Evaluating IT security performance with quantifiable metrics

ERKAN KAHRAMAN

DSV SU/KTH
Institutionen för Data- och Systemvetenskap

Abstract

The growing attention of organizations' towards information security raised from the need for protection of their most valuable assets and companies started to invest more on information security. But security, as it has always been, still is seen as a cost center since the return on security investments (including the budget, hiring professionals, education programs) could not be calculated effectively.

As said, "An activity can not be managed, if it can not be measured." IT security is such an activity that is in need for a tool to be measured. This requirement is not only driven by managerial, but also financial and regulatory tools.

The goal of this master thesis is to identify the steps of IT Security Officers/Auditors to measure IT Security Performance and the adequacy of security policies and protocols by setting up a Metrics Scorecard evaluated with quantifiable metrics and so, to continuously validate the security level.

I believe, when preparing the tool, a holistic approach to system science and system theory would help to understand the security performance goals and objectives better by combining all technical, organizational and ethical assets of information systems.

From this perspective, the objective of the project is to create a vendor-free, organization-wide tool based on system theory which will help decision makers in measuring and managing security. Methods of research includes also OCTAVE technique for risk management and the project is based on previous academic works, best practices and theories that implement quantifiable efficiency, effectiveness, impact and implementation metrics for IT Security.

Acknowledgements

I would like to thank everybody that put their effort in preparation of this thesis and their continuous support during the whole project. Job A. Chaula in the first place, as my adviser for his ideas, comments and knowledge; Louise Yngstrom and the Department of System Sciences, for providing everything I needed.
Then finally, my dear family and Lukas Kunz for his idealistic motivations, who has been as close as my family to me.

Contents

List of Tables

List of Figures

Chapter 1

Introduction

With the companies' growing dependability on intangible assets in a "network economy age", importance of information technology and its protection is indisputable. From this perspective, information security is getting to have a vital role in companies' future strategies. Coping with the new technology and at the same time securing your information and communication assets is now a prior action.

While talking about managing IT security, security metrics is a must-to-perform. As William Boni, SECurity METrics (SECMET) consortium President, said *"Network security experts can't measure their success without security metrics, and what can't be measured can't be effectively managed."*[1] So what are these security metrics and how should they be applied? IT security metrics are quantifiable measurement tools to aid an organizations decision making, improve performance and raise accountability on IT system security.

At a higher level, metrics are quantifiable measurements of the aspects of a system or organization.

In an organizations networking system, for which security is an important asset, there are some identifiable (measurable) attributes that can collectively characterize the performance level of the system's security. Further, the security metrics system is a quantitative approach to measure how much does the system comply with the requirements. This security metrics can be built from lower level physical measures to the higher level managerial issues.

"Security metrics focus on the actions (and results of those actions) that organizations take to reduce and manage the risks of loss of reputation, theft of information or money, and business discontinuities that arise when

[1] William Boni, SecMet President CISO, Motorola Inc. Announcement on Security Metrics Consortium Web Page [http://www.secmet.org] at 2004-09-10

security defenses are breached. They are useful to senior management, decision makers, users, administrators, or other stakeholders who face a difficult and complex set of questions regarding security." [SSE-CMM 2003]

Using security metrics continuously over a period to evaluate a company's IT security performance, based on its performance goals; tracks implemented controls for improvement and measures efficiency of those controls. With the system thinking, measurement creates data and data creates information which will bring us knowledge and finally lead our knowledge to wisdom. With quantifiable metrics like percentages, averages or numbers, security authorities can clarify the progress in a system. As security is often seen as a cost center and it's difficult to get approval for security budgets and expenditures on software, hardware, staff, services, training, process and procedures; security metrics can give us a clear vision of return on security investments. For management, it's always better to see the change in average virus infections monthly on a system or the number of password breaches after spending money on security investments, to understand the reduced level of risk. In a way, security metrics are also tools to justify IT security investment.

Of course, the benefits are not limited with improving accountability to stakeholders and ensuring an appropriate level of mission support. Besides demonstrating compliance with regulations, laws and policies drawn by many governments or unions; understanding the level of our IT security will also help us take control of risks and manage them intelligently and proactively.

Finally, we can sum up the necessity reasons for IT security metrics as Elizabeth Lennon stated, *"IT Security Metrics provide a practical approach to measuring information security. IT Security Metrics are tools that facilitate decision making and accountability through collection, analysis and reporting of relevant performance data."*[2]

1.1 Background

According to Information Security Survey of 2002 by KPMG Consulting Inc., only 35 percent of organizations currently measure and report security performance using standardized metrics. While, at 42 percent more organizations use formal metrics for reporting on performance now, and a 17 percent plans to do so, but this still is a very small percentage. [ISS 2002]

[2]Lennon, Elizabeth B., "IT Security Metrics", NIST USA, 2004, http://www.itl.nist.gov/lab/bulletns/bltnaug03.htm

We can say that security performance measurement by using standardized metrics gained recognition during the last years with the help of guidelines, code of practices and standards accepted widely over the world with the efforts of international organizations and companies.

Code of Practice BS7799 by British Standards Institute [BS7799 1995], published in 1995, which is also modified and accepted later as ISO17799 standard has informative sectors covering introduction, scope, terms and definitions of information security [ISO/IEC 17799:2000]. ISO17799 provides a non-technical point of view to the needs of security in organizations.

Compliance is necessary for public companies as well as financial services, healthcare sector and government agencies. HIPAA (The Health Insurance Portability and Accountability Act of 1996) and corresponding regulations bind health sector in "Medical Privacy" as a national standard to protect the privacy of personal health information. Similarly, GLBA (The Gramm Leach Bliley Act) requires a higher level of security awareness in finance sector. Laws supporting the protection of the security (confidentiality, integrity and availability) of consumer information are also alike in European Union member states.

Other development standards like ITSEC, TCSEC, CTCPEC (European, North American and Canadian standards respectively) which later on transformed to Common Criteria [CCIMB 2004] etc. are also formed to have a unique pint of view and level of security among organizations. In February 24, 2004 "Security Metrics Consortium -SECMET-" was founded to define standardized quantitative security risk metrics for industry, corporate and vendor adoption by top CSO/CISOs of the sector [secmet.org].

Meanwhile, governments around the world already released laws and regulations facilitating IT security measurements. The Data Protection Directive 95/46/EC of the European Parliament and of The Council was ready by October 24th of 1995; which enforces the protection of individuals with regard of processing personal data and free movement of such data. While, in the United States of America "FISMA" The Federal Information Security Management Act of 2002 clearly stated that "Departments and agencies require to demonstrate that they are meeting applicable security requirements and to document the actual level of performance based on the results of the annual program reviews." to enforce IT security performance measurement.

To cope with the scope of this regulations, laws and standards some guidelines were published. One of the widely accepted one is National Institute of Standards and Technology's Special Publication SP 800-55 (July 2003) called "Security Metrics Guide for Information Technology Systems" which

I have also used as a baseline for my project. [NIST SP800-55] The document does not indicate the standardized quantitative metrics, but gives guidance on how to define these metrics. In this paper, I wanted to go one step further by defining actual parameters and metrics.

