniques. The model is a support for communication and is a common language between IT security officers and managers.

6.2 Model

6.2.1 Model Components

Our objective was to identify major components of security, with a focus on the human element. The final decomposition is the following:

- **User:** Anyone who uses a computer,
- **Threat:** Anything that has the potential to do harm. It includes the attackers,
- **Organization:** “A social arrangement, which pursues collective goals, which controls its own performance, and which has a boundary separating it from its environment” [103]. It includes the IT security team and managers,
- **Asset:** Anything that is owned by a person or by the organization that can be converted into money. It includes 1) physical entities such as computers, and 2) data that can be sensitive, such as passwords, credit card numbers, organizational secrets, or intellectual property.

6.2.2 Model Characteristics

The validated model, based on interviews and surveys, is shown in Figure 6.1. “Security” is impacted by two groups of nodes: a group that includes attacker related characteristics (“Attacker’s Motivations”, “Attacker’s Resources”, and “Value of the Asset from the Attacker’s Point of View”) and a defense group (all characteristics going through the “Depth of Protection of the Asset”). Both users and the organization have a role in the defense process. Besides, the model depicts how the organization can increase security by educating users.

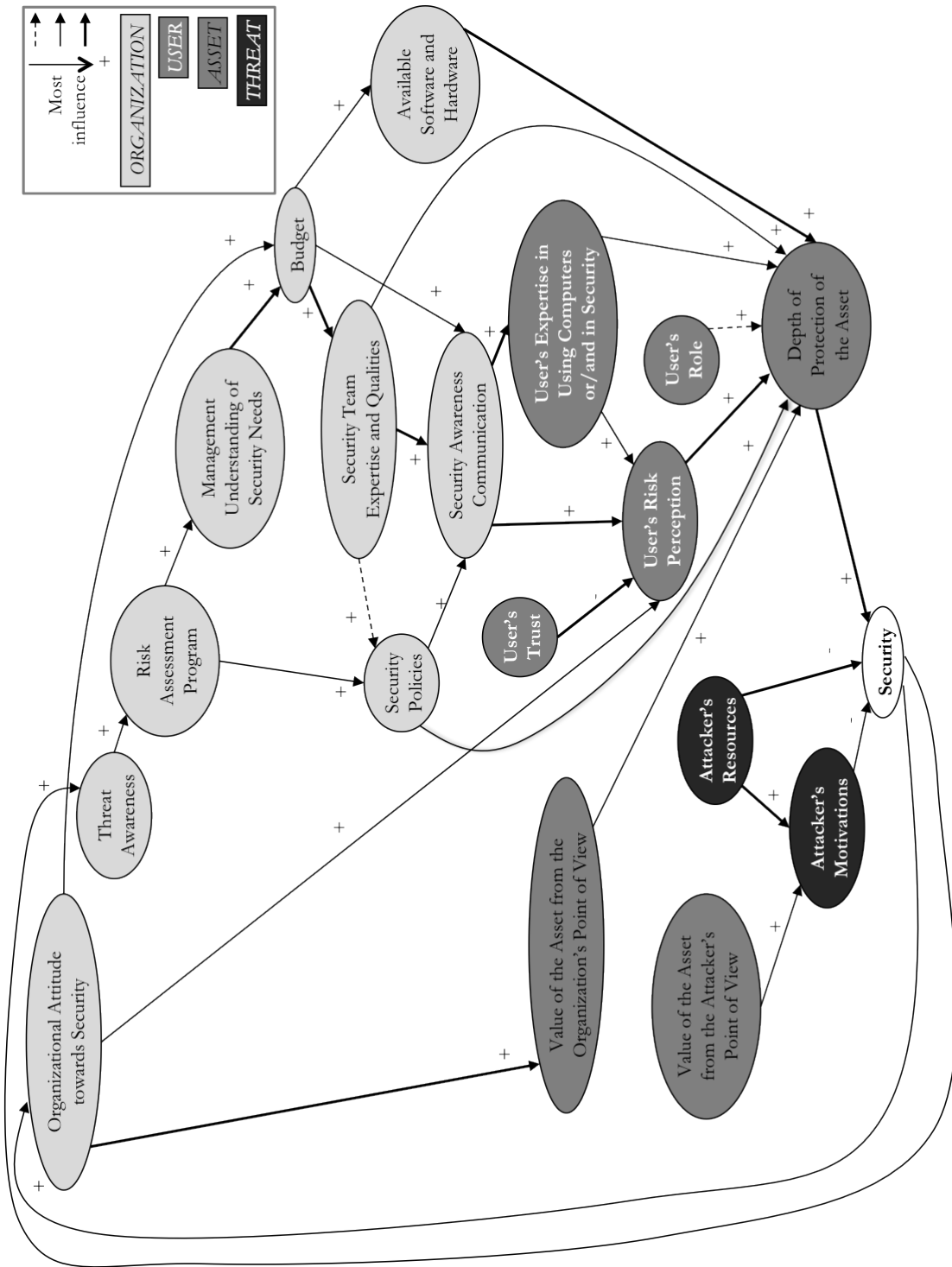


Figure 6.1: Final Model

The identification of characteristics is based on the literature and inputs of experts. In Chapter 2, the literature was investigated to identify some characteristics to consider. These findings are summarized in Table 6.1.

Table 6.1: Characteristics found in the Literature

| Characteristic | References |
|--|-------------------------------|
| User's Risk Perception | [73], [76], [82], [106] |
| User's Trust | [105], [111] |
| User's Expertise in Using Computers or/and in Security | [82], [105] |
| Attacker's Motivations | [15], [92], [96], [126] |
| Attacker's Resources | [92], [96], [126] |
| Organizational Attitude towards Security | [38], [60], [72], [81], [101] |
| Risk Assessment Program | [81] |
| Management Understanding of Security Needs | [72], [119] |
| Budget | [72], [81] |
| Security Team Expertise and Qualities | [94] |
| Security Policies | [81] |
| Security Awareness Communication | [26], [54], [99], [119] |
| Available Software and Hardware | [94] |
| Value of the Asset | [114] |

Each characteristic for the user, threat, organization, and asset is defined in Tables 6.2, 6.3, 6.4, and 6.5. "Security" is not part of any of the four components previously identified. Defining security is challenging: there is no accepted definition of what good security or bad security means. One can view security as a risk informed process: as the objective is to increase the level of security, organizations ultimately aim at decreasing the frequency or the gravity of successful attacks.

Table 6.2: Characteristics of the User Component and their Description

| Characteristic | Description | Comments |
|--|---|---|
| User's Risk Perception | Subjective judgment one makes on the risks related to security | A high number of accounts corrupted by phishing attacks may reveal that users do not perceive the risks related to such attacks |
| User's Trust | Belief one has that one's asset is not at risk | People may trust the IT security team to fully protect their assets |
| User's Expertise in Using Computers or/and in Security | Knowledge, training, and experience in using computers or/and security one has or gains | Means to gain more knowledge or experience include reading the news, using computers, or taking classes |
| User's Role | Function one has (for an academic environment, if the user is an undergraduate, graduate student, a faculty, or a staff member) | Represents how much one cares about protecting one's assets - An intern may care less than a faculty member |

Table 6.3: Characteristics of the Threat Component and their Description

| Characteristic | Description | Comments |
|------------------------|---|--|
| Attacker's Motivations | Reasons why people attack assets | Can consist of a specific purpose (steal information), or no purpose (leisure) |
| Attacker's Resources | All resources (personal and material) available to the attacker | Include expertise (computer or attack skills gained by academic learning, experience, or reading news/blogs), qualities (such as perseverance), and material (software and hardware) |

Table 6.4: Characteristics of the Organization Component and their Description

| Characteristic | Description | Comments |
|--|---|--|
| Organizational Attitude towards Security | How an organization feels about security | An organization involved with critical non-IT risks (e.g. military, banking, nuclear power) has a culture of risk intolerance. The relative lack of gravity in the risks faced by some other organizations (such as universities) results in a culture of risk acceptance. |
| Threat Awareness | Represents the knowledge of threats by the IT security team and the understanding of how relevant these threats are to the organization | |
| Risk Assessment Program | Program to evaluate IT security risks | |
| Management Understanding of Security Needs | Level to which the organization understands the needs for security | May translate into the budget allocated to IT security or the political cover provided (for instance in the case of unpopular password policies) |
| Budget | Financial resources available for IT security | Includes resources to buy devices and hire IT security officers |
| Security Team Expertise and Qualities | Theoretical knowledge of security, of how to protect a network, experience gained, and personal qualities useful to deal with security issues | Qualities include the capacity to withstand stress, perseverance, and efficiency |
| Security Policies | IT security requirements (high-level expectations) | |
| Security Awareness Communication | How the organization communicates security issues to its users | Awareness campaigns include sending emails to users or posting fliers |
| Available Software and Hardware | Includes resources available for IT security | Includes patches (software), Intrusion Detection Systems (hardware) |

Table 6.5: Characteristics of the Asset Component and their Description

| Characteristic | Description | Comments |
|--|---|--|
| Value of the Asset from the Attacker's Point of View | Gain for the attacker if the attack is successful | Includes storage space and confidential data |
| Value of the Asset from the Organization's Point of View | Represents the importance of an asset to the organization | Servers and institutional data are likely to be highly valued |
| Depth of Protection of the Asset | Layers of protection deployed to protect the asset from attacks | Includes all protections of an asset, at the network, system, application, and data levels (intrusion detection systems, firewalls, passwords) |

6.3 Qualitative Use of the Model

The model aims at helping reasoning about IT security and easing communication between IT security officers and managers. It is a resource for security officers to convince decision makers on how to invest in security. In the following subsections, we illustrate how IT security officers can discuss with managers where to invest in security, and how to identify causes of a low security level.

6.3.1 How to Use the Model to Decide Security Strategies?

Let us consider three security strategies and show how security officers can discuss with managers the impacts of implementing each measure, and which measure they should invest in. We investigate the following security solutions:

- Solution 1: Send frequent emails to make users sensitive to issues related to security such as phishing. This means a high value of node “Security Awareness Communication”,
- Solution 2: Implement new policies. This means a high value of node “Security Policies”,
- Solution 3: Buy security devices to protect the network (such as intrusion detection or prevention systems). This means a high value of node “Available Software and Hardware”.

Increasing the organization’s communication (Solution 1) allows the user to have a better exposure to security. Therefore, his/her risk perception has a higher probability to be high: in other words, the user is more aware of security issues.

In addition, the user gains expertise in security through awareness communication. As the user is more aware of risks and more knowledgeable, he/she is more inclined to better protect his/her assets (“Depth of Protection of the Asset” in the model). For example, he/she can protect his/her system by updating the anti-virus, or by choosing a strong password to protect his/her assets. Implementing new policies (Solution 2) has a direct consequence on the “Depth of Protection of the Asset”. The increase of the availability of resources (Solution 3) positively impacts the “Depth of Protection of the Asset”.

Therefore, all solutions positively impact the “Depth of Protection of the Asset” but the strength of the impacts differ. Solution 1 has a strong influence on the “Depth of Protection of the Asset”, through the “User’s Risk Perception” and “User’s Expertise in Using Computers or/and in Security”, Solution 2 has a medium influence on the “Depth of Protection of the Asset” and Solution 3 has a strong influence on it.

Consequently, Solution 1 has the most impact on the target node “Security” as it positively influences the “Depth of Protection of the Asset” through two paths, one being a strong influence, the other one being a medium influence. Solution 2 impacts the “Depth of Protection of the Asset” with a unique medium positive influence, whereas Solution 3 impacts it with a unique strong influence.

The outcomes of this analysis may be discussed as in IT security, budget plays a major role. Comparing the three aforementioned methods, managers may decline implementing Solution 3, given the monetary cost it would imply. The model provides a basis on which to open the discussion between IT security officers

and managers. With this tool, IT security officers can help managers reason about the impacts of implementing a security measure. For example, sending frequent emails may have a double effect on security: the action increases users' knowledge on security issues ("User's Expertise in Using Computers or/and in Security") but also increases their perception of security-related risks ("User's Risk Perception"). Therefore, the model allows people (managers and security officers) brainstorming about security in order to implement the most efficient security strategy.

6.3.2 How to Identify Causes of Security Issues?

Let us consider the following scenario: data show that users do not perceive the risks related to social engineering. This translates in the model as a low "User's Risk Perception". In order to deal with this issue, the model allows identifying the causes of the problem: the user's trust, expertise, or exposure to security (through security awareness communication). Therefore, the organization can directly decide how to increase the value of one or all three nodes.

Moreover, additional evidence can support decision making in this case. Let us assume that in the previous months, 1) the organization has especially focused on communicating with the users by sending emails about security issues and 2) media have developed reports on stories in which users have been stolen credentials on the Internet. Therefore, the value of the node "Security Awareness Communication" is high. This evidence reveals that the causes that explain a decrease of the user's risk perception are related to one of the two following causes: the user's trust or the user's expertise.

Thus, the organization may decide to develop workshops to educate users. Such an initiative would increase the user's theoretical knowledge, hence the "User's Expertise in Using Computers or/and in Security".

6.4 Discussion

The model development and validation may be questioned. First, its development relied on the identification of characteristics in the literature (Chapter 2), but mostly on expert opinion. Therefore, the development process may be criticized for the subjectivity involved at several steps of the process. However, the structure of the model is flexible so that characteristics or influences in the model may be modified, added, or removed. In addition, the description of the carefully thought methodology that involves experts and combines several expert opinions and several sources of information (interviews and surveys) and the outcomes of the interviews and of the surveys are made available in this dissertation for reuse. Second, the validation of the model relied on expert opinions but also on data collected at UMD. The analysis of available data before and after the implementation of a security measure at UMD allows validating paths in the model. However, it was not possible to validate all paths in the model because of the lack of sound, available data relevant to all paths. Also, case studies allowed the validation of the type of influence from one node to the node "Security", but did not allow the validation of one node on another along the path, nor the validation of the strength of influences.

6.5 Summary

In this chapter, we defined model components, listed descriptions of characteristics of each component, and presented the final model. We then showed how the model can be used in a qualitative manner for security officers to have a justified discussion with managers on how to invest in security. The model shows how the implementation of a measure translated in the model affects other parameters of security. It aims at facilitating communication between security officers and managers by providing a visual support to reason about security.

Chapter 7

Towards a Quantitative Model

7.1 Introduction

At this point of the dissertation, we have presented a model for decision making in IT security. The objectives of the model are to represent causal relationships among characteristics of the user, threat, organization, and asset and improve communication between IT security officers and decision makers. In Chapter 6, we showed how the model can be qualitatively used to reason about security. For example, we showed how the model can help discussing and comparing several security decisions such as the implementation of new security policies, the installation of security devices, and the implementation of an awareness communication campaign.

In Chapter 7, we start the discussion on how to further push the capabilities of the model. We want to give insights into the following question: *How can an IT security team use the presented model in their organization to start the discussion on security decisions with their managers?* Ultimately, we want to give practical directions on how organizations can measure characteristics identified in the model. Measurements are either qualitative or quantitative. Chapter 7 tries to answer questions such as: How can I know the level of expertise of my security team? How can I evaluate the depth of protection of the assets in my organization? How can I measure the user's risk perception? The objective is not to provide measurements for all characteristics in the model but to provide directions on qualitative and quantitative measurements of a set of characteristics.

We first detail the approach for measuring characteristics in the model. This task is difficult for the reasons that were raised in this dissertation: there may not be obvious measurements for characteristics in the model, and data in security are difficult to obtain. In this chapter, we provide a series of techniques and examples to illustrate how quantification, although imperfect, is possible. The objective is to provide recommendations on measurements of characteristics in the model that are practical and achievable. For example, in the second section of this chapter, we focus on attacker-related nodes. Challenges exist while trying to understand attackers targeting an organization. Often, it is not possible to have a complete picture of the attackers targeting a specific organization. We suggest using nodes related to the attacker as parameters of the model. In the next section, we compare the use of the model over all assets of the organization and the use of the model for categories of assets. Next, we provide directions of measurements (qualitative and quantitative) for selected characteristics in the model: IT security team's expertise and qualities, security awareness communication, and user's risk perception. At the end of this chapter, we present a five-step methodology to use the model and an example. We then introduce the concept of facets: the model can be used by focusing on selected attributes of the attacker or specific categories of assets in the organization. We illustrate the use of the model through two selected facets: servers and phishing attacks.

7.2 Approach

The major objective of the model is to provide IT security officers with a support when discussing with decision makers what security solution to implement. For example, when deciding between hiring additional staff or buying a new security device, IT security officers face the issue of convincing their managers of the benefits of these solutions. With the presented model, IT security officers can explain that hiring additional staff impacts several aspects of security: for instance, a newly hired analyst can help the current team to develop stronger security policies, work on developing security awareness communication to improve the user's risk perception, or participate in identifying security issues in the organization. These justifications are possible with the model as node "Security Team Expertise and Qualities" positively impacts "Policy", "Security Awareness Communication" and "Depth of Protection of the Asset".