1.2 Problem

The challenge of defining security metrics lies on the problem that metrics must be quantifiable information (like percentage, average or even absolute numbers) for comparison, applying formulas for analysis and tracking the changes. The result from our manual collection or automated resources should be meaningful performance data and must be based on IT Security performance goals of the organization.

Metrics should also be easily obtainable and feasible to measure. But research methodology plays an important role here, not to have biased data as a result; and to cover all dimensions of IT security from organizational (people), technical and operational points of view.

Concerning these conditions, the problem is to set standardized quantitative IT security risk metrics for efficient evaluation of IT security performance.

1.3 Questions

Master thesis research implies to find answers to following questions:

- Can we measure the level of IT security performance of an organization?
- What is the level of IT Security of an organization according to quantifiable metrics?
- How does the security level of an organization change during the periods?
- What is the Return on Security Investments?

Answers of these questions will facilitate decision making and help organizations to set their future strategies.

1.4 Goal

This document seeks to compile and present Security Metrics principles and applications into an easy-to-use document for those concerned with information systems security. Implementing non-vendor-specified and industry-neutral quantitative metrics to a balanced-score-card-like document will

hopefully help organizations to have an idea about their security level. In some cases, a deeper approach may be needed as this document is industry-neutral and prepared according to common IT security goals and objectives of different sectors.

The results will indicate a certain comparable level of IT security, but this comparison is to be done within different time periods and states of an organization; not within two different organizations. Using security metrics can be valuable only if it's applied constantly over time. Because, only then we can see the effects of implemented security measurements and return on security investments.

1.5 Purpose

The purpose of this project is to create a useful tool in such an area as Security Metrics which is not very well established yet, and there are not so many tools around. I find this task extremely important as managing security, performing risk analysis, strategic decision making are important areas to protect an organizations business assets; and they all facilitated by security metrics.

Managers want to see a payback for the investments, security officials have to be able to prove how many times there has been an incident, and how fast the problem was resolved and whether these measures are getting better or worse. Using quantitative measurement criteria and techniques will help organizations to see the progress in their systems. To make it easy-to-use, a balanced-scorecard will provide usability and effectiveness.

This document, as mentioned before, is to be used by anyone concerned with information security.

1.6 Method

"To understand different points of view to the security and to address three facets of security -confidentiality, integrity and availability- what IT security evaluation criteria can do for the area and what other measurements of security there might be, a systemic-holistic approach should be used."[3]

With the perspective stated by Louise Yngstrm, I made a field research on the topic of "Security Metrics" with a systemic-holistic approach. As a system can not be adequately secured unless all interconnecting systems are

[3]Yngstrm, Louise; Systemic-Holistic Approach to IT Security, DSV - SU / KTH, Stockholm, SWEDEN 2003.

also secured, all facets of information security organizational, technical and operational security are combined and the evaluation includes all.

The three key aspects of Operationally Critical Threat, Asset And Vulnerability Evaluation (OCTAVE) are the main inspiration in this project: 'Operational Risks', 'Security Practices' and 'Technology Solutions'[OCTAVE 2003] which directed my method of approach to the problem. The structure of this research is based on evaluating IT Security metrics in four different categories, which are organizational, operational, technical and people aspects of security. Finally IT security is not only the IT department's concern; it's the entire organization's concern. Departments such as Human Resources (privacy issues, inappropriate email, internet abuse) Finance (protections of rates, financial standing, projections) Legal (privacy issues, compromise of protected data) and Physical Security (to understand fundamentals that can apply no matter what the venue)

A simple example to this, the rate of insider attacks are (although most of them are unintentional) rapidly growing so that we have to find a way to measure and avoid it. So, when measuring IT security, applying metrics to awareness, culture, standards, policies, management etc. are non-seperative parts of the holistic approach. When measuring awareness, effectiveness of education etc., surveys and questionnaires are common methods to reach empiric data.

Metrics I have developed are inspired from the "Security Requirement Functions" in Common Criteria, Part 2 [CCIMB 2004]; capability evaluation methodology of SSE-CMM [SSE-CMM 2003] and some criteria specified in ISO17799 [ISO/IEC 17799:2000]. Another similar work was "Information Security Management BS7799.2:2002 Audit Check List" [BS7799.2:2002] which includes significant amount of checklist requirements and auditing functions, but then again no quantitative metrics. Blending these requirements with the metrics model offered by NIST [NIST SP800-55]; I have tried to create an original tool to measure IT Security performance level. The quantitative metrics I have developed fits into a total metrics program offered by NIST, as shown in Fig. **??** When applying these metrics, two ways of obtaining data can be used. "Manual Data Collection" and "Semi Automated or Automated Data Resources". Developing questionnaires and conducting interviews and surveys with organizations' staff is called "Manual Data Collection" [Marion 2000]. If an organization has a password policy, calculating the passwords that are actually generated according to this policy, or making surveys to understand the security awareness level can be given as an example to this. In my project, I used this method for the survey part and for the checklist part of evaluation procedure.

Figure 1.1: "Security Metrics Program Structure", [NIST SP800-55]

Semi Automated & Automated Data Resources can be defined as self assessment tools, certification and accreditation databases, incident reporting and response databases. Computing the Average number of intrusions detected monthly is a way to perform this approach. More examples can be found, like computing the percentage of crackable passwords within a predefined time in order to measure the effectiveness of an organizations password policy; but I'll give a deeper look on applications in the following chapter. Automated data resources are very helpful to fill our evaluation balanced-score-card; as they provide solid quantifiable data ready to be processed.

For an efficient metrics program and a meaningful evaluation of the performance, the difficulty of measurement will decrease as more data gets available. As the security controls are documented and placed with the metrics system implemented into it, the ability to collect the outcome (metrics data) will also improve. Still, data collection automation depends on the availability of data from automated sources and the technical abilities of equipment, although it usually has a higher rate than the availability of data from people.

"Once security is integrated into an organization's processes, the processes become self- regenerating, measurement data collection becomes fully automated, and the mission or business impact of security-related actions and events can be determined by data correlation analysis."[4]

In order to implement a metrics program effectively, there are certain traps to be avoided as stated by Karl Wiegers also [Wiegers 1997]. As in OCTAVE,

[4][NIST SP800-55] Swanson M., Bartol N., Sabato J., Hash J., Graffo L., "Security Metrics Guide for Information Technology Systems" NIST Special Publication 800-55; July 2003. http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf, 2004-09-09

creating a business case, having management commitment is the most important part to generate a measurement culture within the organization. Other traps to avoid -or goals to achieve- can be listed as:

- Lack of management commitment
- Measuring too much, too soon
- Measuring too little, too late
- Measuring the wrong things
- Imprecise metrics definitions
- Using metrics data to evaluate individuals
- Using metrics to motivate, rather than to understand
- Collecting data that is not used
- Lack of communication and training
- Misinterpreting metrics data[5]

Finally, using ratios, scales, percentages and averages to gain a quantitative method of measuring with numerical values instead of trying to describe the security level by qualitative metrics will give us a solid view over Return on Security Investment (ROSI). And hopefully, we'll be able to say "Our risk score reduced by 20% after the investment" instead of saying "Trust me, we are more secure than before we spent the money.".

[5][Wiegers 1997] Karl E. Wiegers, "Software Metrics: Ten Traps to Avoid" http://www.processimpact.com/articles/mtraps.html at 2004-11-23

Chapter 2

Metrics Development

In this section, I have been prepared for data collection, which includes activities that are key for establishing a comprehensive IT Security metrics program, to effectively measure IT Security performance. To start with, determining the performance targets, the goals and objectives of an organization (and also the goals by measuring IT Security performance) is the first step in implementing quantifiable metrics. Following that, identification, definition, development and selection of IT security metrics are the core parts of this Master's Project.

As also stated in the Common Criteria, "In order to achieve greater comparability between evaluation results, evaluations should be performed within the framework of an authoritative evaluation scheme that sets the standards, monitors the quality of the evaluations and administers the regulations to which the evaluation facilities and evaluators must conform." [CCIMB 2004] But there is no official method of evaluation that is specified. So that the evaluation authorities are free to choose or build their own method and scheme of evaluation. Metrics I have developed, are not part of a CC evaluation methodology, but derived from the same source and need for a tool.

2.1 Determining Performance Targets

Performance targets has to be set for efficiency, effectiveness and impact metrics, as these aspects of security operation do not assume a specific level of performance (like reducing the number of virus infected computers, decreasing the amount of easy-to-guess passwords..). Defining a company's IT security performance goals and objectives should be expressed in the form of high level policies and requirements. Existing laws, regulations and best practices (as I mentioned before in "background" section of this master thesis) describe the dimensions of an effective IT security program.

"IT security performance goals identify the desired results of system security program implementation, while IT security performance objectives enable the accomplishment of goals. IT security metrics monitor the accomplishment of goals and objectives."[1]

The objective of our measurement process should be collecting objective data about the current state of the system so that metrics we collect may allow managers and administrators to make data-driven decisions. Metrics, when applied constantly over time will track the organizations progress toward its goals and assess the impact of changes. In this project, knowing that every organization as unique needs and different assets (differing to the sector), I focused on metrics that are to be used as an internal performance indicator. What insights are to be gained and what were the reasons for collecting a specific metric is explained for each metric chosen.

KPIs (Key Performance Indicators) for IT Security performance can be defined as:

- Efficiency and the effectiveness of IT Security policy
- The impact of training on employees
- Robustness of network systems
- Incident response and contingency efforts
- and The assurance of Access Control

According to these goals and objectives, I have tried to develop metrics that are applicable to a wide variety of organizations with similar performance targets.

2.2 Types of Metrics

Evaluation is, according to Webster's New Riverside University Dictionary, "to determine or fix the value of or to examine carefully"[2]

Types of metrics that are to be used may differ between industries as the performance goals also differ. Access control maybe crucial in a finance network managing business transactions, than a health care system for storing data. But as long as I have been trying to prepare an industry-neutral system, I focused on the basic measurements that are important for any

[1]Lennon, Elizabeth B., "IT Security Metrics", NIST USA, 2004 http://www.itl.nist.gov/lab/bulletns/bltnaug03.htm

[2]Webster's II New Riverside University Dictionary, Riverside Publishing Company; Boston, 1984. 2001-2003

implementations of metrics system.

In this sense, it is possible to classify metrics in four main types, which are implementation metrics, effectiveness metrics, efficiency metrics and impact metrics. Metrics that we chose should be in harmony with performance targets and should help to evaluate key performance indicators. When implementation metrics require full complementation, other three kinds of metrics may establish the performance goals decided by the management.

Although I define metrics to be implementation, effectiveness or efficiency metrics; the structure of this document is free from this classification. In the following chapters you will find metrics developed regarding the specification area of evaluation (e.g. Organizational, People and Technical aspects of evaluation).

2.3 Evaluating Organizational Security

2.3.1 Policies

"Policies allow an organization to set practices and procedures in place that will reduce the likelihood of an attack or an incident and will minimize the damage caused."[3]

A policy, usually seen as a salad dressing on top of company's network security mixture of firewalls, virus scanners, IDSs is actually the critical definition of a plan or course of action to provide security and hold the whole security structure together. A policy should be intendent to influence and determine decisions, actions, and other matters. A policy should be to provide management direction and support for information security.

Most technical controls are the responsibility of the information systems manager or the network administrator. Policy, on the other hand is the responsibility of the upper management. Security policy should document the philosophy and the strategy of an organization, with regard to confidentiality, integrity and availability. Unfortunately this is not the usual case. As seen in the figure, majority of the security policies are not approved at board level according to Information Security Survey 2002 [ISS 2002]. Of course, this may differ between organizations; confidentiality of data can be the main theme of a military or government security policy while integrity has priority in commercial sector. When determining an organizations information security philosophy, main object is not to prevent a concrete defense and a discrete attack, but to make things easier for users and ease the sys-

[3]Charl van der Walt, SecurityFocus, 2001-06-11

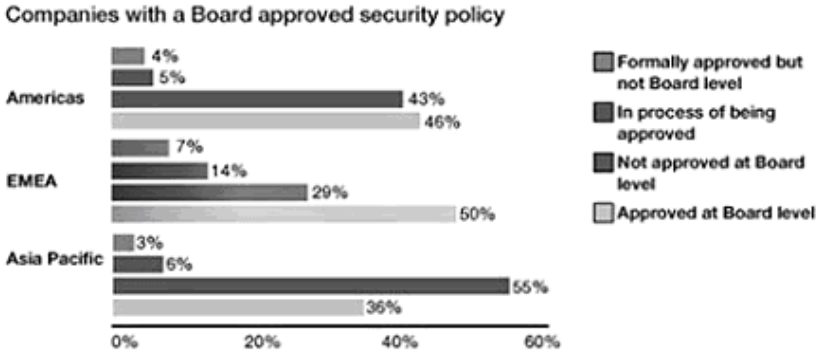

Figure 2.1: "Companies with a Board approved Security Policy", [ISS 2002]

tem administrators work load. Then the strategy should determine whether to defend the security implicitly or explicitly. Finally a series of procedures implement how to apply policy rules.

If policies are not console, consistent and easily available, nobody will apply them. My aim was to evaluate a security policy both with its content and with its ease of use. To ensure this, I have included not only implementation but also effectiveness and efficiency metrics to measure the performance level of IT Security Policy.

For the implementation part, there are certain measures that a security policy should cover. This content is also necessary to get ISO17799 compliance. But this does not mean that an ISO certified policy does not need to be measured with performance metrics, as the performance of policies are depended on performance on people generating and using policies. Metrics should still be applied regularly to see the improvement or disprovement achieved with the policy. Still, as it compromises 137 control objectives that must be achieved before an organization can apply for certification standard, ISO ease the development of metric program a lot. Similarly, GMIT takes a business oriented approach while ITSec tends to focus on technology.

Policy should cover:

- Physical security
- Network security
- Access control
- Authentication
- Encryption

- Key management
- Compliance
- Auditing & Review
- Security Awareness (Training & Education)
- Incident response and disaster contingency plan

It is more a business case rather than technology, to create strong policies, defining specific roles and responsibilities as it will lead the company to a secure business. And a secure business is the only business that will be able to grow safely.