When applied to an organization, the model needs to be organization-specific. Indeed, organizations are different from the perspective of their policies, IT security team attributes such as the IT security team size, or attacks targeting them. Therefore, the question is *"How can organizations translate the specifics of their attributes into the model?"*

First, in order to use the model, organizations need recommendations on how to measure characteristics in the model. However, characteristics may not be easily quantifiable: for example, how can we measure the "Organizational Attitude towards Security"? Measurements have several attributes. First, they can be either

qualitative or quantitative. Second, these measurements may not directly assess the nodes: a set of indicators may provide evidence on the measurement of nodes (see Section 3.4.4.4 for more details). In addition, one should identify data or evidence that can be gathered in the organization and used to measure characteristics. Besides, once measurements are available, the objective is to determine how they translate into the model as high, medium, or low values. For example, if the number of incidents is available and is considered an indicator of node “Security” in the model, does a number of 4 incidents for a given day mean a low, medium, or high value for “Security”? Often, an absolute number does not have much meaning in the model. Instead, relative values may be preferred: an increasing number of incidents over a period of time has more meaning than an absolute number of incidents for a given day. In addition, measures are organization-specific: a number of 4 incidents for a given day may be usual for some organizations whereas it may be low for others. Therefore, the translation of the measures (4 incidents for a given day or an increasing number of incidents over a period of time) into a high, medium, or low value in the model requires the expertise of an analyst. The analyst decides, with respect to the organization, if the value is high, medium, or low. In this task, the concern appears when a set of indicators is provided to measure a node and there is a need to aggregate these measures into one unique value (high, medium, or low) of the corresponding node in the model. This is even more challenging when indicators provide contradictory conclusions.

In summary, providing recommendations on measurements of characteristics is a tedious task, and achieving a recommendation of all characteristics in the model

requires considerable research. In this chapter, we provide a set of practical and achievable techniques for the measurement of selected characteristics and illustrate the approach with examples. This proof-of-concept shows that measurement, although imperfect, is possible.

The following sections consider several characteristics or groups of characteristics in the model. Each section lists examples of measurements inspired from existing techniques. Then, we suggest approaches to measure some characteristics through one or a set of measurements (direct or indicators) and explain how the measurement or set of measurements can be translated into a high, medium, or low value in the model. Finally, we illustrate the measurement approach through examples.

7.3 Attacker-Related Nodes as Parameters of the Model

In the model, characteristics related to the attacker are his/her motivations and his/her resources. Resources include knowledge and expertise, the available software, hardware, and financial resources.

Organizations have visibility into some attacks targeting their network as they result in a large amount of traffic in the case of scanning activities, or in corrupted machines. However, organizations cannot have a complete picture of all targeting attacks. For example, they do not have information on all attacks that are attempted but not successful. In addition, organizations do not have information on motivations behind attacker's actions or know exactly the resources available to attackers. In this context, how can nodes related to the attackers be assessed? The solution is

to consider these characteristics as parameters of the model. In other words, nodes “Attacker’s Resources” and “Attacker’s Motivations” can be used to model profiles of attackers. Looking more closely at attacker profiles allows the organization to implement measures targeting specific attackers.

In the literature, taxonomies of attackers exist ([92] and [96]). These taxonomies often rely on the knowledge or motivations of the attackers. On the one hand, Rounds [96] suggests an extension of the taxonomy of attackers provided by Falk [48] based on attackers’ motivations. The decomposition includes script kiddies, malware developers, hacktivist, vigilante, state sponsored hacking, thieves, defensive hackers, innocent hackers, enforcement DOS hackers terrorists. According to Landreth [96], attackers can be divided into five categories depending on their motivations (fun, curiosity, or money): novice, student, tourist, crasher, and thief. On the other hand, Pfleeger [91] bases his taxonomy on motivations of attackers but also their knowledge: amateurs, who have no motives and no knowledge, crackers, who have general knowledge but no motives, and career criminals, who are knowledgeable and motivated by money.

In the model, we can describe profiles of attackers with combinations of low, medium, and high values for “Attacker’s Resources” and “Attacker’s Motivations”. For the following analysis, we limit these two characteristics to two possible values: low and high. This allows to have four attacker profiles based on combinations of these values, which are shown in Table 7.1. At one end of the spectrum, attackers have many resources, such as strong attack skills, and are highly motivated, by money for example. In particular, this category includes professional attack-

ers. This situation translates into high values for the “Attacker’s Resources” and “Attacker’s Motivations”. At the other end of the spectrum, attackers who have little resource, such as knowledge or hardware and software resources, and little motivation, translate into the model as low values for both nodes. We include in this category scripts kiddies or attackers who have no specific motivation other than having fun and no specific material to launch attacks besides their personal computers. When attackers have specific motivations but few resources, they fall into the case where node “Attacker’s Resources” is low and node “Attacker’s Motivations” is high. This category is often neglected in existing taxonomies, as shown in Table 7.1: hacktivists, described by Falk [48] and Round [96], have political motivations but their apparent skills are low because their objective is to propagate a political message and they want to be seen. However, professional hacktivists may fall in the category of high “Attacker’s Resources” and high “Attacker’s Motivations” (e.g. Anonymous [1]). The last category with low “Attacker’s Motivations” and high “Attacker’s Resources” include attackers who have some level of motivations and have knowledge, but not enough to make it a professional activity, as opposed to the category composed of attackers with high resources and high motivations.

Both “Attacker’s Motivations” and “Attacker’s Resources” have a negative influence on “Security”, according to the model. Therefore if both characteristics have a high value, “Security” is more likely to be low than high. The only action organizations can work on is to act on the “Depth of Protection of the Asset”: Figure 7.1 shows a simplification of the model focusing on the four nodes of concern in this section.

Table 7.1: Attacker Profiles in the Model

| Attacker's Resources | Attacker's Motivations | Attacker Profile | | |
|----------------------|------------------------|----------------------------------|--------------------------|---------------------|
| | | Rounds' taxonomy | Landreth's taxonomy | Pfleeger's taxonomy |
| High | High | State-sponsored hacker, thief | Thief | Career criminal |
| High | Low | Vigilante | Crasher | Cracker |
| Low | High | Hactivist | - | - |
| Low | Low | Script kiddie, malware developer | Novice, student, tourist | Amateur |

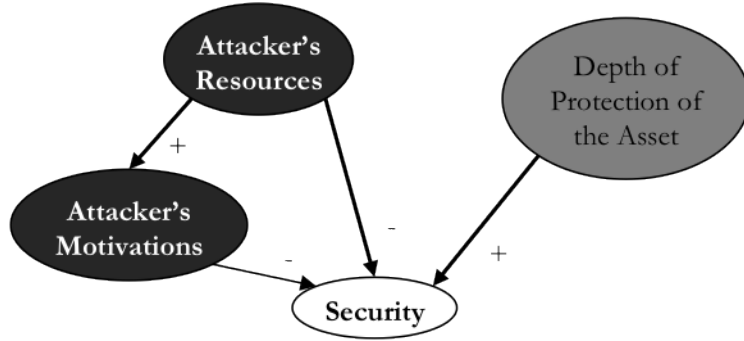


Figure 7.1: Attacker's Motivations, Resources, and Depth of Protection of the Asset in the Model

The value of “Security” is based on combinations of low and high values for characteristics “Attacker’s Motivations”, “Attacker’s Resources”, and low, medium, and high values of the “Depth of Protection of the Asset”. These three characteristics have different impacts on security: positive or negative, medium or strong influences. Intuitively, among all combinations, the case where the organization is the most secure (high “Security”) is when the “Depth of Protection of the Asset” is high and the other two attacker-related nodes are low. On the other hand, the case where the organization is the least secure is when the “Depth of Protection of the Asset” is low and the other two nodes are high. Other combinations lead to a

level of security between these two extreme cases. Values of “Security” based on its three parent characteristics are derived based on Appendix D and are referenced in Table 7.2.

Table 7.2: Value of Security given Two Possible Values of Attacker’s Motivations and Resources and Three Possible Values for Depth of Protection of the Asset

| Depth of Protection of the Asset | Attacker’s Resources | Attacker’s Motivations | Security |
|----------------------------------|----------------------|------------------------|----------|
| High | High | High | Medium |
| High | High | Low | Medium |
| High | Low | High | High |
| High | Low | Low | High |
| Medium | High | High | Low |
| Medium | High | Low | Medium |
| Medium | Low | High | Medium |
| Medium | Low | Low | High |
| Low | High | High | Low |
| Low | High | Low | Low |
| Low | Low | High | Medium |
| Low | Low | Low | Medium |

Based on this approach, IT security officers can use the model and Table 7.2 to discuss with managers that in some specific situations (where an attacker profile is considered), security needs to be enforced by improving the “Depth of Protection of the Asset”. For example, let us consider the case where an organization is targeted by highly motivated attackers (high “Attacker’s Motivations”) who appear to have strong knowledge about attacks (high “Attacker’s Resources”). If the “Depth of Protection of the Asset” is evaluated to be medium, the level of security is low according to Figure 7.2. In order to increase the level of security, actions need to be taken to improve the “Depth of Protection of the Asset”, from medium to high,

which would result in a medium level of security. Therefore, IT security officers can justify, thanks to the model, the implementation of an awareness campaign or a change in policies in order to improve the “Depth of Protection of the Asset”, hence “Security”.

7.4 Using the Model per Category of Assets

In quantitative security risk assessments, assets need to be given a value in order to perform ALE analyses. The SANS institute provides a guide step-by-step for security risk assessments [114] in which they differentiate two types of assets: tangible assets such as computers and software, and intangible assets such as patents and users’ personal data. On the one hand, the value of assets of the first category can be determined through several alternatives: IT managers can be asked the cost of tangible assets, these values can be researched on the Internet for example, or the value can be estimated from previous projects. On the other hand, two approaches are possible to value intangible assets: the cost approach consists in assessing the fair market value whereas the income approach focuses on the income-producing capability of the asset. In reality, assessing the value of assets is difficult. This section looks at the use of the “Value of the Asset from the Organization’s Point of View” in the model.

One approach to measure node “Value of the Asset from the Organization’s Point of View” consists in aggregating the value of all assets in the organization to determine a unique value. A simple scheme for aggregating the value consists in using the following equation with parameters i as the asset category, v_i as the value

for category i , and w_i as the normalized importance weight assigned to category i of assets:

$$V = \sum_{i=1}^k v_i * w_i \quad (7.1)$$

$$\sum_{i=1}^k w_i = 1 \quad (7.2)$$

Categories of assets for a University environment can include: laboratory computers, personal computers, servers and data centers, data related to human resources, grades, and health. Table 7.3 provides an example of categories and weights. Privately-owned computers, mobile devices, and personal data present on these computers and devices are of lower concern to the organization: the organization gives more importance to desktop computers because they are the organization's property and it is held liable if any problem occurs. Institutional data are of major concern as their loss would result in the loss of highly sensitive information such as financial or health data. Servers, data centers and the network infrastructure are another focus for organizations because their loss may result in unavailability of services. Research data may also be important in research universities that base their recognition among national universities on successful research.

The value v_i of category can be evaluated by an analyst or it can be calculated by multiplying the value of one asset in category i by an average value av_i of an asset in category i . For example, for an organization of 40,000 users, the value of the category "personal computers" can be calculated by multiplying 40,000 by an

Table 7.3: Example of Categories of Assets for a University Environment and Quantitative Value

| Category of asset | Weight |
|--|--------|
| Privately-owned computers, mobile devices, and personal data | 0.005 |
| Desktop computers | 0.015 |
| Research data | 0.2 |
| Servers, data centers, and network infrastructure | 0.28 |
| Institutional data (human resources, financial data, grades, health information) | 0.5 |

average value of one personal computer, assuming that each user in the organization owns a personal computer. Determining whether the computed aggregate value V is high, medium, or low in the model depends on the analyst and may be difficult to do. In addition, when managing security, IT security officers are interested in risks or potential attack scenarios targeting specific asset. Therefore, focusing on categories of assets makes more sense than looking at an aggregate asset.

Let us consider the decomposition suggested in Table 7.3. For each category, the importance of a category translates into a high, medium, or low value of “Value of the Asset from the Organization’s Point of View”. For example, if the university considers that the most important assets are the servers and data centers, and data, both categories are assigned a high value. Data concerning research may be considered of medium value and the remaining categories may be considered of low value to the organization. Table 7.4 shows an example of values by category of assets. Deciding whether a category has a high, medium, or low value depends on the analyst.

By looking at several classes of assets, instead of looking at an aggregate as-

Table 7.4: Example of Categories of Assets for a University Environment and Qualitative Value

| Category of assets | Value of the asset |
|--|--------------------|
| Privately-owned computers, mobile devices, and personal data | Low |
| Desktop computers | Low |
| Research data | Medium |
| Servers, data centers, and network infrastructure | High |
| Institutional data (human resources, financial data, grades, health information) | High |

set, IT security officers can suggest defense mechanism specific to the class of assets under investigation. Thus, the model can be used with a low value of assets when investigating personal computers for example whereas the model can be used with a high value of assets when investigating sensitive data such as grades or health information. Deciding whether a class of assets is of high or low value can be determined respectively to other classes of assets. For example, let us consider servers in the organization. Servers are a major concern for organizations as successful attacks against them can lead to unavailability of services in the organization. If the organization noticed that servers were recently attacked, it may reveal a low value for characteristic “Depth of Protection of the Asset”, the asset being the pool of servers in the organization. Therefore, IT security officers can emphasize buying new hardware or software (characteristic “Available Software and Hardware” in the model) in order to improve the “Depth of Protection of the Asset”, hence “Security” for the servers category.

7.5 Security Team Expertise and Qualities

There is an extensive literature on how to measure expertise. For example, in the field of human factors, expertise is characterized by attributes such as knowledge, experience, training, skills and familiarity with a given situation [61]. Knowledge is the “understanding of the system design, purposes, elements, functions, and operations, in relation to one’s responsibilities, position, and the specific activities or tasks undertaken” whereas experience is the knowledge and practice gained through training and interactions with the system or activities. In this work, training is defined as the common training all employees undergo while skills are defined as the abilities that require little cognitive effort. There may be similarities between present and past situations, this is how the familiarity with a given situation is defined.

Forrester’s work focuses on attributes of experts [50], which includes publications in the field of concern, professional memberships in the field, average years of academic experience on specific topics and in the field, average years of experience on specific topics and in the field, nominations by peers on specific topics or in the field, type of employee (company, organization, institution), if the company/organization/institution specializes in specific or similar fields.

Houmb suggests characterizing the trustworthiness of an information source based on two trust variables: knowledge level and expertise level. The knowledge level is evaluated by assigning weights to knowledge domains. Examples of domain knowledge include security management, network management, and code develop-

ment. The author develops a simple mathematical framework to combine all experts and domains of knowledge to derive a knowledge score and an expertise score for the set of experts.

Inspired from the previous work, we define several attributes for each member of the IT security team to characterize the “Security Team Expertise and Qualities”:

- Knowledge: Based on the SANS Training and Career Roadmap [5], the curriculum of an IT security officer should include intrusion analysis, system administration, incident handling, penetration testing, and network security. These five fields can be used to assess the level of knowledge of an IT security team. Most of the time, all officers have general knowledge in each field but they often specialize in two or three of them,
- Number of years of experience in IT security,
- Number of years of experience in IT: This indicator reveals the experience of an officer in general IT topics, such as networking. This experience allows officers to have a bigger picture of security instead of a narrowed vision,
- Number of years at current position: This information may reveal qualities of officers. If an officer has been serving for several years at the current position, it shows familiarity with tasks handled on a day-to-day basis,
- Position in diverse environments, such as a company or a governmental agency: It reflects versatility of the officer.

Table 7.5 shows an example of a team of four IT security officers. For each

attribute of the “Security Team Expertise and Qualities”, we decided on an equivalent level of “Security Team Expertise and Qualities”. This assessment relies on the analyst’s judgment. For example, regarding the knowledge within one of the five knowledge categories, if three or all four experts have the knowledge in the field, we assume a high value for the overall knowledge level. If two experts out of four have the knowledge, the overall level is considered medium. If fewer than two experts have the knowledge, we assign a low value. We apply the same rule for the attribute “Position in diverse environments”. Our rationale behind assigning a high value for the remaining three attributes rely on the presence in the team of an experienced IT security officer. For the example depicted in Table 7.5, we believe that characteristic “Security Team Expertise and Qualities” has a high value in the model.

Table 7.5: Example of Expertise and Qualities of the IT Security Team

| Information | Officer | | | | Team |
|--|---------|---|---|----|--------|
| | 1 | 2 | 3 | 4 | |
| Knowledge | | | | | |
| Incident handling | | x | | x | Medium |
| Penetration testing | | | | x | Low |
| Intrusion analysis | x | | x | x | High |
| System administration | | | x | x | Medium |
| Network security | x | x | x | x | High |
| Number of years of experience in IT Security | 1 | 3 | 2 | 10 | High |
| Number of years of experience in IT | 1 | 4 | 7 | 13 | High |
| Number of years at current position | 1 | 1 | 2 | 10 | High |
| Position in diverse environments | | x | x | | Medium |

Another approach consists in looking at the “Security Team Expertise and Qualities” given a specific attack or asset. The rationale behind this type of analysis is that domains of knowledge may have more or less importance considering a type

of attack or asset. For example, knowledge on incident handling is useful when focusing on users' personal computers or when focusing on spreading viruses. On the other hand, penetration testing may be of more concern to servers than personal computers.