2.3.2 Procedures

Biggest problem of the companies are derived not from the technical difficulties but from lack of control over the work flow and the employee behaviors. Procedures tend to solve this problem by formulizing and describing how to implement the IT Security Policies. Effectiveness of a policy is directly proportional to the support of procedures that enforce the application of the policy. Processes should go through a certain procedure that keeps thing running in a certain format and in order.

Is there a specified password length and character requirements? Does the system respond negative is password selection is not made according to these rules? How does the maximum age of a password and the uniqueness applied?

Procedure should be a step-by-step guide to usage and application of TT Security controls.

2.4 Evaluating "Minds"

The human factor in the information systems can affect security in many ways. In fact, the security depends on the human factor. End users may lead to an accidental breach or social engineering attacks. Of course there can also be inside attacks to a company by malicious employees, but as long as this is more a matter of trust in recruitment system, I will try to evaluate the awareness, training and education (knowledge) of employees which is necessary to prevent incidents and vulnerabilities.

As said, *"The biggest threat to a computer system is not a virus, an unpatched hole in a key program, nor a badly installed firewall. In fact the*

biggest threat could be you."[4] Kevin Mitnick to the BBC news online "How to Hack People" October 14, 2002.

It's easy to manipulate people rather than technology as most of the time organizations overlook that human element. Some "built-in" behaviors of many people (like trust, carelessness, desire to be helpful, curiosity and fear of the unknown) make employees vulnerable to Social Engineering attacks. This makes a well documented (easy-to-read) and accessible security policy and education on the policy crucial. For the policy to be affective education must be a regular feature. Some companies require all employees to review the policy each year to catch up with revisions, if any.

There are certain ways of creating awareness; this may include training and education programs, or real-life examples and stories of hacking caused by inside information or over trust or ignorance on an employees part. Most of the time, security mistakes of the employees are the same, and derived from so called "bad habits" which include:

- Post-It Passwords
- "I did it my way" attribute
- Leaving the computers on and walking away..
- Curiosity (opening attachments)

as the most common ones according to NSI Security Sense Project.

2.4.1 Awareness, Training, Education

"Agencies and organizations can not protect the integrity, confidentiality and availability of information in today's highly networked systems environment without ensuring that each person involved understands their roles and responsibilities and is adequately trained to perform them" [NIST 800-16]

IT security training should be focused on job functions or roles and responsibilities specific to individuals, not to job titles. And, with recognition that individuals have unique backgrounds, therefore different levels of understanding [Nichols 2001]. Steps to achieve IT Security knowledge

is as shown in the figure, a long-term goal. And in each of these steps the method for measuring the impact of training should be different. By measuring awareness of staff, companies also measure the effectiveness of their training program.

[4][Mitnick 2002] Kevin Mitnick, "How to Hack People", BBC News 2002-10-14, http://news.bbc.co.uk/1/hi/technology/2320121.stm

	Awareness	Training	Education
Attribute	"What"	"How"	"Why"
Level	Information	Knowledge	Insight
Learning Objective	Recognition and Retention	Skill	Understanding
Example Teaching Method	Media(Videos, newsletters, posters)	Practical Instruction (Lectures, Case Studies, Hands-on Practice)	Theoretical Instruction (Seminar and discussion, Reading and study, Research)
Test Measure	True/False, Multiple choice	Problem Solving Recognition	Essay

Table 2.1: "Employee Training Matrix", [SP 500-172]

But as it was with the policy development, there isn't enough managerial attention to Security Education either. Information Security Survey 2002 clearly showed that respondents named "lack of security awareness by users" as the top obstacle to effective information security, however, only 28% listed "raising employee information security training or awareness" as being a top initiative in the organization's future [ISS 2002]. This also shows many employees think it is up to the employer to provide IT Security training although the same survey indicates less than 50 percent of the companies have an IT security and awareness program. Training of employees is crucial to perform security awareness. Training of current employees and new employees (within certain amount of days of hire) or when an employee enters a new position dealing with sensitive information is a must.

"Security training is the best return-on-investment of any security safeguard"[5]

A well trained staff can often compensate for weak technical procedural safeguards. Companies spend millions of Euros every year improving hardware and software in order to prevent malicious attacks. All this is of no use if the end users do not follow good security practices. The first line of defense is employee awareness, the critical "humanware" component of the security. According to NSI (National Security Institute), nearly 80 percent of information security breaches and resulting losses originate from inside an organization. Employees must be aware of the facts about:

- How to protect a company's critical information

[5][NIST SP800-16]

How Many Incidents? by percentage	1 – 5	6 – 10	>10	Don't Know
2004	47%	20%	12%	22%
2003	38%	20%	16%	26%
2002	42%	20%	15%	23%
2001	33%	24%	11%	31%
2000	33%	23%	13%	31%
1999	34%	22%	14%	29%
How Many Incidents From the Outside?	**1 – 5**	**6 – 10**	**>10**	**Don't Know**
2004	52%	9%	9%	30%
2003	46%	10%	13%	31%
2002	49%	14%	9%	27%
2001	41%	14%	7%	39%
2000	39%	11%	8%	42%
1999	43%	8%	9%	39%
How Many Incidents From the Inside?	**1 – 5**	**6 – 10**	**>10**	**Don't Know**
2004	52%	6%	8%	34%
2003	45%	11%	12%	33%
2002	42%	13%	9%	35%
2001	40%	12%	7%	41%
2000	38%	16%	9%	37%
1999	37%	16%	12%	35%

Figure 2.2: "How many incidents? From outside? From inside?" [CSI/FBI 2004]

- How do they fit in the company's information security program
- How their actual job security depends on information security in networked business

There can be found many information security awareness tests and services over the internet, (NIS, SANS, CERT) provided by different organizations. My object was to create a checklist that measures results of awareness and training programs, covering the key points of IT security and evaluating the effectiveness of a past training, if there has been any.

Some of these services are the Enterprise Security Manager by Symantec and Security Sense by NSI -a continuous information security awareness service for employees-. Another way is the tests like ITAA (Information Technology association of America) Information Security Awareness Test [ITAA 2004], or ISSA (Information Systems Security Association) The Human Firewall Information Security Awareness Survey [ISSA 2004].

Finally, in organizations, the utility of the system is affected -or even determined- by users, so the measuring of the functionality of the technology can not

solely have a machine view but also a people view, eg. the functionality of the people who use the technology.

2.4.2 Certificates

As I mentioned the tests as a way of measuring IT Security awareness and education level of employees, why not consider a certificate that is also given after succeeding in certain tests. There are a large number of certificates accepted and respected in the business area and although I personally believe that they don't necessarily promise the holder to be an IT Security professional, they may be helpful to evaluate an organization's staff.

May assume that a certified individual holds the appropriate level of knowledge and skills necessary for key areas of information security which are referred as common body of knowledge and can be listed:

- Access Control
- Application Security
- Cryptology (and its IT applications)
- Legal Aspects of Information Security
- Business Continuity
- Operational Security
- Physical Security
- Security Architecture
- Telecommunications and Network Security

As there are vendor neutral certificates, covering these common aspects of IT Security, there are also vendor specified ones. Widely accepted, CISSP (Certified Information Systems Security Professional) issued by (ISC)2 ; GIAC (Global Information Assurance Certification) by SANS Institute and CISA (Certified Information Systems Auditor) by ISACA are most famous certificates in the market.

The vendor specific certificates (like Cisco, Symantec) are not eligible to give an overview understanding of IT Security in my opinion; so I did not include them in this metrics system

2.5 Evaluating Technical Security

Technology is rapidly advancing and security techniques and technologies along with it. VPN requirement, IDS s, firewalls, routers, OSs, penetration testing tools and DNS are a few technologies that security professionals must be able to keep up with and learn inside and out.

When it comes to security metrics, there are certain data resources both automated and semi-automated that can be used to measure IT Security Performance from a technical point of view. This section implies to measure, the implementation of Access Controls, effectiveness of firewalls and IDSs and the efficiency of backup & contingency plans, configuration management. To perform these checks and measurements, I have divided the IT structure into six parts as seen; which is a common methodology.

Once described what aspects to be measured, the problem is where to find the data from. The biggest source to be used are application data sources. Many applications collect data as part of their function which can be measured. An example is an anti virus application running on servers that can report all the machines that are managed and have updated virus definitions. Another can be a log shipping server. These systems are designed to collect data and report on other systems.

Nowadays, with the advanced network scanning tools it's possible to see which machines on the network are running which operating systems, whether they are patched or not and even the number of open ports and vulnerabilities to these services. Nmap, a free network exploration and security auditing tool, is an open source utility that works fine to scan large networks [insecure.org/nmap] As alike, GFILanGuard [gfi.com/lannetscan], Nessus [nessus.org/] and many else are useful applications that can be used -among from their purposes- to obtain metrics data from the network. These tools can give detailed information about what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use

With so many resources, there is only one question left to answer, what shall we measure, how much shall we measure?

2.5.1 Access Control

Access control is a core aspect of information security as it is the key for authentication and confidentiality. Access control policies and rules for identification, authentication and authorization of IT assets are the prerequisites

for protecting the confidentiality, integrity and availability of sensitive information. Any type of security program begins with access control. Access by unauthorized personnel / people (intruders) must be denied in order to protect what is believed to be confidential. Organizations put physical bars and guards at the gates and around the systems, then what? The systems are connected to the internet expanding vulnerabilities and means of physical access totally by passed.

In many of the best practices, methodologies or industry standards access control six key objectives are considered:

1. To control access to information
2. To prevent unauthorized access to information systems
3. To ensure the protection of networked services
4. To prevent unauthorized computer access
5. To detect unauthorized activities.
6. To ensure information security when using mobile computing and telenetworking facilities

When said "access" the first thing pops up in our heads is of course, passwords. To check the effectiveness of password policy and to test the average number of "good" passwords that are eligible, we should crack -or at least attend to crack- them. But as long as passwords are supposed to be private and secret, there comes a legal issue to check. Privacy statements must be considered before taking an action and users should be warned.

Once it is going to be done, problem of calculating incompliant passwords and decreasing the amount of them is not so difficult. Many of the user ids and passwords are easy to guess or crack and most of the time even though the organization has a password policy, users deny to apply it. Tools like "LophtCrack" [atstake.com/products/lc/] -a password auditing application- can crack windows passwords from hashes or perform dictionary and brute force attacks. As this is a commercial product, companies on low budget may also try "John the Ripper" [openwall.com/john/] or Cain and Abel [oxid.it/cain.html].

2.5.2 Auditing and Monitoring Security Logs

Auditing and monitoring services are crucial for today's network administrators. A security officer or any network administrator with security in mind should pro actively monitor what is going on the network. But this does not only mean to keep logs from IDS and other log shipping servers on

a file and never looking back to them again, as it is the case most commonly. Usually firewalls and IDS systems produce too many meaningless data for administrators and they are never being checked. It is also common to outsource Managed Security Services for the 24/7 analysis of security logs.

But these logs are actually meaningful and can even be more meaningful with the implementation of metrics system. As a source for automated and semi-automated data, security logs give us the chance to measure IT Security performance regularly over same queries and conditions so that the changes can clearly be seen within following periods.

If the number of unauthorized connections is less than the previous month or the percentage of dropped connections has decreased, we may say that the organization's security risk is also reduced.

2.5.3 Viruses

As they are one of the biggest threats against computer security, viruses are also a very good source for quantitative metrics system. The data we can collect from virus checks, programs and so on, does not only inform us about network security, but also the awareness of employees. Again, human curiosity -to attachments- causes most of the viruses spread as I mentioned before.

Installing up-to-date anti-virus programs and statistically watching them provides sound knowledge on IT Security performance. Measures like percentage of virus protected computers or number of work stations with up-to-date virus definitions will reflect the level of implementation quality. Especially when performed periodically, these metrics show great contribution to our understanding of organizational security.

2.5.4 Backups

System without backups and contingency plans can not be safer than driving on the highway without a seatbelt and airbags. In an overall metrics program, level of IT Security Performance depends a lot on backups. Implementation of back up technologies and designing efficient procedures to effectively maintain frequent backups are certain measures that need to be taken.

When evaluating the level of backup systems and contingency plans, it must be understood that systems are not going to be tested only of technical aspects but of procedural view. Having backup systems, tapes and machines does not mean anything if they are not managed properly. The same way, having a contingency plan is not enough if this plan is not distributed to the appropriate users and if it's not being tested over the years. So when

it is backups and contingency plans we are talking about, measurement is mostly non-technical.

Of course it is not possible to have a complete non-technical view, as long as the mission is to measure IT Security performance, I can not throw away all the bits and bytes. Backup frequency of critical data and operations, the percentage of data that has been backed up are important measures. In many of the best practices, it is chosen the way of counting the number of files while calculating the percentages like these which is usually the number of backed up critical files divided by the number of critical files (this will be explained in the next chapter in more detail). Being quite radical, I chose a different way of calculating data related percentages. Instead of "number of files", I use "the size of files" which is described in MB (Megabytes). I believe this is an easier way to perform measurement also as it's more appropriate not to count a critical data file of 2MB the same with a critical data file of 0,5 MB as 1 file.

2.5.5 Configuration Management

Term of Configuration Management does usually refer to know what hardware and software products are being used and by which users in the system. This is quite a wide area that makes security administrators able to spot potential conflicts.

To give an example, non-repudiation of origin, ensuring that a subject that receives information during a data exchange is provided with evidence of origin [CCIMB 2004], meaning who actually sent the data is a part of configuration management. But more simply, having the list of IP addresses and MAC (Physical) addresses on the network is the most basic step of configuration management. Organization must be able to know what is going on the network.

Configuration management can also help to track what software is used and reduce costs by ensuring everyone is using standardized package when possible. In this sense, I have developed the metrics for measurement of configuration management with the generic requirements of Common Criteria [CCIMB 2004] and NIST Special Publication 800-55 [NIST SP800-55]. Requirements I have specified in this part varies from implementation and management of a configuration database to patch management and OS hardening. Other metrics that concerns implementation facts but does not fit under previous sections also take place here. These include operations concerning encryption and non-repudiation functions.