7.6 Security Awareness Communication

The human element is considered the weakest link in security because it is sometimes the reason why attacks such as phishing are successful. A solution to prevent these attacks to succeed are to educate users of the organization. This is done through awareness programs.

Brodie and Wanner suggest types of training that can be used in companies to educate employees of the company [26]: classroom-style training, security awareness website, helpful hints on user screens when they log in, advertisement means such as posters and flyers. Brodie also lists a series of topics to include in security awareness: physical security, desktop security, wireless networks and security, password security, phishing, hoaxes, malware, file sharing and copyrights. On the other hand, Voss emphasizes that upper management support and funding are critical for an awareness program to be successful [119]. In addition, there should be an organizational structure with an individual or a team to support training with a specific plan. Another recommendation includes the use of multiple means of communication. Finally, Voss suggests several specific topics to include in awareness training: who the threats are and what is protected in the organization, physical and technical security awareness, policies and procedures, how incidents are handled in the

organization, social engineering, password management, email and web threats.

Table 7.6 provides a list of suggested measures that can be in place in a University environment. In an organization, the analyst should reference all means of educating users and qualitatively assess whether this list reflects a low, medium, or high level of security awareness communication. Intuitively, some measures cited in Table 7.6 have more impact than others. For example, flyers or posters are less visible than warning messages on the webmail page, therefore they may have less impact on users' awareness.

Table 7.6: List of Possible Awareness Measures

| Measure | Examples |
|----------------------------|---|
| Classroom-style training | Brown bag lunches over an IT security issue Class/workshop on IT security |
| Security awareness website | Website with podcasts, videos, examples |
| Hints on websites | "Do not share your password" on webmail "Do not share your password" on user login page |
| Advertisement | Monthly IT newsletter Posters hung at strategic places Occasional flyers distributed to users |
| Mass emails | Mass email sent when increase in phishing attacks |
| Other | Phishing attack launched by the organization |

Table 7.7 provides an example where some of the listed measures listed in Table 7.6 are implemented in an organization. In order to assess whether characteristic "Security Awareness Communication" is high, medium, or low in the model, we provide an efficiency level for each measure. Efficiency measures the impact on users. An objective measure of efficiency can be the number of users exposed to the measure. For example, the total population is concerned by messages displayed on webmail or login pages and by mass emails: therefore, the efficiency is considered

high. One can argue that after a period of time, users get used to the displayed message and do not pay attention to it anymore. However, these messages are still useful for users who are new to the organization. On the other hand, newsletters, website, posters, and flyers concern a small portion of the users population: only users who notice these actions are impacted, and these actions are considered of low efficiency. Brown bag lunches and workshops are considered of medium efficiency because their advertisement can be done via email, hence the measures target the entire user population. In addition, because they are intended to go into more details than posters or flyers on security issues, brown bag lunches and workshops are expected to improve users' knowledge and understanding of security. Hence, their efficiency is considered high.

Table 7.7: Examples of Awareness Measures in an Organization

| Efficiency | Examples | Present? |
|------------|--|----------|
| High | “Do not share your password” on webmail | Yes |
| | “Do not share your password” on user login webpage | No |
| | Mass email sent when increase in phishing attacks | Yes |
| | Phishing attack launched by the organization | No |
| Medium | Brown bag lunches over an IT security issue | Yes |
| | Class/workshop on IT security | No |
| Low | Monthly IT newsletter | Yes |
| | Website with podcasts, videos, examples | No |
| | Posters hung at strategic places | No |
| | Occasional flyers distributed to users | No |

In the example presented in Table 7.7, the organization has implemented two of the most efficient measures, one of the two medium efficiency ones, and one of the low efficiency ones. Therefore, we can consider that the “Security Awareness Communication” has a high value. Another analyst may assign different efficiency

levels than the ones suggested or may decide another value for “Security Awareness Communication”. Alternatively to the qualitative approach, a semi-quantitative one consists in providing weights to the list of possible measures and calculating an awareness score. This approach has the advantage of providing a quantitative measure but the analyst still needs to decide the thresholds between low and medium awareness levels and between medium and high awareness levels.

7.7 User’s Risk Perception

Risk perception represents the awareness of users regarding security issues. For example, if a user has a high risk perception, there is a lower probability that he/she falls for a phishing attack than for a user who has a low risk perception.

Kruger and Kearney provide a methodology to measure awareness (or risk perception) by using a scoring model [73]. A questionnaire intended to be given to users of an organization is developed and focuses on one of the three following aspects, borrowed from the social sciences: knowledge (what users know), attitude (what users think), and behavior (what users do). Each question is answered on a two-point scale (true or false) or a three-point scale (true, false, I don’t know) and a score per aspect is computed based on a weight assigned to the aspect and the number of answers. Similarly, the evaluation is done with respect to six main rules instead of the three aspects: rules include the adherence to policies, keeping passwords secret or using emails or Internet with care. This methodology provides a quantitative measurement for the organization relative to one of the three aspects and one of the three policies and allows identifying where to make improvements.

In Section 5.3.1, we provided an example of an indicator of the “User’s Risk Perception” at UMD, which is the trend of the rate of accounts corrupted by phishing attacks. Phishing attacks are attributed to users not knowing or not recognizing phishing attacks. The number of accounts corrupted by phishing attacks collected at UMD focuses on attacks targeting UMD usernames and passwords. The number of successful phishing attacks can be interpreted in a relative manner by looking at trends (e.g. through Laplace test), or in an absolute manner. If the rate of these incidents is increasing, either user’s risk perception is worsening or there is a higher number of phishing attacks. In both cases, users were not able to detect the masquerading website or email. This translates into a low value for the “User’s Risk Perception” in the model. On the contrary, if the rate is decreasing, it can be because there are fewer phishing attacks, or there are fewer victims. In the second case, the trend can be decreasing because the number of successful phishing attacks is decreasing and also because there are no successful phishing attacks. If there are no phishing attacks, the “User’s Risk Perception” is considered to be high. If the trend is decreasing but phishing attacks are still occurring, we can consider the “User’s Risk Perception” as medium in the model. Table 7.8 summarizes the values of characteristic “User’s Risk Perception” in the model based on the observed trend and values of the number of successful phishing attacks.

Investigating specific incident records collected in an organization may reveal the awareness of users. For example, viruses that spread through email attachments need that users open the attachment. When successful, these attacks reveal that users were not able to detect potential malicious content. Another example of

Table 7.8: Values of the User’s Risk Perception based on the Number of Successful Phishing Attacks

| Observation | Value of the User’s Risk Perception |
|---|-------------------------------------|
| Increasing trend | Low |
| Decreasing trend and number of successful phishing attacks not equal to 0 | Medium |
| Number of successful phishing attacks equal to 0 | High |

incident that reflects the unawareness of users is the case of viruses spreading through Instant Messenger. The same analysis on the trend of the number of these incidents as the one suggested previously provides insights into the value of the “User’s Risk Perception” in the model.

7.8 Example

7.8.1 Overall Security

We introduce a five-step method to use the model (Figure 7.2):

1. Collect evidence in the organization: Data such as the expertise of the security team, the awareness communication measures in place, or the user’s risk perception should be gathered,
2. Set evidence in the model: Collected evidence should be mapped to the model and translated into a low, medium, or high value,
3. If needed, consider parameters: If the organization is concerned by a category of attackers with low or high values of resources and/or motivations, the model allows representing specific scenarios. This step is optional,

4. Propagate evidence and parameters in the model: The types and strengths of influences allow propagating values related to evidence and parameters through the model. Appendix D provides a technique to propagate values in the model,
5. Provide recommendations: The visual representation allows determining the actions that the organization can take to improve security.

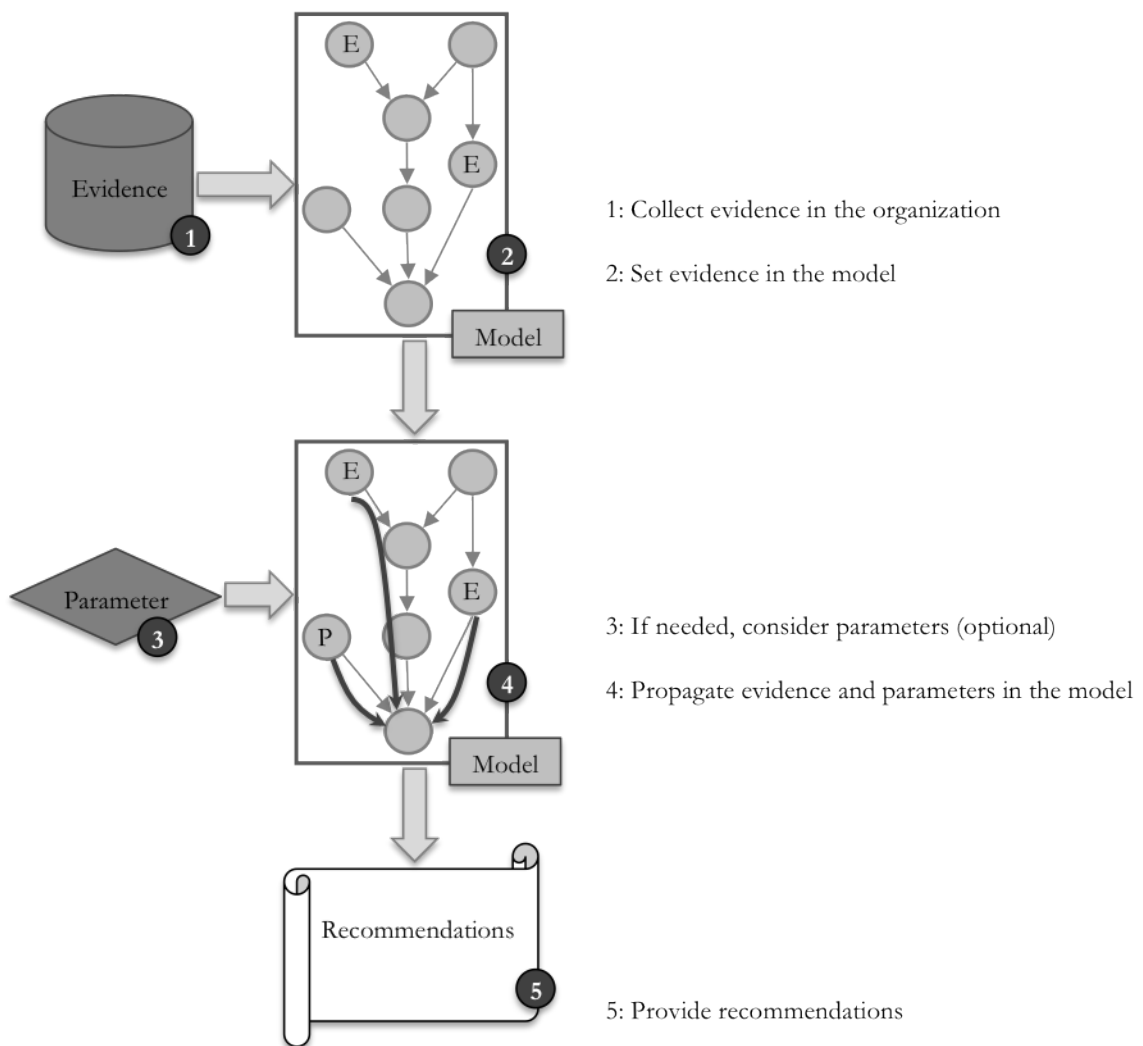


Figure 7.2: Five-Step Method to Use the Model

Let us consider a fictional organization for the purpose of illustrating the use of the model. This organization is a university including 40,000 users. The IT security team is composed of four experts whose expertise and qualities are the ones depicted in Table 7.5. In addition, awareness measures are in place to raise users' awareness on attacks and include mass email sent to warn users against current attacks and a "Do not share your passwords with others" on the webmail page. If a budget of 100,000 US dollars is available, how should the budget be allocated to improve the overall security?

Both pieces of information on the IT security team expertise and qualities and on the awareness communication campaigns in place represent gathered evidence resulting from step 1. With this set of experts, we assess that the value of the "Security Team Expertise and Qualities" is high and communication measures are interpreted by a medium value for "Security Awareness Communication" (step 2). On the one hand, "Security Team Expertise and Qualities" positively influences "Security Policies", which results in a high value of "Security Policies". On the other hand, "Security Awareness Communication" positively influences "User's Expertise in Using Computers or/and in Security", which provides a medium value of the latter characteristic. Besides, "User's Risk Perception" is influenced by medium values of "Security Awareness Communication" and "User's Expertise in Using Computers or/and in Security", thus has a medium value. "Depth of Protection of the Asset" is then impacted by four parent characteristics:

- "Security Policies", which has a medium positive influence and a high value,

- “User’s Risk Perception”, which has a strong positive influence and a medium value,
- “User’s Expertise in Using Computers or/and in Security, which has a medium positive influence and a medium value,
- “Security Team Expertise and Qualities”, which has a medium positive influence and a high value.

These pieces of information result in a medium value of “Depth of Protection of the Asset”, as explained in Appendix D. With no evidence on the attacker, this value translates into a medium value for “Security” (step 4). Figure 7.3 shows the model with set evidence and propagated values: evidence gathered in steps 1 and 2 are represented as bubbles whereas propagated evidence resulting from step 4 are depicted by dashed squares.

IT security officers can then use the model to start the discussion with managers on how to invest in security. Improving security implies improving the level of the “Depth of Protection of the Asset”. Several alternatives are possible. First, improving the “User’s Risk Perception” by implementing additional awareness measures would result in a high value of the “Security Awareness Communication”, which impacts “User’s Risk Perception” and “User’s Expertise in Using Computers or/and in Security”. Ultimately, this alternative propagates into high values of the “Depth of Protection of the Asset” and of “Security”. Another solution consists in buying new security devices or software in order to set a high value to characteristic “Available Software and Hardware”, which would result in high values of “Depth

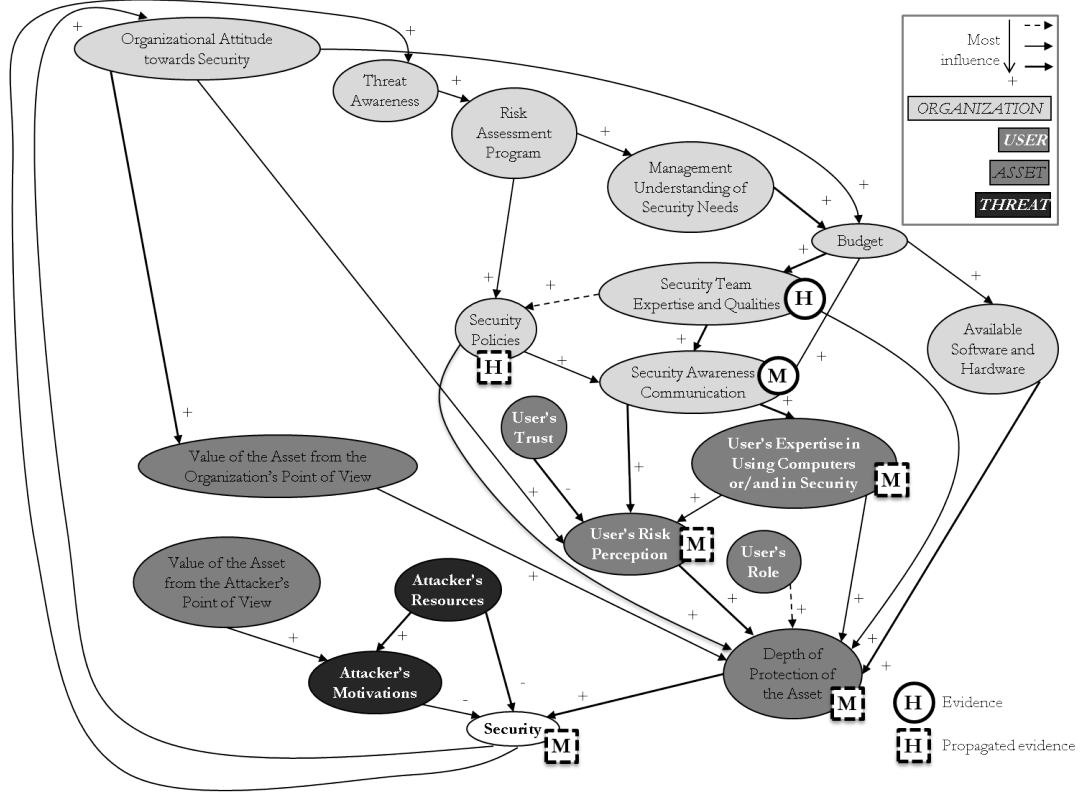


Figure 7.3: Model with Pieces of Evidence Gathered in an Organization - H, M, and L stand for High, Medium, and Low respectively

of Protection of the Asset” and “Security”. In order to compare both alternatives, we need to look at the weights of each measure on the first common characteristic in the model. On the one hand, the first solution, through “User’s Risk Perception” and “User’s Expertise in Using Computers or/and in Security”, impacts the “Depth of Protection of the Asset” with a strong and a medium influence. On the other hand, the second solution impacts the “Depth of Protection of the Asset” with a strong influence. Therefore, the first solution is preferred. The strength of the model resides in the common language that it brings between experts in IT security and managers, who have less IT security expertise. The model allows opening the discussion between the two parties in order to implement the most suitable solution.