Chapter 3

Quantifiable Metrics

3.1 Security Check-Up with Quantifiable Measures

This section aims to create the actual metrics in order to collect detailed measures of performance. The data collected by these metrics can then be analyzed to create a quantitative understanding of security level in the organization. I have established the measurable targets raised from security criteria and best practices mentioned in the *"Background"* section of this thesis so to evaluate important assets of a system.

3.2 Part1: Organizational View

3.2.1 Policy Check-Up

1. Does the organization have a security policy developed?
To start with, there must be an existing Security Policy in order to be evaluated.
Method: Check List.
Evaluation: Yes (1), No (0).

2. Is it obligatory to read and sign the Security Policy during the recruitment procedure?
First step of making the Security Policy accepted in the organization. This procedure should be repeated every time a new employee is recruited or changed working position
Method: Check List
Evaluation: Yes (1), No (0)

3. What is the percentage of departments with the latest version of Security Policy posted?
It is not enough to have a Security Policy, but to distribute it to the relevant

departments and responsible chiefs.
Method: Scorecard
Evaluation: [(Number of dept. with SP posted)/ (Total Number of Dept.)] * 100

4. What is the percentage of employees who have read and signed the Security Policy?
Derived from the second metric, the policy to be effective, it has to be known and accepted by the users of the system.
Method: Scorecard
Evaluation: [(Number of Employees signed the policy) / (Total number of employees)] *100

5. What is the percentage of websites with a posted privacy policy?
If the public accesses the system, are there controls implemented to protect the integrity of the application and the confidence of the public. [NIST SP800-45]
Method: Scorecard
Evaluation: [(Number of web sites with a posted policy)/ (Total num. web sites)]* 100

6. What is the percentage of incidents happened against preventive measures in the Security Policy?
This indicates the effectiveness and simplicity of the Security Policy. Do the accidents still happen although there are preventative measures defined in the policy?
Method: Scorecard
Evaluation: [(Number of incidents with preventative measures stated in policy)/ (Total number of incidents)]* 100

7. Is the IT Security Policy easy-to-use (simple and practical)?
A policy that is written only to be on shelves is not going to be effective at all. A policy may be less of an art piece of literature but it should be understood well and applied to daily business procedures. Management should ensure that users are "happy" with the policy.
Method: Survey
Evaluation: Not at all (0), (1), (2), (3), (4) Easy-to-use and practical

8. Is the IT Security Policy easy to manage and maintain?
Policy has to be open to changes and evolution. As best policies are time-proof, documentation should be technology-neutral and vendor-free.
Method: Survey
Evaluation: Not at all (0), (1), (2), (3), (4) Easy-to-manage and maintain

9. What is the average time gap between the system reviews for policy changes?
Is the policy being reviewed for changes and additions? How often? It is good to have a lower average of time gap between reviews, although regular checks within a pre-specified date and irregular checks during the technical changes and advancements are also advantageous.
Method: Scorecard
Evaluation: Specified time period /Total Num. of Reviews within specified time period

10. Is the IT Security Policy easy to access by people seeking specific information?
Availability of the policy is evaluated by this measure. Is the policy stored electronically in company network to access and search for information or do the users have a hardcopy? Is it indexed and structured for specific applications?
Method: Survey
Evaluation: Not at all (0), (1), (2), (3), (4) Easy-to-access and search for information

11. Is the data classification defined in the IT Security Policy?
Is the data classified for confidentiality and aim of use? Most commonly as: unclassified, shared, company only and confidential.
Method: Checklist
Evaluation: Yes (1), No (0)

12. What is the percentage of data compliant with "data classification" principle?
Calculated as megabytes, this metric is important to evaluate the implementation level of data classification principle in IT Security Policy.
Method: Scorecard
Evaluation: [(Size of data compliant to data classification) / (Total size of stored data)] *100

13. Are the physical network equipment classified the same way?
Laptops and other portable devices, mainframes, servers and access points etc must be specified the same way for usage rules and physical protection directives.
Method: Checklist
Evaluation: Yes (1), No (0)

14. Does the policy state that information security everybody's responsibility?
It cannot be meaningful for the users to sign an IT Security policy that they

don't think it is under their responsibility, protecting IT infrastructure.
Method: Checklist
Evaluation: Yes (1), No (0)

15. Is the designation authority (to the CSO or whoever that is responsible) mentioned?
The IT Security policy should refer to somebody responsible in order to get response and feedback from the users, this authority will also be in charge of managing and maintaining the document. It is not necessary that the policy should be owned and signed by the very same person as higher managerial owning usually get more attention.
Method: Checklist
Evaluation: Yes (1), No (0)

16. Are the functions and responsibilities of security officer clarified?
Is Security Officer's role with its warrant and limits pointed out in the document?
Method: Checklist
Evaluation: Yes (1), No (0)

17. Does anyone else have the permissions to change the policy else from the owner?
To protect the integrity of the IT Security policy, it must be ensured that only one authority (a person or a board of members) have the right to make changes on the document.
Method: Checklist
Evaluation: Yes (1), No (0)

18. Is the responsibility of specific technical issues designated to related people?
Does the IT Security Policy state who owns the technical management of a specific system? Does the policy require sensitive information and technologies to be physically secured at all times? As a result of classification of technical infrastructure, important technical assets require specific attention. These include the firewalls, IDSs, log-servers, access control mechanisms, back up facilities and etc.
Method: Checklist
Evaluation: Yes (1), No (0)

19. Does the policy mandate minimum authentication controls?
Authentication controls like minimum password length, minimum change interval etc should be stated in order to have a powerful security policy.
Method: Checklist
Evaluation: Yes (1), No (0)

20. Does the policy include guidelines for securing many of your principle technologies?
Aim of a security policy is also to ensure an organizational understanding and strategy towards IT Security risks and assets. It is important to have certain basic lines for principle technologies like operating systems, databases, networks etc in order to create time-proof and vendor-neutral policies that last for a long period.
Method: Checklist
Evaluation: Yes (1), No (0)

3.2.2 Procedures Check-Up

21. Is there a user registration procedure?
Does the IT department register every user according to specified procedures with compliance of IT Security Policy? Is selection of unique and hard-to-guess user names & passwords ensured with this procedure?
Method: Checklist
Evaluation: Yes (1), No (0)

22. Is there a user de-registration policy?
The same way, is there a procedure for terminating an old users account. It's widely known that existing accounts, after a users' unemployment, may be abused.
Method: Checklist
Evaluation: Yes (1), No (0)

23. What is the percentage of systems that perform password policy verification?
Are procedures in place to determine compliance with password policies? With a query against user password directory or password cracking tool records, numbers can be obtained easily.
Method: Scorecard
Evaluation: [(Num. of Sys. Perform policy verification) / (Total Num. of Sys.)]*100

24. Is there a procedure for the projects to go through security policy compliance test as well as quality assurance?
Projects may use confidential data and important assets of information technology; to prevent the leak of information or vulnerabilities projects must be evaluated within IT Security measures.
Method: Checklist
Evaluation: Yes (1), No (0)