7.8.2 Using Facets

Although organizations are interested in managing the overall security, they are often also concerned with specific categories of assets or classes of attackers. We introduce the concept of facet to address this issue. A facet is *a perspective of the model*. The model can be used by focusing at specific facets, including a specific asset category or attack type. For example, the model can be used to study the facet “phishing attacks” to determine the actions to pursue to improve the level of security of the organization against phishing attacks.

We define a systematic six-step method to use the model in an organization. The six steps are the following (Figure 7.4):

1. Select a facet: The organization can decide to investigate a specific attack type (e.g. phishing) or a category of assets (e.g. institutional data),
2. Collect evidence on the specific facet: Evidence can be collected in the organization, such as the level of IT security team expertise for the specific asset. For instance, network security knowledge and skills are important when focusing on asset category “servers”,
3. Set evidence in the model: Evidence is mapped to low, medium, or high values of characteristics in the model,
4. If needed, consider parameters: The organization may be concerned with a specific category of attackers (of high or low values of resources and motivations). This step is optional,

5. Propagate evidence and parameters in the model: Through the types and strengths of influences in the model, collected evidence and parameters are propagated in the model to determine a level of security with respect to the facet under study. Appendix D provides a technique to propagate values in the model,
6. Provide recommendations: Depending on the analysis, IT security officers can recommend security solutions to improve the level of security with respect to the facet.

In order to illustrate the approach, let us consider a fictional organization. This organization is a university including 40,000 users. The IT security team is composed of four experts whose expertise and qualities are the ones depicted in Table 7.5. We present in the next subsections two examples to illustrate how to set evidence in the model, propagate evidence throughout the model, and draw conclusions. These examples show how the model can be used from specific facets.

7.8.3 Facet 1: Servers

In this first facet, we are concerned with the level of security of servers in the organization (step 1). The second step of the analysis consists in gathering evidence on this facet. According to Section 7.4, servers are considered an important asset for which the value is high (Table 7.4). All knowledge domains for IT security officers defined in Table 7.5 but incident handling are concerned with servers: indeed, incidents mostly focus on computers rather than servers. Based on the other four knowledge domains and the other attributes, we interpret that the level of expertise

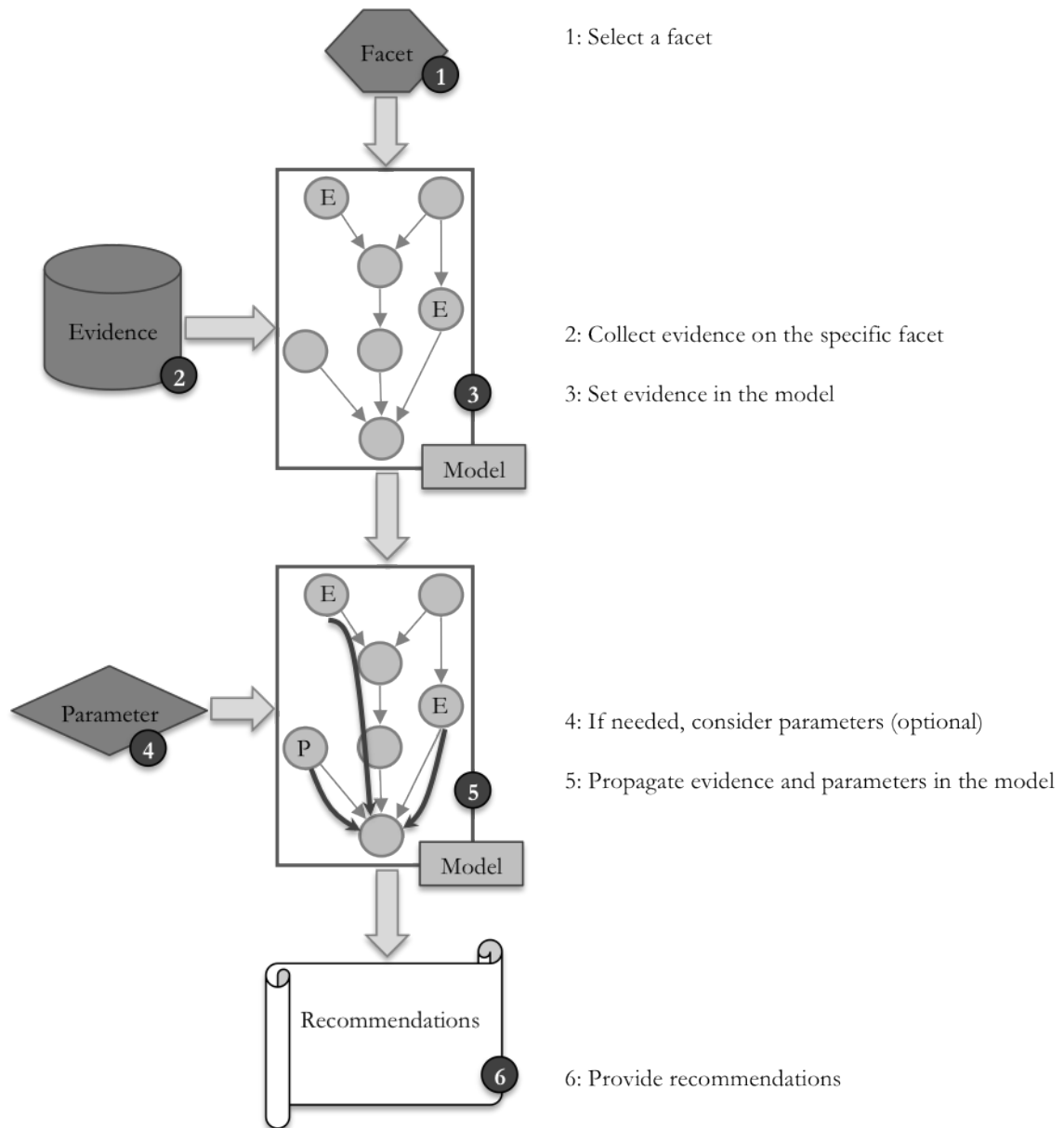


Figure 7.4: Six-Step Method to Use the Model within a Facet

and qualities of experts is high. In the model, we translate these two pieces of evidence as (step 3):

1. Characteristic “Value of Asset from the Organization’s Point of View” is high because we focus on servers which has been identified as one of the most important assets of the organization,

2. Characteristic “Security Team Expertise and Qualities” is high based on the attributes of the team of four experts.

The next step of the analysis consists in propagating these values into the model. On the one hand, “Value of the Asset from the Organization’s Point of View” positively impacts the “Depth of Protection of the Asset”. On the other hand, the “Security Team Expertise and Qualities” positively impacts the “Depth of Protection of the Asset” through several paths. The ones that go through characteristics related to users, such as “Security Awareness Communication”, do not concern servers. The paths that are concerned by servers are the following:

1. From “Security Team Expertise and Qualities” to “Security Policies”, and “Depth of Protection of the Asset”,
2. From “Security Team Expertise and Qualities” directly to “Depth of Protection of the Asset”.

Therefore, the high value of “Security Team Expertise and Qualities” transfers to “Security Policies”. “Depth of Protection of the Asset” is influenced by high values coming from “Value of the Asset from the Organization’s Point of View”, “Security Policies”, and “Security Team Expertise and Qualities”, and is subsequently high. In addition, “Depth of Protection of the Asset” impacts “Security”. Its effects are counteractions of the “Attacker’s Motivations” and “Attacker’s Resources” and depending on their values (high or low), “Security” has different values. Based on Figure 7.1, the only case where “Security” is not high is the case where both “Attacker’s Motivations” and “Attacker’s Resources” are high. Figure 7.5 shows

the model for the facet under investigation: evidence on characteristics “Value of the Asset from the Organization’s Point of View” and “Security Team Expertise and Qualities” are set as bubbles, parameters on the attacker-related characteristics are depicted by diamonds, and propagated values of “Security Policies”, “Depth of Protection of the Asset”, and “Security” are represented by dashed squares (step 5).

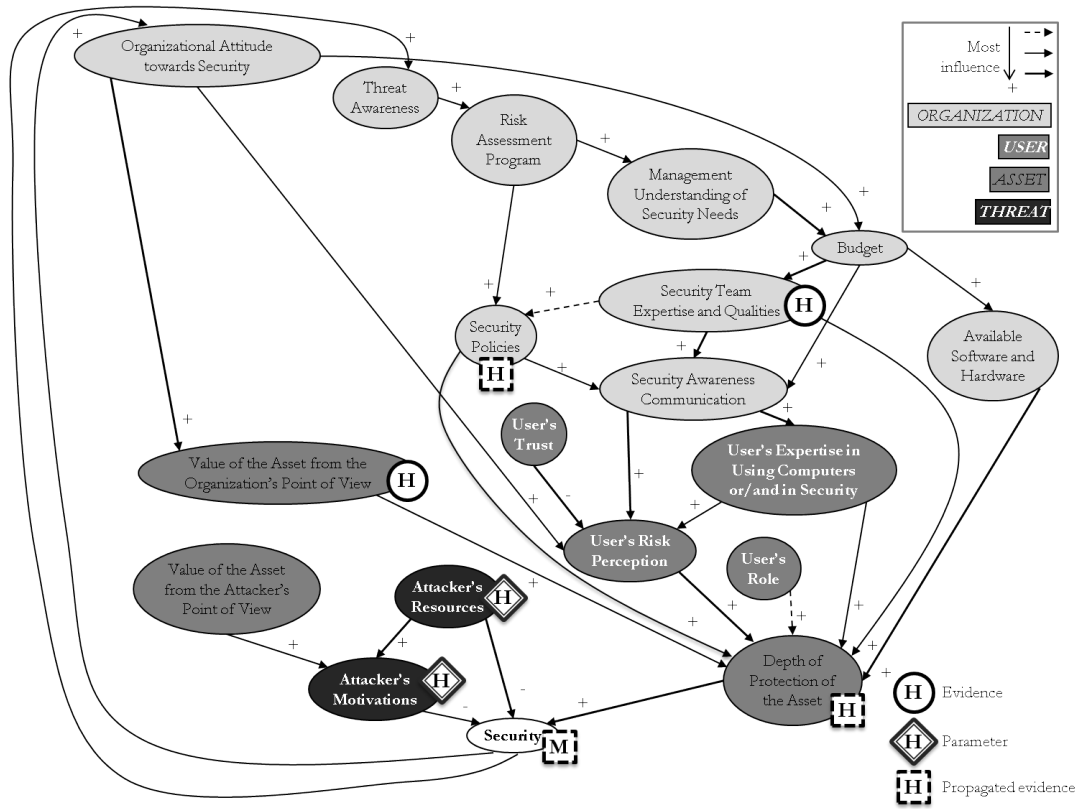


Figure 7.5: Model with Pieces of Evidence for Servers - H, M, and L stand for High, Medium, and Low respectively

In order to increase the level of “Security” of servers, the model identifies a set of possible actions (step 6). The “Depth of Protection of the Asset” can be improved by only targeting characteristic “Available Software and Hardware”, as the other actions impact users (“User’s Risk Perception”, “User’s Role”, and “User’s

Expertise in Using Computers or/and in Security”) and users are not concerned with the facet servers. Therefore, IT security officers can recommend investing in stronger software or additional hardware to protect servers. The model serves as a support for IT security officers and managers to discuss security solutions specific to a category of asset.

7.8.4 Facet 2: Phishing Attacks

In this section, we focus on a common social engineering attack: phishing (step 1). Step 2 consists in collecting evidence: as we are concerned about phishing attacks, assets at risk are users’ personal data. In addition, the expertise of IT security officers relevant to phishing attacks should be gathered. Finally, security awareness actions in place are important to raise users’ awareness.

Phishing attacks target information of users, which is considered as a low-value asset by the organization (Table 7.4) with respect to other assets that belong to the organization, such as servers and institutional data. Based on the fact that the IT security team is an experienced one with an IT security officer having 13 years of experience in IT, we interpret that their expertise with respect to phishing attacks is high. In addition, awareness measures are in place to raise users’ awareness on phishing attacks and include mass email sent to warn users against current phishing attacks and a “Do not share your passwords with others” on the webmail page. These measures are interpreted by a medium value for awareness communication on phishing attacks. In summary, pieces of evidence regarding this facet are the following (step 3):

- Low value for the “Value of the Asset from the Organization’s Point of View”,
- High value for the “Security Team Expertise and Qualities”,
- Medium value for the “Security Awareness Communication”.

Next, these values propagate in the model. On the one hand, the value of “Security Team Expertise and Qualities” results in a high value of “Security Policies”. On the other hand, the value of “Security Awareness Communication” translates into a medium value of “User’s Risk Perception” and “User’s Expertise in Using Computers or/and in Security”. Therefore, “Depth of Protection of the Asset” is influenced by five values:

- Low value of “Value of the Asset from the Organization’s Point of View” which has a medium positive influence,
- High value of “Security Policies” which has a medium positive influence,
- Medium value of “User’s Risk Perception” which has a strong positive influence,
- Medium value of “User’s Expertise in Using Computers or/and in Security” which has a medium positive influence,
- High value of “Security Team Expertise and Qualities” which has a medium positive influence.

The combination of this information results in a medium value of “Depth of Protection of the Asset”. More details on how to combine these pieces of information

to derive this value are provided in Appendix D.

In addition, “Depth of Protection of the Asset” positively impacts “Security” but the value of “Security” also depends on parameters related to the attacker’s attributes. Phishing attacks are highly motivated as the objective is to gather credentials of users. Phishing attacks are considered a professional activity, thus characteristic “Attacker’s Resources” is considered high. Considering high values of the “Attacker’s Motivations” and “Attacker’s Resources” and a medium value of the “Depth of Protection of the Asset”, “Security” is low (Figure 7.1). Figure 7.6 shows the model representing the facet under concern (step 5).

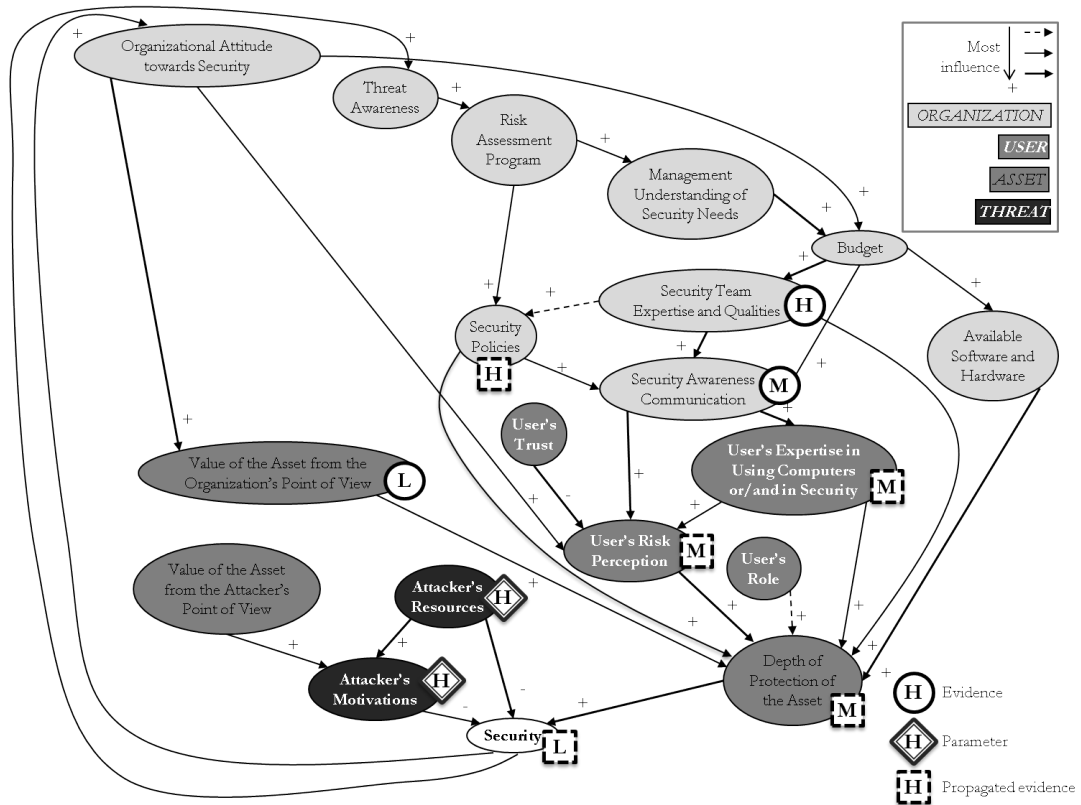


Figure 7.6: Model with Pieces of Evidence for Phishing Attacks - H, M, and L stand for High, Medium, and Low respectively

In order to increase the level of security, IT security officers can recommend

actions based on the model (step 6). Increasing “Security” implies increasing the “Depth of Protection of the Asset”, which is impacted by five characteristics. “Available Hardware and Software” are not concerned with phishing attacks as the success of phishing attacks relies on the inability of users to recognize a masquerading entity. Besides, organizations cannot act on characteristics “Value of the Asset from the Organization’s Point of View” and on “User’s Role”. However, organizations can make decisions that impact the “User’s Risk Perception” or the “User’s Expertise in Using Computers or/and in Security” by improving the “Security Awareness Communication”. For example, organizations can implement additional awareness measures such as adding a warning message against phishing attacks on the login webpage or increase the funding allocated to awareness to develop workshops to make users sensitive. Improving awareness communication to act against phishing attacks is intuitive but the model brings a support for communication and a common language between IT security officers and managers.