25. What is the percentage of projects that went through security policy compliance test?
Derived from the previous metric, I aim to measure the effectiveness of procedures here.
Method: Scorecard
Evaluation: [(Number of security approved projects) / (Total number of projects)]*100

26. Is there a procedure for updating virus definitions?
Are the virus definitions updated continuously within certain time gaps or do the updates take place after a new threat is exposed?
Method: Checklist
Evaluation: Yes (1), No (0)

27. What is the average time gap between virus definition updates?
Following the previous metric, shorter gaps between updates will provide better protection against viruses and worms. Still, tracking news services and security vendors for immediate updates are important if a regular schedule is not applied.
Method: Scorecard
Evaluation: Specified time period / Total num. of updates within the specified period

28. Is there a procedure for patching process?
Some vendors provide automated updates, but administrators still has to manage the schedule and the priority of the patches. Is there somebody or a service responsible for this process and is it stated how often programs have to be checked for updates?
Method: Checklist
Evaluation: Yes (1), No (0)

29. What is the average time gap between the time when a patch is released, and time when it is installed?
Systems include OS, firewalls and servers have to be updated continuously, shorter periods will again give a better view of protection. Usually vendors have regular dates for releasing new patches (like the first Thursday of the month), administrators has to be up to date with new information.
Method: Scorecard
Evaluation: Total amount of delay time for a patch to be installed / Total num. of patching processes within the specified period

30. Is there a procedure for backup process?
An approved procedure for backing up systems is highly recommended for scheduling the process, managing the tapes and storing them. More metrics

about this topic is included in "Backup & Contingency Check Up" part.
Method: Checklist
Evaluation: Yes (1), No (0).

31. Is there a procedure for testing and authorizing new/revised hardware before implementation?
Part of the configuration management system, all new and revised systems must be tested and enrolled to the database.
Method: Checklist
Evaluation: Yes (1), No (0).

32. What is the percentage of employees gone through a background check before employment?
Although it may not sound nice, this process ensures that confidential data is not given to the hands of people who have previous criminal records or restrictions due to hacking activities.
Method: Scorecard
Evaluation: [(Num. of Emp. Gone through process) / (Total num. of employees)] *100

33. Is there a disciplinary process for violation of organizational security?
Does the policy enforce a disciplinary process in place for employees who have violated organizational security processes and procedures?
Method: Checklist
Evaluation: Yes (1), No (0).

34. What is the number of employees faced a disciplinary process during the last year?
Is the system actually being used and how effective the rules are? The number of employees faced a disciplinary procedure should be in balance (or in direct ratio) with number of incidents reported.
Method: Scorecard
Evaluation: Total number of Employees that faced a disciplinary process last year.

35. Is there a procedure for reporting security incidents, weaknesses or software malfunction?
Does the policy enforce users to feel responsible about security incidents and weaknesses so that they will inform the administrators about the case.
Method: Checklist
Evaluation: Yes (1), No (0).

36. What is the number of incidents, weaknesses and software malfunctions reported last period of time?

Method: Scorecard
Evaluation: Total number of reports (warnings) received.

3.3 Part2: Evaluation of "Minds"

37. Are users informed about the security policy and how to protect critical information?
Is the security policy just printed and published, or even signed by the users without giving particular information and training about "what it is for" or "how it works"?
Method: Checklist
Evaluation: Yes (1), No (0)

38. Are users informed of their responsibility of security?
Keeping the passwords secure, not leaving the computers unattended while logged on to network, not opening attachments and un-trusted storage devices (USB sticks, floppy disks etc.) are key points that users have to be informed about.
Method: Checklist
Evaluation: Yes (1), No (0)

39. Is the principle of individual responsibility of users for security of information systems achieved?
Not only enforced by the IT Security Policy, but also supported by trainings, newsletters, booklets, "horror stories", coffee-machine-posters and etc, and organizational strategy should be created to achieve the principle of individual responsibility.
Method: Survey
Evaluation: Couldn't achieved (0), (1), (2), (3), (4) Achieved.

40. What is the percentage of employees with significant security responsibilities who have received specialized training?
Have employees received adequate training to fulfill their security responsibilities? Is employee training and professional development documented and monitored? This metric defines the level of expertise among designated security roles and security responsibilities for specific systems within the organization. Employee training records or database; course completion certificates can be used as a data source.
Method: Scorecard
Evaluation: [(Num. of Certified/Trained Employees) / (Total Num. of Employees)] *100

41. Can you indicate the awareness level of employees?
Resulted from an awareness test or Security Officer's personal overview, awareness level also indicates the effectiveness of the training programs done previously; if there are any.
Method: Survey
Evaluation: Not Aware of IT Security Risks (0), (1), (2), (3), (4) Aware of IT Security issues.

42. What is the average "hours of training" per employee?
With higher educational process over employees, greater amounts of awareness will be achieved. Without discrimination, all employees from CEOs to a single office boy using a computer, should be trained same way for higher average of security awareness.
Method: Scorecard
Evaluation: (Total time spent on training processes) / (Total Number of Employees)

43. What is the percentage of highest level of education?
I classified the level of education into three parts as "undergraduate, graduate and post-graduate"; data can be obtained from employee records or database to evaluate the metric. Number of employees with post-graduate education, with graduate level of education and under-graduate level of education should separately calculated to be used.
Method: Scorecard
Evaluation: [(Num. of Emp. with post-graduate level education) / (Total. Num. Emp.)] *100

3.4 Part3: Technical View

3.4.1 Access Control Check-Up

44. Is there a strong password policy enforced by the management?
Setting up the rules for access control is the beginning of the game, without the policy and procedures implemented, no efficiency can be expected. A "strong" password policy should require at least 8 characters of an alpha-numerical string and restrict the use of names etc
Method: Checklist
Evaluation: Yes (1), No (0)

45. Are the users authenticated individually with passwords, smartcards, or other devices?
"Pass phrases" are no doubt more secure then simple 6 character passwords but usage of secure hardware authentication implementations like smartcards etc. ensure an even higher level of security. Data regarding this issue can be obtained from risk assessments, system audits, and baseline security

requirements.
Method: Checklist
Evaluation: Yes (1), No (0)

46. What is the percentage of unique user IDs?
Does the access control mechanism enforce segregation of duties? Access control lists and password files would be suitable to calculate the metric.
Method: Scorecard
Evaluation: [(Num. of users with unique IDs) / (Total Num. of users)] *100

47. What is the percentage of inactive users?
Depending on the log statistics of total number of accounts that are not logged on to the network within the last sixty days, this measure will help administrators to identify inactive accounts that may have occurred from unemployment of former employees or duplication of user accounts. These accounts must be terminated in order to prevent access vulnerabilities.
Method: Scorecard
Evaluation: [(Num. of Accounts not logged in last 60 days)/ (Total Num. of Accounts)]*100

48. What is the percentage of highest level of systems without active vendor-supplied passwords?
Many products support passwords "out from the box", these vendor-supplied passwords must be replaced immediately as they are widely known and vulnerable to attacks. This metric implies to measure implementation process of changing the passwords.
Method: Scorecard
Evaluation: [(Num. of Sys. without vendor supplied passwords)/ (Total Num. of Sys.)] *100

49. Is there a documentation that clarifies access control rules and rights for different user groups and levels?
Access control rules and rights should be identified according to the policy, and must be documented for future reviews. For efficiency, documentation must be regularly reviewed and tested to have integrity with the actual set of rules.
Method: Checklist
Evaluation: Yes (1), No (0)

50. Is there a regular formal review of users' access rights?
This is a measure to constantly check access lists and related documentation for implementation mistakes.
Method: Checklist
Evaluation: Yes (1), No (0)

51. What is the number of users with access to secure software and applications without being security administrators?
Derived from the previous metric, with data obtained from access control lists; security officers can measure the level of access to security software restricted only to security administrators. This is an implementation metric and requires 100 percent completion which means nobody must be able to access these services except from security administrators.
Method: Scorecard
Evaluation: (Num. of Users with access to secure software & applications.) - (Num. of Security Administrators.)