7.9 Summary

In this chapter, we presented an approach to incorporate in the model measurements collected in organizations. We looked at five characteristics in the model: “Attacker’s Motivations”, “Attacker’s Resources”, “Value of the Asset from the Organization’s Point of View”, “Security Team Expertise and Qualities”, “Security Awareness Communication” and “User’s Risk Perception”. We suggested using the first three characteristics to derive facets to investigate. For example, high values of the attacker’s motivations and resources represent professional hackers whereas low

values represent script kiddies. In addition, we defined categories of assets so that analyses can focus on specific assets of importance for the organization such as institutional data or servers and data centers. We provided recommendations on how to measure the “Security Team Expertise and Qualities” through a set of attributes, including the IT security officers’ knowledge and years of experience at the current organization. “Security Awareness Communication” is measured through a checklist of several awareness measures such as the implementation of IT security classes in the organization. Finally, we used the trends of the number of successful phishing attacks as evidence on the “User’s Risk Perception”. Presented measurements are mostly qualitative and the use of an analyst usually allows the interpretation of a measurement into a low, medium, or high value in the model. For each measurement, we provided an example to show how we would interpret the measurements.

In the last section of this chapter, we presented a systematic five-step method to incorporate evidence in the model. The method is illustrated with an example in order to study how to invest in security in an organization. We introduced a systematic six-step method to focus on facets. The approach is illustrated through two facets. The first one focused on the category of assets composed of servers in a fictional organization. We integrated pieces of evidence collected at the organization that are specific to the facet. Other characteristics in the model serve as parameters, such as the attacker-related characteristics. We illustrated the propagation of evidence and parameters in the model to derive a level of security and suggest recommendations that would specifically target servers. In the second selected facet, we looked at phishing attacks. These examples show that not only the model can be

used to make decisions at the high level, but also by specifically looking at facets.

Chapter 8

Conclusions

8.1 Summary

In this dissertation, we presented an approach to help decision making in IT security. The approach consists in the development of a model that identifies major components of security, with a focus on the human elements (attacker, user, organization), characteristics of each component, and causal influences among characteristics. Influences have two attributes: a type, which is positive, negative, or neither positive nor negative, and a strength, which is weak, medium, or strong. The model is represented with nodes to represent characteristics and arrows to depict relationships among them. The visual representation of the model allows IT security experts and people with less expertise, such as managers, to communicate on a common basis.

In the second chapter of this dissertation, we presented existing frameworks to manage IT security. We emphasized that existing methods are often not applicable in practice and that it may not be easy to communicate their results with other key players in IT security. We then referenced supporting literature on characterization of the human elements involved in security: user, attacker, and organization. Finally, we documented the literature to develop and validate a model.

In the third chapter of this dissertation, we introduced an approach for developing and validating such a model based on experts' opinions and empirical data. However, as there is mistrust of anyone who tries to understand how practitioners

act and think, managing to involve experts in the model development and validation processes is difficult. Second, obtaining empirical data collected in organizations is challenging because organizations are often not inclined to share data, even if they were, there is no accepted security metrics, and available information is frequently incomplete. In this context, we developed a carefully thought approach, although imperfect, for the development and validation of a model. The development is based on interviews and surveys of IT security experts, and the validation is based on both experts and data.

In the fourth chapter of the dissertation, we presented the results of the model development for academic environments. We first developed a model based on the existing literature of characteristics of the human elements involved in security (attacker, user, organization) and on several months of discussion with the Director of Security at UMD. We interviewed experts at other academic environments and managed to obtain two two-hour interviews. The outputs of the interviews were the following: a suggestion of a decomposition of security (for example attacker, user, organization, and asset) and a complete model with characteristics and influences among them. Characteristics of these models are extracted and used in the survey. The survey was sent to an EDUCAUSE listserv and fifteen experts took the survey. The survey's objective was to gather agreement or disagreement on a suggested decomposition of security in "threat, user, organization, and asset" and to gather experts' opinion on the strength of the influence of a list of characteristics on security. A model was derived from these three sources of information (initial model, interviews, and surveys).

The model is then submitted to the validation process in the fifth chapter of this dissertation. We presented a two-step validation process. First, the model was sent to interviewed experts and to experts who took the survey and provided us with an email address. Two out of five experts provided us with feedback and the model was modified accordingly. Second, we developed a method to validate influences in the model with data collected at UMD. We investigated the trend of the rate of security incidents before and after the implementation of a security measure to see if it matches the outcomes expected after the implementation of the measure (e.g. sudden decrease afterwards). Besides, the measure is mapped to a path in the model, from a characteristic to “Security” for example. Therefore, if analysis of the trend matches the expected outcomes, the portion of the model under validation is validated. Otherwise, the model should be reviewed accordingly. We presented the analysis of five different measures and showed that none contradicted the expected outcomes.

The model that was developed and partly validated in Chapter 4 and Chapter 5 is presented in Chapter 6 of the dissertation. We identified four components of security: threat, user, organization (IT security officers and managers), and asset. For each of these components, we described a list of characteristics. They include the attacker’s motivations and resources, the user’s risk perception and expertise in using computers or/and in security, the organizational attitude towards security, the security team expertise, the value of the asset, and its depth of protection. In this chapter, we also show how the model can be used qualitatively to reason about security.

In Chapter 7, we tried to push the capabilities of the model further. When using the model in their environment, organizations want to know how to make the model organization-specific, in other words, they want to know how they can measure characteristics. However, the road towards the full measurement of characteristics the model is a tedious one. We proposed a series of techniques and examples to show that measuring characteristics in the model, although imperfect, is possible. We focused on five characteristics: “Attacker’s Motivations”, “Attacker’s Resources”, “Value of the Asset from the Organization’s Point of View”, “Security Awareness Communication, and “User’s Risk Perception”. We introduced the concept of facet as a perspective of the model: the model can be used by looking at a specific class of attackers or at a specific category of assets. We present a systematic five-step approach to use the model in an organization, and derived a six-step approach to use facets.

8.2 Contributions

The objective of this research is to provide IT security officers a tool to start reasoning about IT security, and a support to communicate with decision makers. More specifically, the contributions are the following:

- *Development of an approach to produce a model to help reasoning and communicating about IT security*: the approach consists in developing an influence-based model that identifies major components of security, characteristics of components, and influences among them. This provides IT security teams and managers a clear, high-level picture of what should be considered when

managing security,

- *Development of a systematic method to apply the model in organizations:* we provided directions on how to measure some characteristics in the model and developed a method to incorporate evidence in the model. We introduced the concept of facet to use the model from different perspectives at a lower level of detail,
- *Development and validation of a model for academic environments:* the development and validation of this model rely on a combination of experts and empirical data. More specifically, they include a detailed model based on the literature and on discussions with the Director of Security at UMD, two models resulting from interviews with experts, surveys answered by fifteen experts, and empirical data collected at UMD. The model is flexible and characteristics or relationships can be added or removed if other analysts disagree with the presented model.

8.3 Future Work

Evaluation of the usability of the model

We showed in Chapter 6 and Chapter 7 how the model can support reasoning about security. We believe that the model would improve reasoning about security and would improve communication while making decisions in practice. However, we did not evaluate it. A relevant approach to address this issue would be to conduct an evaluation of the usability of the model: it would be insightful to take part in

a meeting with IT security officers and observe them brainstorm on security issues as well as to observe IT security officers convince managers to invest in a solution. In addition, brainstorming and convincing managers without the model on the one hand and with the model on the other hand should be compared. We envision that the model allows a documentable, repeatable, justifiable process of brainstorming and decision making.

Measurement of the model

In Chapter 7, we provided measurements for a set of characteristics. Although the task is tedious and complex, we demonstrated that providing useful, practical measurements for characteristics in the model is achievable. It is important for organizations to have directions on indicators of characteristics in the model, such as the “User’s Expertise in Using Computers or/and in Security”, “Organizational Attitude towards Security” and “Budget”, and on how to map measurements in the model. Indicators can be qualitative or quantitative, and measuring them in organizations should be possible in practice.

Quantification of the model

The model presented in this dissertation is qualitative at several levels. First, values of characteristics are assessed through low, medium, and high values. Second, the influence of one characteristic on another is a weak, medium, or strong influence. Third, when alternatives are possible, one decision is made because it has relatively more impact on security than another one. We showed in Chapter 6 and Chapter 7 that, although qualitative, the model is still useful and insights can be gained. Deriving a quantitative model would allow more accurate conclusions.

Several aspects in the derivation of a quantitative model could be considered:

- *Development of a quantitative framework:* For example, a Bayesian Belief Network (BBN) can be derived from the causal model presented in this dissertation. The quantification of the BBN can be supported by experts or empirical data, but may be challenging. A solution is to derive an algorithm to quantify the BBN based on the type and strength of influences. By setting evidence on characteristics in several alternatives, a probability may be computed for security that would be meaningful in a relative manner. If a BBN is selected, one should take care of loops in the model,
- *Incorporation of models at a lower level:* The model presented in this dissertation is a high-level model. For some characteristics, such as attackers' behavior, models have been developed at a lower level. It would be relevant to study how to incorporate these detailed models into our comprehensive approach,
- *Fusion of several types of data:* Empirical data can support the quantification of characteristics. Another relevant approach, when empirical data is unavailable, is to use simulations. Combining experts' opinions, empirical data, and simulations, would bring another level of refinement and more accuracy to the model.

Development of the model in other environments

In this dissertation, we introduced an approach to help reasoning and communicating about security issues and presented a model. Although the model was

developed based on experts and data in academic environments, we believe that some characteristics and influences in the model are applicable to other environments. In addition, as the model is flexible, one can easily modify it by changing, adding, or removing characteristics or influences. A solution to address the issue of the applicability of the model in other types of organizations is to conduct the development and validation of a model in these environments based on the method provided in Chapter 3.

Appendix A

Interview Questionnaire

This appendix is composed of two elements:

- An interview sheet: It is a support for interviewees to gather general information on the interviewer's expertise and organization,
- A six-page questionnaire: It is provided to the interviewer and is collected at the end of the interview.

Interview

Interview date and time: _____

Expert's name: _____

Email: _____

Phone number: _____

Address: _____

Organization: _____

1/ What is your job title?

2/ How many computers/servers do you manage?

3/ How many people are there in the IT department? How many specifically work in IT security?

4/ How many years have you been at this position?

5/ What is your total number of years of experience?

6/ What are your previous work experiences?

Model-Based Information Security Management

This interview is part of a research led at the University of Maryland to develop a model to manage security. This model will 1) **allow security administrators assess and manage information security** at their organizations and 2) be a **tool for communication** with decision makers and users. The model is a causal model that 1) identifies **characteristics that influence security**, and 2) determines **relationships between these characteristics**.

Question 1: What are the characteristics for each of the 4 main components that increase or decrease the number of unsuccessful attacks in an organization?

In our study, we will consider 4 main components:

- The **attacker** (“an individual who attempts one or more attacks in order to achieve an objective”),
- The **user** (“someone who uses a computer”),
- The **organization** (“a social arrangement, which pursues collective goals, which controls its own performance, and which has a boundary separating it from its environment”; includes the IT team), and
- The **asset** (everything owned by a person or company; includes computers and data).

► Should other components be considered?

Characteristics consist in attributes of each of the 4 main components that have an influence on increasing or decreasing security.

► On Page 2, provide the list of characteristics for each of the 4 main components.

Example: We want to model human error in a power plant. A characteristic for human error is the operator’s fatigue, stress, or knowledge of procedures.

Model-Based Information Security Management

| | |
|--------------|-------|
| Attacker | User |
| Organization | Asset |

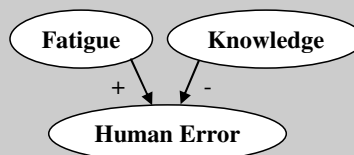
Model-Based Information Security Management

Question 2: How do characteristics influence one another to increase or decrease the number of unsuccessful attacks?

In order to end up with a tool for communication purposes, we will use a visual representation where characteristics will be represented as **bubbles**. Relationships between characteristics will be depicted by **arrows**. We will define **positive** (“+”) or **negative** (“-”) influences.

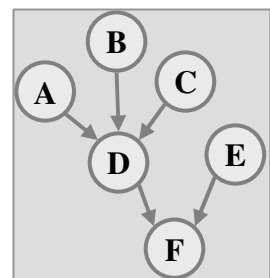
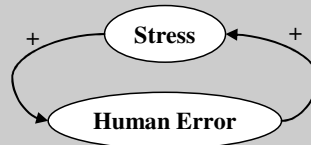
► Draw a figure that includes a) bubbles to represent the characteristics you identified in question 1, b) arrows to represent influences between these characteristics, c) “+” or “-” to represent the type of influence.

Example: The operator’s fatigue and knowledge influence the human error. The more fatigue, the more prone to error. On the contrary, the more knowledge on the procedures, the fewer errors. These influences are depicted by a positive influence (“+”) of the fatigue on the human error and by a negative influence (“-”) of the knowledge on the human error.

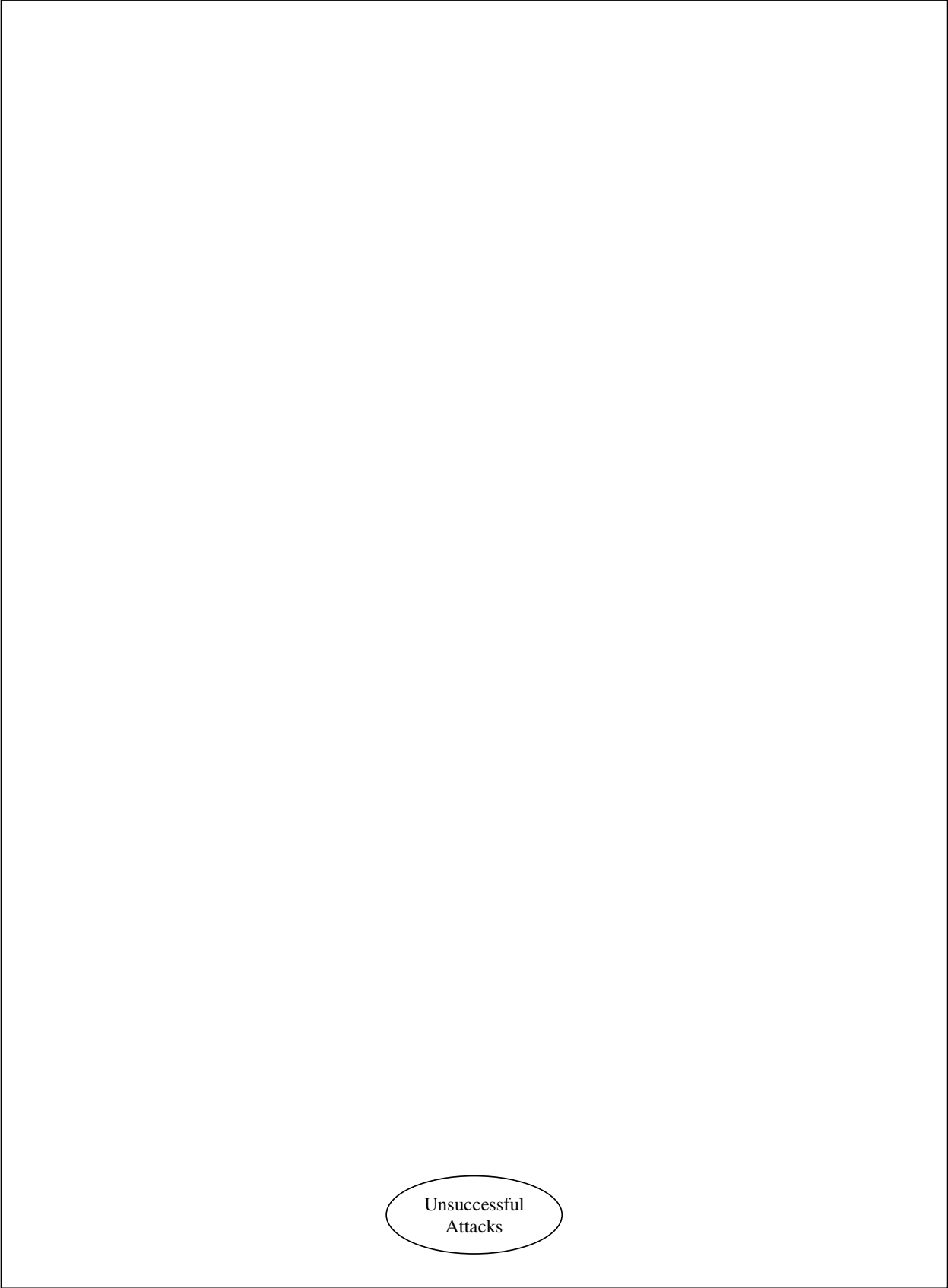


Loops may be considered.

The more stress an operator is exposed to, the more prone to error he/she is. Besides, the more errors he/she makes, the more stress he/she has.



Model-Based Information Security Management



Unsuccessful
Attacks

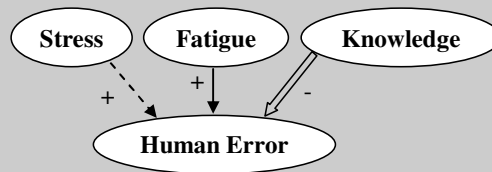
Model-Based Information Security Management

Question 3: What are the most/least influencing characteristics?

When several characteristics influence one characteristic, the thickness of the arrow will depict the strength of the influence.

► Depict the strengths of arrows in your figure (Page 4).

Example: The operator's fatigue, knowledge and stress influence the human error. Fatigue and stress positively influence the human error whereas knowledge negatively influences the human error. We will assign a thickness to arrows to depict the strength of influences. For example, knowledge of the operator has the highest influence on the human error: we will assign a thick arrow to that influence. Fatigue has a higher influence than stress on the human error and will be assigned a thin arrow while stress will be assigned a dashed arrow.



Blank Page

Appendix B

Survey Questionnaire

This appendix provides snapshots of the online survey sent to IT security officers. It includes:

- Introduction page,
- Questions about the experts' experience and organization,
- Questions on the decomposition of security into “users, organization, threat, assets”,
- Questions on the strength of characteristics on security,
- Questions on the impact of two security measures,
- Thank you page.



Model for assessment of IT security

This questionnaire is part of a research led at the University of Maryland to develop a model for IT security to **help security-related decision making**.

Our objective is to provide decision makers with a model to **justify their choices** of implementing one security decision versus another one. Examples of questions that the model will address include:

- How well do our current protections perform?
- How can we justify our security decisions?
- What would change if we implemented additional protections?

This survey consists of 5 pages and should take you **15 minutes to complete**. Please make sure to click on the "Submit" button on the last page to send your answers.

Information that may identify you will remain **strictly confidential**. We will never share this information with any third party. The results of this study will be **anonymized for further publications**.

Start the survey

Model for assessment of IT security

* Required

Page 1/5 - About you

This section allows us to assess your background and expertise in IT security.

What is the name of your organization?

What is your job title? *

How long have you spent at this position? *

Please list your previous IT-related job experiences along with the number of years spent at that position.

Please use the following format: experience - n years. For example "IT security officer - 2 years"

Continue »

Model for assessment of IT security

* Required

Page 2/5 - About your organization

This section allows us to assess the size of your organization.

Number of users? *

A user is anyone who uses a computer (includes students).

Number of people working in the IT department? *

Number of people working specifically in IT security? *

« Back

Continue »

Model for assessment of IT security

* Required

Page 3/5 - Components of security

When modeling security, we identified four components: a) users (anyone who uses a computer), b) organization (includes security team and managers), c) threat (anything that has the potential to do harm and includes attackers), d) assets (include computers and data).

How confident are you in the previous decomposition (users, organization, threat, assets)? *

- ☐ Very confident
- ☐ Confident
- ☐ Somewhat confident
- ☐ I don't believe in this decomposition

If you don't believe in this decomposition, what decomposition would you recommend?

How confident are you in the description of the components users, organization, threat, assets? *

Users: anyone who uses a computer. Organization: includes security team and managers. Threat: anything that has the potential to do harm and includes attackers. Assets: include computers and data.

- ☐ Very confident
- ☐ Confident
- ☐ Somewhat confident
- ☐ I don't agree with one or some of the descriptions

If you don't agree with one or some of the descriptions, what description would you recommend?

« Back

Continue »

Model for assessment of IT security

* Required

Page 4/5 - Influencing characteristics

In this section, we want to capture your opinion on the characteristics that influence security. Characteristics consist in attributes of the users, organization, threat or assets, which may have an influence on increasing or decreasing security.

Please indicate how strong you consider the influence of the following characteristics on the security level.

Characteristics related to the component "users" *

Users: anyone who uses a computer.

| | No influence | Weak influence | Medium influence | Strong influence |
|--|-----------------------|-----------------------|-----------------------|-----------------------|
| User's risk perception | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| User's trust | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| User's exposure to security (for example through media) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| User's theoretical knowledge in using computers or/and in security | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| User's experience in using computers or/and in security | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| User's gender | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| User's age | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| User's place of birth | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

| | | | | |
|---|-----------------------|-----------------------|-----------------------|-----------------------|
| User's role (if the user is an undergraduate/graduate student, a faculty, a staff, an intern, etc...) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
|---|-----------------------|-----------------------|-----------------------|-----------------------|

Characteristics related to the component "organization" *

Organization: includes security team and managers.

| | No influence | Weak influence | Medium influence | Strong influence |
|---|-----------------------|-----------------------|-----------------------|-----------------------|
| Security awareness communication to users | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Management understanding of security needs | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Security team talent | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Security team qualities (for example withstanding stress) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Financial resources available for security | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Available security hardware (for example security devices such as intrusion prevention systems) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Available security software (for example patches, signatures) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Risk assessment program | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Security policies | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Organizational attitude towards security | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Threat awareness | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Characteristics related to the component "threat" *

Threat: anything that has the potential to do harm and includes attackers.

| | No influence | Weak influence | Medium influence | Strong influence |
|---|-----------------------|-----------------------|-----------------------|-----------------------|
| Attacker's motivations | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Attacker's expertise | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Attacker's qualities (for example perseverance) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Characteristics related to the component "assets" *

Assets: include computers and data.

| | No influence | Weak influence | Medium influence | Strong influence |
|---|-----------------------|-----------------------|-----------------------|-----------------------|
| Value of the asset from the attacker's point of view | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Value of the asset from the organization's point of view | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Depth of protection of the asset (includes all protections of an asset - passwords, firewalls...) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

If there are other characteristics that influence security and that were not cited before, please list them here.

[« Back](#)[Continue »](#)

Model for assessment of IT security

* Required

Page 5/5 - Influencing characteristics

In this section, we want to capture your opinion on the impact of the implementation of two security decisions: a) implementation of a communication campaign to make users sensitive to security issues, b) installation of additional security devices such as intrusion prevention systems.

How would you rate the impact on security of the aforementioned implementations? *

| | No impact | Weak impact | Medium impact | Strong impact |
|---|-----------------------|-----------------------|-----------------------|-----------------------|
| Implementation of a communication campaign to make users sensitive to security issues | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Installation of additional security devices, such as intrusion prevention systems | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

Please rate the influence of the implementation of a communication campaign on the following characteristics. *

| | No influence | Weak influence | Medium influence | Strong influence |
|---|-----------------------|-----------------------|-----------------------|-----------------------|
| User's risk perception | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| User's exposure to security (for example through media) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| User's education | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| User's expertise | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Risk assessment program | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Depth of protection of the asset (includes all protections of an asset - passwords, firewalls...) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

| | | | | |
|--|-----------------------|-----------------------|-----------------------|-----------------------|
| Financial resources available for security | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Organizational attitude towards security | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

What other characteristics, if any, are impacted by the implementation of a communication campaign?

Please rate the influence of the installation of additional security devices on the following characteristics. *

| | No influence | Weak influence | Medium influence | Strong influence |
|---|-----------------------|-----------------------|-----------------------|-----------------------|
| Depth of protection of the asset (includes all protections of an asset - passwords, firewalls...) | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Risk assessment program | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Security policies | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Organizational attitude towards security | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Attacker's motivations | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

What other characteristics, if any, are impacted by the installation of additional security devices?

« Back

Continue »

Model for assessment of IT security

Thank you for your participation!

Please leave here any comments you may have regarding the research goals or the survey.

If you wish to be contacted for clarifications, you may leave your email address here.

« Back

Submit

Appendix C

Results of the Survey

This appendix presents the results to the question: “Please indicate how strong you consider the influence of the following characteristics on the security level”.

Table C.1: User’s Risk Perception

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 1 | 7% |
| Medium influence | 4 | 27% |
| Strong influence | 10 | 67% |

Table C.2: User’s Trust

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 2 | 13% |
| Medium influence | 2 | 13% |
| Strong influence | 11 | 73% |

Table C.3: User’s Exposure to Security (for example through media)

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 3 | 20% |
| Medium influence | 6 | 40% |
| Strong influence | 6 | 40% |

Table C.4: User's Theoretical Knowledge in Using Computers or/and in Security

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 5 | 33% |
| Medium influence | 7 | 47% |
| Strong influence | 3 | 20% |

Table C.5: User's Experience in Using Computers or/and in Security

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 0 | 0% |
| Medium influence | 13 | 87% |
| Strong influence | 2 | 13% |

Table C.6: User's Gender

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 11 | 73% |
| Weak influence | 3 | 20% |
| Medium influence | 1 | 7% |
| Strong influence | 0 | 0% |

Table C.7: User's Age

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 1 | 7% |
| Weak influence | 7 | 47% |
| Medium influence | 7 | 47% |
| Strong influence | 0 | 0% |

Table C.8: User's Place of Birth

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 7 | 47% |
| Weak influence | 6 | 40% |
| Medium influence | 2 | 13% |
| Strong influence | 0 | 0% |

Table C.9: User's Role (if the user is an undergraduate/graduate student, a faculty, a staff, an intern, etc...)

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 4 | 27% |
| Medium influence | 11 | 73% |
| Strong influence | 0 | 0% |

Table C.10: Security Awareness Communication to Users

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 3 | 20% |
| Medium influence | 9 | 60% |
| Strong influence | 3 | 20% |

Table C.11: Management Understanding of Security Needs

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 0 | 0% |
| Medium influence | 3 | 20% |
| Strong influence | 12 | 80% |

Table C.12: Security Team Talent

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 1 | 7% |
| Medium influence | 4 | 27% |
| Strong influence | 10 | 67% |

Table C.13: Security Team Qualities (for example withstanding stress)

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 1 | 7% |
| Medium influence | 9 | 60% |
| Strong influence | 5 | 33% |

Table C.14: Financial Resources Available for Security

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 1 | 7% |
| Medium influence | 10 | 67% |
| Strong influence | 4 | 27% |

Table C.15: Available Security Hardware (for example security devices such as intrusion prevention systems)

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 1 | 7% |
| Medium influence | 9 | 60% |
| Strong influence | 5 | 33% |

Table C.16: Available Security Software (for example patches, signatures)

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 1 | 7% |
| Medium influence | 7 | 47% |
| Strong influence | 7 | 47% |

Table C.17: Risk Assessment Program

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 1 | 7% |
| Medium influence | 8 | 53% |
| Strong influence | 6 | 40% |

Table C.18: Security Policies

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 2 | 13% |
| Medium influence | 6 | 40% |
| Strong influence | 7 | 47% |

Table C.19: Organizational Attitude towards Security

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 0 | 0% |
| Medium influence | 2 | 13% |
| Strong influence | 13 | 87% |

Table C.20: Threat Awareness

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 1 | 7% |
| Medium influence | 7 | 47% |
| Strong influence | 7 | 47% |

Table C.21: Attacker's Motivations

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 1 | 7% |
| Medium influence | 6 | 40% |
| Strong influence | 8 | 53% |

Table C.22: Attacker's Expertise

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 2 | 13% |
| Medium influence | 6 | 40% |
| Strong influence | 7 | 47% |

Table C.23: Attacker's Qualities (for example perseverance)

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 0 | 0% |
| Medium influence | 6 | 40% |
| Strong influence | 9 | 60% |

Table C.24: Value of the Asset from the Attacker's Point of View

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 0 | 0% |
| Medium influence | 8 | 53% |
| Strong influence | 7 | 47% |

Table C.25: Value of the Asset from the Organization's Point of View

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 1 | 7% |
| Medium influence | 8 | 53% |
| Strong influence | 6 | 40% |

Table C.26: Depth of Protection of the Asset (includes all protections of an asset - passwords, firewalls...)

| Type of influence | Number responses | Percentage |
|-------------------|------------------|------------|
| No influence | 0 | 0% |
| Weak influence | 0 | 0% |
| Medium influence | 7 | 47% |
| Strong influence | 8 | 53% |

Appendix D

Propagating Values in the Model

In this appendix, we present the technique used to propagate values of characteristics in the model, based on the type and strength of the influence. The technique used is a simple one but other techniques such as fuzzy logic or Bayesian Belief Networks could have been used to propagate values.

D.1 Method

If a child node C has n parent nodes of influence of type positive or negative and of strength s_i (strong, medium, or weak), as depicted in Figure D.1, and we have evidence for parent nodes, the value v_C of the child node is calculated based on the following simple equation:

$$v_C = \frac{\sum_{i=1}^n s_i * v_i}{\sum_{i=1}^n s_i} \quad (\text{D.1})$$

Each variable is defined as follows:

- s_i is the strength of the influence of parent i on child node C : It is equal to 1, 2, or 3 if the influence is weak, medium, or strong respectively,
- v_i is the value of parent i : If the parent node has a positive influence on C , it is equal to 1, 2, and 3 if the value of the node is low, medium, and strong respectively. If the parent node has a negative influence on C , the values 1, 2, and 3 are assigned to high, medium, and low respectively (reverse order).

Indeed, if a node has a positive influence on a node, and the parent node is high (respectively low), then the child node is more likely to be high (respectively low). On the contrary, if a node has a negative influence on another node, and the parent node is high (respectively low), the child node is more likely to be low (respectively high).

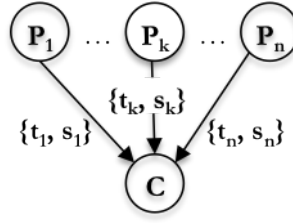


Figure D.1: Child Node with n Parent Nodes - Each parent P_k has an influence of type t_k and of strength s_k on child node C .

Once a value v_C is determined, thresholds are set to decide what values of v_C are low, medium, or strong. These thresholds may vary from one analyst to another.

We chose the following thresholds:

- If $v_c \leq 1.5$, then child node C has a low value,
- If $1.5 < v_c < 2.5$, then child node C has a medium value,
- If $2.5 \leq v_c$, then child node C has a high value.

This technique was verified for the case of two parent nodes. Each combination of strength of influence (strong, medium, or weak influence), type of influence (positive, or negative), and value of the parent nodes (high, medium, or low value), was checked for inconsistency. For example, in the case of two nodes positively impacting a child node (irrespectively from the strength of the influence), if parent

nodes are high, the child node should be high. In the case where the strength of the influence of both parent nodes on the child node are similar, if one of the parent node is high and the other one is low, the child node should be medium. However, if one parent is high and the other one is medium, it may be unclear for an analyst whether the child node should be high or medium. In this case, the described technique allows discriminating between a medium and a high value. This value is flexible and can be changed according to the analyst by modifying the thresholds.

D.2 Examples

D.2.1 Example 1: Two Parent Nodes

In this example, we consider two parent nodes P_1 and P_2 influencing node C with a medium positive influence (Figure D.2). Values of C are derived from values of P_1 and P_2 and are shown in Table D.1. We show in parenthesis the computed value v_C based on values of A and B , with $s_{P_1} = s_{P_2} = 2$.

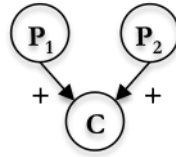


Figure D.2: Example of Two Parent Nodes

From Table D.1, the highest (respectively lowest) value of C is obtained when both parents are high (respectively low). When both parents are medium, the child node is medium. When one parent is low and the other one is high, the child node is medium. These results match the intuition one may have when thinking about the qualitative values only. However, in the two cases where 1) one of the

Table D.1: Values of the Child Node C based on Values of its Two Parents P_1 and P_2 in Example 1

| Value of P_1 | Value of P_2 | Value of C |
|----------------|----------------|------------|
| High | High | High (3) |
| High | Medium | High (2.5) |
| High | Low | Medium (2) |
| Medium | High | High (2.5) |
| Medium | Medium | Medium(2) |
| Medium | Low | Low (1.5) |
| Low | High | Medium (2) |
| Low | Medium | Low (1.5) |
| Low | Low | Low (1) |

parent is low and the other one is medium, and 2) one of the parent is medium and the other one is high, it may be unclear to determine the value of the child node with qualitative thinking. This technique is deterministic by nature through the thresholds: a quantitative value of 1.5 for the child node falls into a low domain while a quantitative value of 2.5 falls into the high domain. These thresholds can be refined by the analyst.

D.2.2 Example 2: Three Parent Nodes

In this subsection, we present the case of a node with three parent nodes. In the model, “Security” has three parent nodes (Figure D.3):

- “Attacker’s Motivations” have a medium negative impact on “Security”,
- “Attacker’s Resources” have a strong negative impact on “Security”,
- “Depth of Protection of the Asset” have a strong positive impact on “Security”.

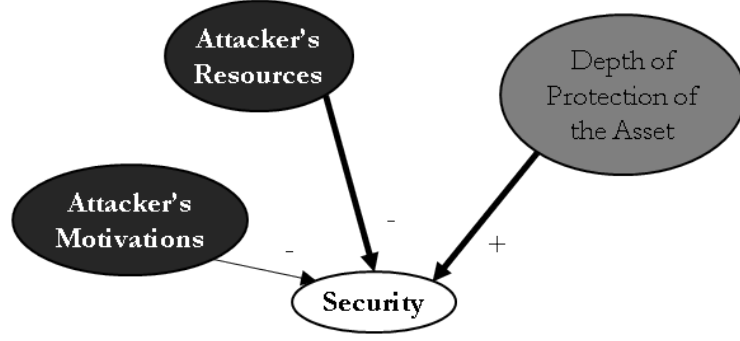


Figure D.3: Example of Three Parent Nodes

The value of “Security” depends on values of its three parent nodes, as shown in Table D.2. In this example, “Depth of Protection of the Asset” has three possible values (high, medium, or low) whereas “Attacker’s Motivations” and “Attacker’s Resources” have two possible values (high or low). For the last two characteristics, $v_i = 1$ if characteristic i is low, and $v_i = 3$ if characteristic i is high.

Table D.2: Value of Security given Values of its Three Parent Nodes

| Depth of Protection of the Asset | Attacker's Resources | Attacker's Motivations | Security |
|----------------------------------|----------------------|------------------------|----------------|
| High | High | High | Medium (1.75) |
| High | High | Low | Medium (2.25) |
| High | Low | High | High (2.5) |
| High | Low | Low | High (3) |
| Medium | High | High | Low (1.375) |
| Medium | High | Low | Medium (1.875) |
| Medium | Low | High | Medium (2.125) |
| Medium | Low | Low | High (2.625) |
| Low | High | High | Low (1) |
| Low | High | Low | Low (1.5) |
| Low | Low | High | Medium (1.75) |
| Low | Low | Low | Medium (2.25) |

As expected, the case where “Depth of Protection of the Asset” is high and the attacker-related nodes are low leads to the highest level of security among the pos-

sible cases. Similarly, the case where the “Depth of Protection of the Asset” is low and the other two nodes are high leads to the lowest level of security: this case represents when assets are not well protected and when attackers are highly motivated and have many resources available (e.g. knowledge, hardware, and software).

D.2.3 Example 3: Four Parent Nodes

This subsection details the propagation of evidence set in the example depicted in Section 7.8.1. We assume a high value of “Security Team Expertise and Qualities” and a medium value for “Security Awareness Communication” (Figure D.4).

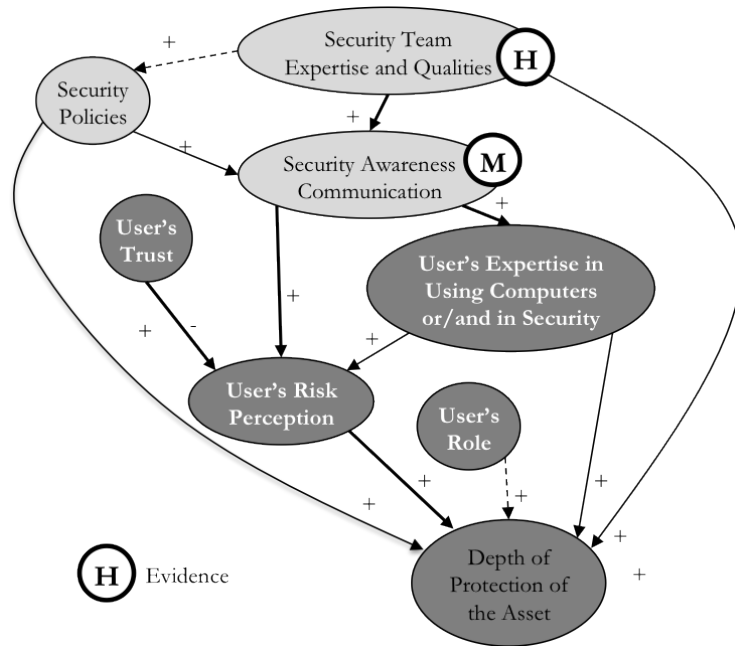


Figure D.4: Example of Two Sets of Evidence - H, M, and L stand for High, Medium, and Low

The high value of the “Security Team Expertise and Qualities” transfer to “Security Policies” while “User’s Expertise in Using Computers or/and in Security” takes the medium value of the “Security Awareness Communication”. On the other hand, “User’s Risk Perception” is influenced by the medium values of “Security

Awareness Communication” and “User’s Expertise in Using Computers or/and in Security”. Therefore, “Depth of Protection of the Asset” has four parent nodes, which values and strength of influence are depicted in Figure D.5 and summarized in Table D.3. In this situation, the value v_c of “Depth of Protection of the Asset” is 2.44 and is therefore medium.

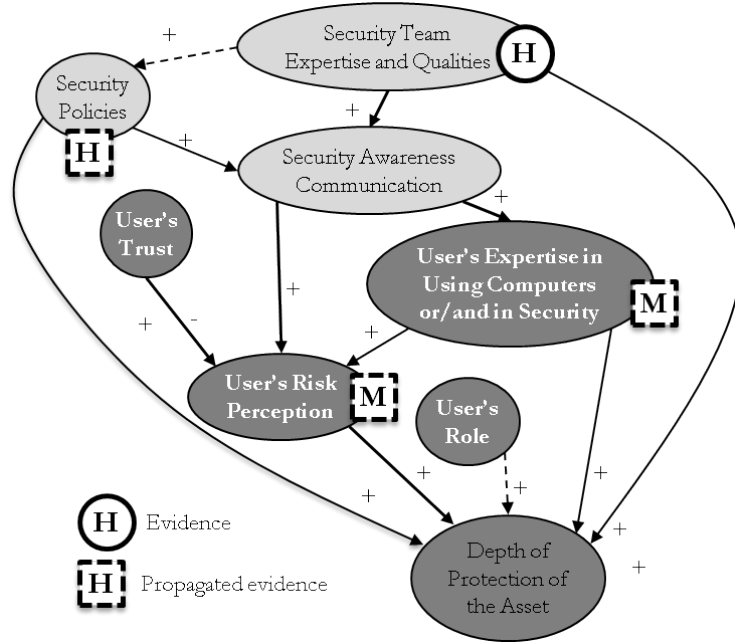


Figure D.5: Example of Four Parent Nodes - H, M, and L stand for High, Medium, and Low

Table D.3: Value of “Depth of Protection of the Asset” based on Values of its Four Parents

| Characteristic | Strength of the influence | Value |
|--|---------------------------|---------------|
| Security policies | Medium (2) | High (3) |
| User’s risk perception | Strong (3) | Medium (2) |
| User’s expertise in using computers or/and in security | Medium (2) | Medium (2) |
| Security team expertise and qualities | Medium (2) | High (3) |
| Depth of protection of the asset | - | Medium (2.44) |

D.2.4 Example 4: Five Parent Nodes

This section explains the propagation of the example depicted in Section 7.8.4 where we have the following pieces of evidence (Figure D.6):

- Low value for the “Value of the Asset from the Organization’s Point of View”,
- High value for the “Security Team Expertise and Qualities”,
- Medium value for the “Security Awareness Communication”.

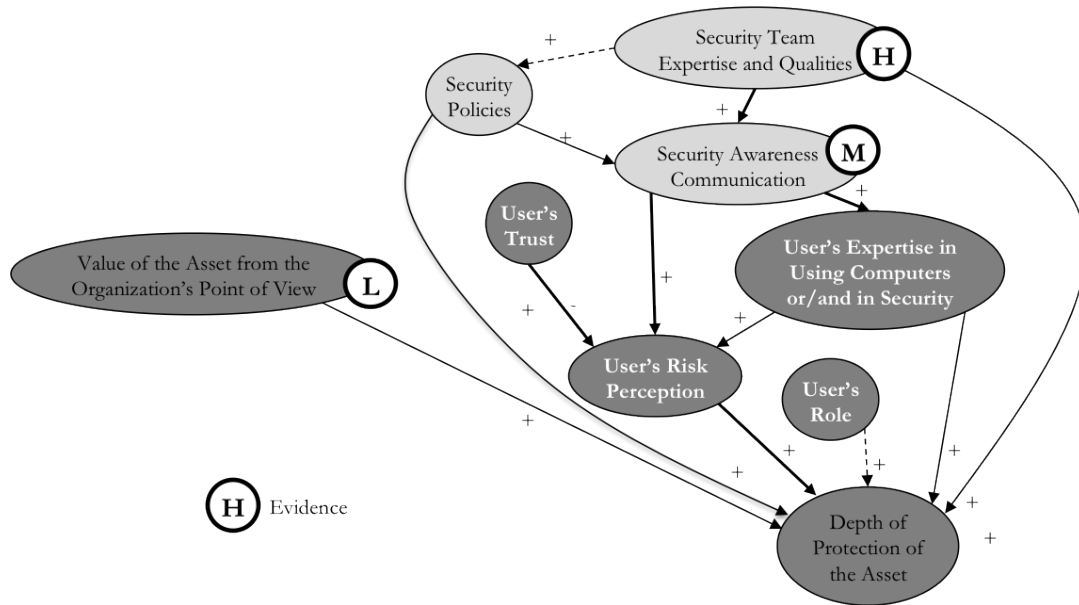


Figure D.6: Example of Three Sets of Evidence - H, M, and L stand for High, Medium, and Low

On the one hand, “Security Policies” have a high value due to its only parent “Security Team Expertise and Qualities”. On the other hand, the medium value of “Security Awareness Communication” propagates to the “User’s Expertise in Using Computers or/and in Security”. “User’s Risk Perception is impacted by a medium value from “Security Awareness Communication and a medium value of “User’s

Risk Perception”, hence it has a medium value. Therefore, “Depth of Protection of the Asset” has five parent nodes with the set and propagated evidence shown in Figure D.7. The evidence used to calculate the value v_C of “Depth of Protection of the Asset” is provided in Table D.4. Based on the three aforementioned pieces of evidence, the value of the “Depth of Protection of the Asset” is medium.

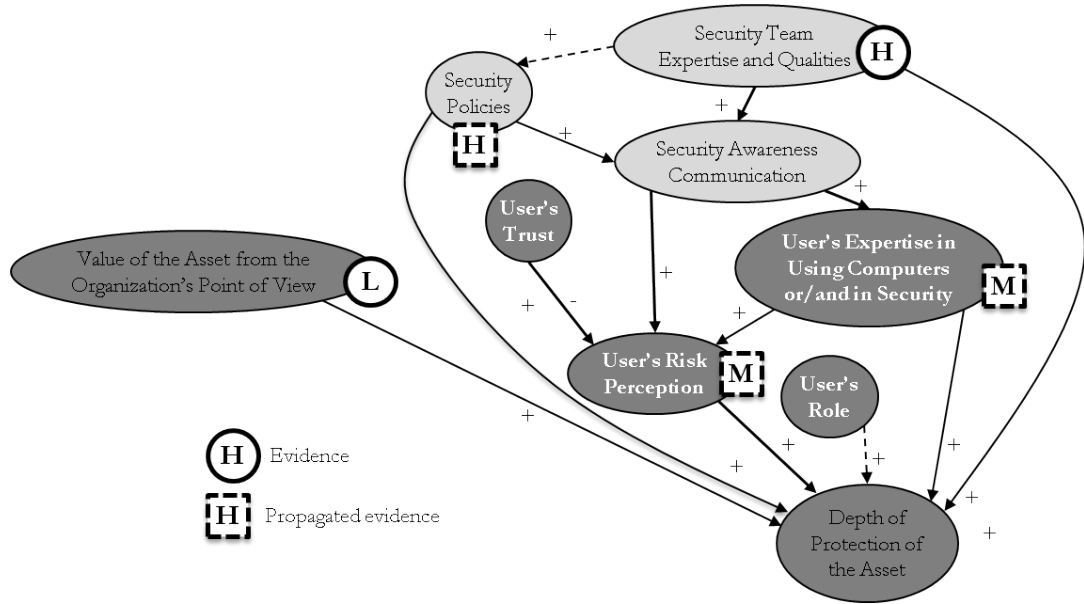


Figure D.7: Example of Five Parent Nodes - H, M, and L stand for High, Medium, and Low

Table D.4: Value of “Depth of Protection of the Asset” based on Values of its Five Parents

| Characteristic | Strength of the influence | Value |
|--|---------------------------|---------------|
| Value of the asset from the organization’s point of view | Medium (2) | Low (1) |
| Security policies | Medium (2) | High (3) |
| User’s risk perception | Strong (3) | Medium (2) |
| User’s expertise in using computers or/and in security | Medium (2) | Medium (2) |
| Security team expertise and qualities | Medium (2) | High (3) |
| Depth of protection of the asset | - | Medium (2.18) |

Bibliography

- [1] 4chan-based group Anonymous targets PayPal to support WikiLeaks. <http://www.digitaltrends.com/computing/4chan-based-group-anonymous-targets-paypal-to-support-wikileaks/>. [Online] Last accessed March 29, 2011.
- [2] EDUCAUSE Main Page. <http://www.educause.edu/>. [Online] Last accessed March 29, 2011.
- [3] National vulnerability database. <http://web.nvd.nist.gov/view/vuln/search-results?cid=2>. [Online] Last accessed March 29, 2011.
- [4] Predict - protected repository for the defense of infrastructure against cyber threats. <https://www.predict.org>. [Online] Last accessed March 29, 2011.
- [5] SANS Training and your Career Roadmap. <http://www.sans.org/security-training/roadmap.pdf>. [Online] Last accessed March 29, 2011.
- [6] University of california office of information technology - netbios blocked from uci's network. <http://www.nacs.uci.edu/security/netbios.html>. [Online] Last accessed March 29, 2011.
- [7] EBay, Amazon, Buy.com Hit by Attacks. <http://www.networkworld.com/news/2000/0209attack.html>, 2000. [Online] Last accessed March 29, 2011.
- [8] Yahoo outage raises web concerns. <http://www.networkworld.com/news/2000/0209yahoo2.html>, 2000. [Online] Last accessed March 29, 2011.
- [9] UC Berkeley Breach Affects 160,000. <http://www.databreaches.net/?p=3821>, 2009. [Online] Last accessed March 29, 2011.
- [10] Cyberattack on Google Said to Hit Password System. <http://www.nytimes.com/2010/04/20/technology/20google.html>, 2010. [Online] Last accessed March 29, 2011.
- [11] Official Google Blog: A New Approach to China. <http://googleblog.blogspot.com/2010/01/new-approach-to-china.html>, 2010. [Online] Last accessed March 29, 2011.
- [12] JO Aagedal, F. den Braber, T. Dimitrakos, B.A. Gran, D. Raptis, and K. Stolen. Model-based Risk Assessment to Improve Enterprise Security. In *Enterprise Distributed Object Computing Conference, 2002. EDOC'02. Proceedings. Sixth International*, pages 51–62. IEEE, 2002.
- [13] C. Alberts, A. Dorofee, J. Stevens, and C. Woody. Introduction to the OCTAVE Approach. *Pittsburgh, PA, Carnegie Mellon University*, 2003.

- [14] D. Andrews, B. Nonnecke, and J. Preece. Conducting Research on the Internet: Online Survey Design, Development and Implementation Guidelines. 2007.
- [15] B. Arief and D. Besnard. Technical and human issues in computer-based systems security. *Technical Report Series - University of Newcastle upon Tyne Computing Science*, 2003.
- [16] R.H. Ashton. Combining the Judgments of Experts: How Many and Which Ones? *Organizational Behavior and Human Decision Processes*, 38(3):405–414, 1986.
- [17] O. Balci. How to assess the acceptability and credibility of simulation results. In *Proceedings of the 21st conference on Winter simulation*, pages 62–71. ACM, 1989.
- [18] O. Balci. Verification, validation, and testing. *Handbook of simulation: principles, methodology, advances, applications, and practice*, pages 335–393, 1998.
- [19] R. Batchelor and P. Dua. Forecaster Diversity and the Benefits of Combining Forecasts. *Management Science*, 41(1):68–75, 1995.
- [20] P.E. Black, K. Scarfone, and M. Souppaya. Cyber Security Metrics and Measures. 2008.
- [21] D.J. Bodeau, R. Graubart, and J. Fabius-Greene. Improving Cyber Security and Mission Assurance via Cyber Preparedness (Cyber Prep) Levels, 2009.
- [22] L.D. Bodin, L.A. Gordon, and M.P. Loeb. Evaluating Information Security Investments Using the Analytic Hierarchy Process. *Communications of the ACM*, 48(2):78–83, 2005.
- [23] R.M. Bowen, R.P. Castanias, and L.A. Daley. Intra-Industry Effects of the Accident at Three Mile Island. *Journal of Financial and Quantitative Analysis*, 18(01):87–111, 1983.
- [24] N.M. Bradburn, S. Sudman, and B. Wansink. *Asking Questions: The Definitive Guide to Questionnaire Design: For Market Research, Political Polls, and Social and Health Questionnaires*. Jossey-Bass Inc Pub, 2004.
- [25] L.C. Briand, K. El Emam, and F. Bomarius. COBRA: A Hybrid Method for Software Cost Estimation, Benchmarking, and Risk Assessment. In *Software Engineering, 1998. Proceedings of the 1998 International Conference on*, pages 390–399. IEEE, 2002.
- [26] C. Brodie and R. Wanner. The Importance of Security Awareness Training. Technical report, SysAdmin, Audit, Network, Security Institute, 2008.

- [27] W.K. Brothby. *Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement*. CRC Press, 2009.
- [28] B.B. Brown. Delphi process: A Methodology used for the Elicitation of Opinions of Experts. *Santa Monica, CA, Rand Corporation*, 1968.
- [29] K.M. Carley. Validating computational models. *Paper available at <http://www.casos.cs.cmu.edu/publications/papers.php>*, 1996.
- [30] H. Cavusoglu, B. Mishra, and S. Raghunathan. A Model for Evaluating IT Security Investments. *Communications of the ACM*, 47(7):87–92, 2004.
- [31] H. Cavusoglu, B. Mishra, and S. Raghunathan. The Value of Intrusion Detection Systems in Information Technology Security Architecture. *Information Systems Research*, 16(1):28–46, 2005.
- [32] H. Cavusoglu, S. Raghunathan, and W.T. Yue. Decision-Theoretic and Game-Theoretic Approaches to IT Security Investment. *Journal of Management Information Systems*, 25(2):281–304, 2008.
- [33] D. Chrun, M. Cukier, and G. Sneeringer. Finding Corrupted Computers Using Imperfect Intrusion Prevention System Event Data. In *Computer safety, reliability, and security: 27th international conference, SAFECOMP 2008, Newcastle on Tyne, UK, September 22-25, 2008: proceedings*, page 221. Springer-Verlag New York Inc, 2008.
- [34] D. Chrun, M. Cukier, and G. Sneeringer. On the Use of Security Metrics Based on Intrusion Prevention System Event Data: An Empirical Analysis. In *High Assurance Systems Engineering Symposium, 2008. HASE 2008. 11th IEEE*, pages 49–58. IEEE, 2008.
- [35] Corporate Information Security Working Group (CISWG). Report of the Best Practices and Metrics Teams. 2005.
- [36] E. Condon, M. Cukier, and T. He. Applying Software Reliability Models on Security Incidents. In *Software Reliability, 2007. ISSRE'07. The 18th IEEE International Symposium on*, pages 159–168. IEEE, 2007.
- [37] M. Cremonini and P. Martini. Evaluating Information Security Investments from Attackers Perspective: The Return-on-Attack (ROA). In *Fourth Workshop on the Economics of Information Security*. Citeseer, 2005.
- [38] A. Da Veiga and JHP Eloff. A Framework and Assessment Instrument for Information Security Culture. *Computers & Security*, 29(2):196–207, 2010.
- [39] R. Dantu, K. Loper, and P. Kolan. Risk management using behavior based attack graphs. In *Information Technology: Coding and Computing, 2004. Proceedings. ITCC 2004. International Conference on*, volume 1, pages 445–449. IEEE, 2005.

- [40] F.D. Davis. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS quarterly*, 13(3):319–340, 1989.
- [41] F.D. Davis. User acceptance of information technology: system characteristics, user perceptions and behavioral impacts. *International journal of man-machine studies*, 38(3):475–487, 1993.
- [42] Adam Dodge. Educational Security Incidents (ESI) Year in Review - 2009. http://www.adamdodge.com/esi/files/esi_yir_2009.pdf, 2009. [Online] Last accessed March 29, 2011.
- [43] D.P. Duggan and J.T. Michalski. Threat Analysis Framework. Technical report, Sandia National Laboratories, 2007.
- [44] A. Ekelhart, S. Fenz, M. Klemen, and E. Weippl. Security Ontologies: Improving Quantitative Risk Analysis. 2007.
- [45] S. Elky. An Introduction to Information System Risk Management. *SANS Institute*, 16, 2006.
- [46] S. Evans, D. Heinbuch, E. Kyle, J. Piorkowski, and J. Wallner. Risk-based Systems Security Engineering: Stopping Attacks with Intention. *Security & Privacy, IEEE*, 2(6):59–62, 2004.
- [47] S. Evans and J. Wallner. Risk-Based Security Engineering through the Eyes of the Adversary. In *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC*, pages 158–165. IEEE, 2005.
- [48] C. Falk. Ethics and Hacking: The General and the Specific. *Norwich University Journal of Information Assurance*, 1(1), 2005.
- [49] S. Fenz and A. Ekelhart. Verification, Validation, And Evaluation In Information Security Risk Management. *IEEE Security and Privacy*, 2010.
- [50] Y. Forrester. The Quality of Expert Judgment: An Interdisciplinary Investigation. 2005.
- [51] G.G. Gable. Integrating Case Study and Survey Research Methods: An Example in Information Systems. *European Journal of Information Systems*, 3(2):112–126, 2010.
- [52] S.I. Gass. Decision-aiding models: validation, assessment, and related issues for policy analysis. *Operations Research*, 31(4):603–631, 1983.
- [53] D. Geer Jr, KS Hoo, and A. Jaquith. Information Security: Why the Future Belongs to the Quants. *Security & Privacy, IEEE*, 1(4):24–32, 2003.
- [54] R. Gibson. Who’s really in your top 8: network security in the age of social networking. In *Proceedings of the 35th annual ACM SIGUCCS fall conference*, pages 131–134. ACM, 2007.

- [55] D. Gollman. *Computer Security*. Wiley, 1999.
- [56] J. Gonzalez, J. Sarriegi, and A. Gurrutxaga. A Framework for Conceptualizing Social Engineering Attacks. *Critical Information Infrastructures Security*, pages 79–90, 2006.
- [57] L.A. Gordon and M.P. Loeb. The Economics of Information Security Investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):438–457, 2002.
- [58] L.A. Gordon and M.P. Loeb. *Managing cybersecurity resources: A cost-benefit analysis*. McGraw-Hill, 2006.
- [59] K. Goseva-Popstojanova, K. Vaidyanathan, K. Trivedi, F. Wang, R. Wang, F. Gong, and B. Muthusamy. Characterizing intrusion tolerant systems using a state transition model. In *dissec*, page 1211. Published by the IEEE Computer Society, 2001.
- [60] G. Greene. Assessing the Impact of Security Culture and the Employee-Organization Relationship on IS Security Compliance. In *5th Annual Symposium on Information Assurance (ASIA10)*, page 1, 2010.
- [61] K.M. Groth. A Data-Informed Model of Performance Shaping Factors for Use in Human Reliability Analysis. 2009.
- [62] R.M. Groves, F.J. Fowler, M.P. Couper, J.M. Lepkowski, E. Singer, and R. Tourangeau. *Survey Methodology*. John Wiley & Sons Inc, 2009.
- [63] F. Hasson, S. Keeney, and H. McKenna. Research Guidelines for the Delphi Survey Technique. *Journal of Advanced Nursing*, 32(4):1008–1015, 2000.
- [64] J. Hitchings. Deficiencies of the traditional approach to information security and the requirements for a new methodology* 1. *Computers & Security*, 14(5):377–383, 1995.
- [65] K.J.S. Hoo. *How much is enough? A risk management approach to computer security*. Citeseer, 2000.
- [66] S.H. Houmb. Decision Support for Choice of Security Solution: The Aspect-Oriented Risk Driven Development (AORDD) Framework. 2007.
- [67] R.A. Howard and J.E. Matheson. Influence Diagrams. *Decision Analysis*, 2(3):127–143, 2005.
- [68] A. Jaquith. *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Addison-Wesley Professional, 2007.
- [69] E. Jonsson and T. Olovsson. A Quantitative Model of the Security Intrusion Process based on Attacker Behavior. *Software Engineering, IEEE Transactions on*, 23(4):235–245, 2002.

- [70] K. Kanoun, M.R. de Bastos Martini, and J.M. de Souza. A Method for Software Reliability Analysis and Prediction Application to the TROPICO-R Switching System. *IEEE Transactions on Software Engineering*, pages 334–344, 1991.
- [71] J.P.C. Kleijnen. Validation of models: statistical techniques and data availability. In *Winter Simulation Conference Proceedings*, volume 1, pages 647–654, 1999.
- [72] A.G. Kotulic and J.G. Clark. Why There Aren’t More Information Security Research Studies. *Information & Management*, 41(5):597–607, 2004.
- [73] HA Kruger and WD Kearney. A Prototype for Assessing Information Security Awareness. *Computers & Security*, 25(4):289–296, 2006.
- [74] A.M. Law. How to build valid and credible simulation models. In *Proceedings of the 37th conference on Winter simulation*, pages 24–32. Winter Simulation Conference, 2005.
- [75] E. LeMay, W. Unkenholz, D. Parks, C. Muehrcke, K. Keefe, and W.H. Sanders. Adversary-Driven State-Based System Security Evaluation. In *Proceedings of the 6th International Workshop on Security Measurements and Metrics*, pages 1–9. ACM, 2010.
- [76] T. Levine and S. Donitsa-Schmidt. Computer use, confidence, attitudes, and knowledge: A causal analysis. *Computers in Human Behavior*, 14(1):125–146, 1998.
- [77] B. Littlewood, S. Brocklehurst, N.E. Fenton, P. Mellor, S. Page, D. Wright, J. Dobson, J. McDermid, and D. Gollmann. Towards Operational Measures of Computer Security. *Journal of Computer Security*, 2(2-3):211–230, 1993.
- [78] J. Lowry. An initial foray into understanding adversary planning and courses of action. In *DARPA Information Survivability Conference & Exposition II, 2001. DISCEX’01. Proceedings*, volume 1, pages 123–133. IEEE, 2002.
- [79] Q. Ma and J.M. Pearson. ISO 17799: “Best Practices” in Information Security Management? *Communications of the Association for Information Systems*, 15(1):32, 2005.
- [80] B.B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan, and K.S. Trivedi. Modeling and Quantification of Security Attributes of Software Systems. In *Proceedings of the 2002 International Conference on Dependable Systems and Networks*, pages 505–514. IEEE Computer Society, 2002.
- [81] A. Martins. Information Security Culture. In *Security in the Information Society: Visions and Perspectives: IFIP TC11 17th International Conference on Information Security (SEC2002), May 7-9, 2002, Cairo, Egypt*, page 203. Springer Netherlands, 2002.

- [82] V.W. Mitchell. Organizational risk perception and reduction: A literature review. *British Journal of Management*, 6(2):115–133, 1995.
- [83] K.D. Mitnick and W.L. Simon. *The art of deception: Controlling the human element of security*. John Wiley & Sons, Inc. New York, NY, USA, 2003.
- [84] A. Mosleh and G. Bier. A Critique of Current Practice for the Use of Expert Opinions in Probabilistic Risk Assessment. *Reliability Engineering & System Safety*, 20(1):63–85, 1988.
- [85] E.A. Nichols and A. Sudbury. Implementing Security Metrics Initiatives. *ED-PACS*, 34(3):10–20, 2006.
- [86] W.J. Nistir, W. Jansen, and P.D. Gallagher. Directions in Security Metrics Research. 2009.
- [87] R.M. O’Keefe, O. Baici, and E.P. Smith. Validation of expert system performance. *IEEE expert*, 2:81–90, 1987.
- [88] R. Ortalo, Y. Deswarte, and M. Kaâniche. Experimenting with quantitative evaluation tools for monitoring operational security. *Software Engineering, IEEE Transactions on*, 25(5):633–650, 2002.
- [89] C. Peake. Red Teaming: The Art of Ethical Hacking. *SANS Institute*, 2003.
- [90] T.R. Peltier. *Information Security Risk Analysis*. CRC press, 2005.
- [91] C.P. Pfleeger and S.L. Pfleeger. *Security in Computing*. Prentice Hall, 2003.
- [92] F. Rambach. Taxonomies of Attackers. 2003.
- [93] D. Ramsbrock, R. Berthier, and M. Cukier. Profiling Attacker Behavior following SSH Compromises. 2007.
- [94] L. Raymond. Organizational Context and Information Systems Success: A Contingency Approach. *Journal of Management Information Systems*, pages 5–20, 1990.
- [95] S.N. Rosenfeld, I. Rus, and M. Cukier. Archetypal behavior in computer security. *Journal of Systems and Software*, 80(10):1594–1606, 2007.
- [96] M. Rounds and N. Pendgraft. Diversity in Network Attacker Motivation: A Literature Review. In *2009 International Conference on Computational Science and Engineering*, pages 319–323. IEEE, 2009.
- [97] R. Saint-Germain. Information security management best practice based on ISO/IEC 17799. *Information Management Journal*, 39(4):60–66, 2005.
- [98] R.G. Sargent. Verification and Validation of Simulation Models. In *Proceedings of the 37th conference on Winter simulation*, pages 130–143. Winter Simulation Conference, 2005.

- [99] M.A. Sasse, S. Brostoff, and D. Weirich. Transforming the Weakest Link A Human Computer Interaction Approach to Usable and Effective Security. *BT technology journal*, 19(3):122–131, 2001.
- [100] S.E. Schechter. *Computer security strength & risk: A quantitative approach*. PhD thesis, Citeseer, 2004.
- [101] T. Schlienger and S. Teufel. Information Security Culture - From Analysis to Change. *South African Computer Journal*, pages 46–52, 2003.
- [102] B. Schneier. *Secrets & lies: Digital Security in a Networked World*. John Wiley & Sons, Inc. New York, NY, USA, 2000.
- [103] W.R. Scott. *Organizations: Rational, Natural, and Open Systems*. Prentice hall Upper Saddle River, NJ, 1998.
- [104] C.H. Shirazi. *Data-Informed Calibration and Aggregation of Expert Judgment in a Bayesian Framework*. PhD thesis, 2009.
- [105] M. Siegrist and G. Cvetkovich. Perception of hazards: The role of social trust and knowledge. *Risk analysis*, 20(5):713–720, 2000.
- [106] L. Sjoberg, B. Moen, and T. Rundmo. Explaining risk perception. *An evaluation of the psychometric paradigm in risk perception research*, 2004.
- [107] W. Sonnenreich, J. Albanese, and B. Stout. Return On Security Investment (ROSI)-A Practical Quantitative Model. *Journal of Research and Practice in Information Technology*, 38(1):45–56, 2006.
- [108] F. Stevens, T. Courtney, S. Singh, A. Agbaria, JR Meyer, W.H. Sanders, and P. Pal. Model-based validation of an intrusion-tolerant information system. In *Reliable Distributed Systems, 2004. Proceedings of the 23rd IEEE International Symposium on*, pages 184–194. IEEE, 2004.
- [109] G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology systems. *Nist special publication*, 800:30, 2002.
- [110] SurveyMonkey. Smart Survey Design. <http://s3.amazonaws.com/SurveyMonkeyFiles/SmartSurvey.pdf>. [Online] Last accessed March 29, 2011.
- [111] M. Sutter and M.G. Kocher. Age and the development of trust and reciprocity. *Papers on Strategic Interaction*, 2004.
- [112] M. Swanson. Security Self-Assessment Guide for Information Technology Systems. *NIST Special Publication*, 800:26.

- [113] M. Swanson, National Institute of Standards, and Technology (US). *Security Metrics Guide for Information Technology Systems*. US Dept. of Commerce, National Institute of Standards and Technology, 2003.
- [114] D. Tan. Quantitative Risk Analysis Step-By-Step. *SANS Institute*, 2002.
- [115] C.F. Tsang. The modeling process and model validation. *Ground Water*, 29(6):825–831, 1991.
- [116] T. Tsiakis and G. Stephanides. The Economic Approach of Information Security. *Computers & security*, 24(2):105–108, 2005.
- [117] A.P. Verhagen, H.C.W. de Vet, R.A. de Bie, A.G.H. Kessels, M. Boers, L.M. Bouter, and P.G. Knipschild. The Delphi List: A Criteria List for Quality Assessment of Randomized Clinical Trials for Conducting Systematic Reviews Developed by Delphi Consensus. *Journal of clinical epidemiology*, 51(12):1235–1241, 1998.
- [118] V. Visintine. An Introduction to Information Risk Assessment. *SANS institute*, 8, 2003.
- [119] B.D. Voss. The Ultimate Defense of Depth: Security Awareness in your Company. *SANS Institute White Paper*, SANS Institute, Bethesda, MD, 2001.
- [120] A.J.A. Wang. Information Security Models and Metrics. In *Proceedings of the 43rd Annual Southeast Regional Conference*, volume 2, pages 178–184. ACM, 2005.
- [121] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia. An Attack Graph-Based Probabilistic Security Metric. *Data and Applications Security XXII*, pages 283–296, 2008.
- [122] B. Whiteman. Network Risk Assessment Tool. *IAnewsletter*, 11(1):4–8, 2002.
- [123] L. Williams, R. Lippmann, and K. Ingols. GARNET: A Graphical Attack Graph and Reachability Network Evaluation Tool. *Visualization for Computer Security*, pages 44–59, 2008.
- [124] L. Woodard, C.K. Veitch, S.R. Thomas, and D.P. Duggan. Categorizing Threat: Building and Using a Generic Threat Matrix. Technical report, Sandia National Laboratories, 2007.
- [125] I. Yaniv. The Benefit of Additional Opinions. *Current Directions in Psychological Science*, 13(2):75, 2004.
- [126] J. Yuill, S.F. Wu, F. Gong, and M.Y. Huang. Intrusion detection for an on-going attack. In *Recent Advances in Intrusion Detection-RAID*, volume 99. Citeseer, 1999.