52. Are secure methods enforced for logging on firewalls, intrusion detection systems and VPNs?
Do the systems allow remote access and in which sense? Is encryption being used? If used, is the encryption algorithm an officially approved secure one? Is the key generation and/distribution process also secure?
Method: Checklist
Evaluation: Yes (1), No (0)

53. Are the access attempts logged?
Log keeping is crucial but of course not enough if these logs are not being monitored and analyzed afterwards. Detailed measurements concerning logs will be presented in the following part, here we ensure the implementation of monitoring access attempts.
Method: Checklist
Evaluation: Yes (1), No (0)

54. Does the IT Security Policy indicate the number of trials before an authentication failure?
Are the requirements for defining values for some number unsuccessful authentication attempts clearly stated in the policy and applied to the authentication system procedure?
Method: Checklist
Evaluation: Yes (1), No (0)

55. Is physical access to facilities and IT systems controlled?
When installing firewalls, IDSs, VPNs and every other ingredient of IT security salad, organizations can sometimes stay vulnerable to the oldest tricks of physical security and social engineering. Are visitors and contractors supervised? Is the equipment coming in and getting out of the organization's site being controlled?
Method: Checklist
Evaluation: Yes (1), No (0)

3.4.2 Security Logs Check-Up

56. Are firewall logs pro actively monitored?
Is there an implemented system or process to actively monitor firewall logs and analyze the data for future actions?
Method: Checklist
Evaluation: Yes (1), No (0)

57. Are IDS logs monitored?
Is there an implemented system or process to actively monitor logs created by intrusion detection system, and analyze the data for future actions?
Method: Checklist
Evaluation: Yes (1), No (0)

58. Is website usage monitored?
Is the website usage monitored for capacity reasons (threat of denial of service)?
Method: Checklist
Evaluation: Yes (1), No (0)

59. What is the number of unauthorized connections during the past period?
Within a pre-defined period, calculating the number of unauthorized connections by monitoring logs and analyzing them will give us an understanding of performance changes over time.
Method: Scorecard
Evaluation: Calculate the total num. of unauthorized connections detected (within certain time period)

60. What is the number of connections dropped?
As firewalls provide logs (data) for this information, connections dropped may mean attack attempts, or insecure connection requests. Measurement is important to see effectiveness of firewall implementation.
Method: Scorecard
Evaluation: Calculate the total number of connections dropped (within certain time period)

61. What is the percentage of e-mails rejected for spam / content restrictions?
Depending on the number of e-mails processed, having a low number of rejected mails, hence a low percentage of rejected/ restricted mails is impor-

tant to see.
Method: Scorecard
Evaluation: [(Num. of Rejected Mails)/ (Number of mails processed)] *100

62. What is the total size (in MB) of e-mails rejected?
To understand the capacity of bandwidth violated by spam e-mails, knowing the total size (in Megabytes) is an efficient measure. This way the impact of spam mails on the system will be clearer.
Method: Scorecard
Evaluation: Calculate the total size (in Megabytes) of rejected mails in the specified period of time

63. What is the number of out-going e-mails with inappropriate content?
Content filters are usually used in mail systems to stop unwanted content and reduce the internet traffic for optimized bandwidth. To evaluate effectiveness of cautions against inappropriate content number of restricted e-mails within pre-defined periods of time, will represent the status level if measured continuously.
Method: Scorecard
Evaluation: Calculate the total number of out-going mails with inappropriate content within the specified period of time

64. What is the false spam identification rate?
According to the report of ITAA, "Seventeen percent of permission based e-mails get incorrectly blocked or filtered by the top twelve internet service providers." To avoid incorrect filtering and effective management of mail system, measurement is necessary.
Method: Scorecard
Evaluation: [(Num. of falsely rejected e-mails) / (Total num. of rejected e-mails)] *100

65. Is the organization actually using the automated audit recording tools?
As known by most security administrators, analyzing logs is a hard and costly work that requires 24/7 observation. Derived from this need, many automated tools are developed in the sector. But still, human expertise is crucial. Does anybody check and review the logs kept?
Method: Checklist
Evaluation: Yes (1), No (0)

66. What is the number of restricted / banned site access attempts?
In some companies/ organizations, internet access is completely prohibited through the company network and in some of them it is restricted to certain sites. Recalled as "Internet Access Management", this managerial bans usually get employee reaction in a bad way. This metric can provide valuable

data to measure the impact of IT security policy over restrictions.
Method: Scorecard
Evaluation: Calculate the total number of restricted site attempts within a pre-defined time period.

Note: In this section, I have avoided measuring metrics like "average surf time per user" or "average surf time for the sites visited most" and "the top abusers for the internet usage" etc; the reason for this is that I consider these kind of metrics to measure the lost of productivity or employee distractions, but not to measure IT Security Performance as my main goal is.

3.4.3 Virus Check-Up

67. What is the percentage of systems being protected against viruses/worms/Trojans?
As it is an implementation metric, the goal of this measurement should be 100 percent. After all systems are ensured to be protected, other measurements can be done effectively.
Method: Scorecard
Evaluation: [(Num. of Sys protected by anti-virus software)/ (Num. of Sys that has to be protected from viruses)] *100

68. Percentage of systems with regular virus definition updates and regular virus scanning?
Anti-virus software requires regular updates and efficient management. Only installation of virus detection and elimination software is not enough, virus scans definition updates and virus scanning must be made constantly over time, automatically or manually.
Method: Scorecard
Evaluation: [(Num. of Sys with regular updates -e.g. weekly-)/ (Total Num. of Sys Protected)] *100

69. What is the number of systems that are alerted of virus infection within the last period of time?
How many virus alerts does the system give within a pre-defined time period (e.g. per month)? Knowing the level of infected computers/ disk drives etc. will prove the efficiency of virus definition updates and virus scan processes.
Method: Scorecard
Evaluation: Calculate the total number of virus infected systems within the last period of time.

3.4.4 Backup & Contingency Check-Up

70. What is the percentage of critical data in the system?
Identifying the most critical data will appoint priority to those files. All data calculations in this section must be done regarding the size of the data (in megabytes) not the number of files. Data classification that has already been addressed in IT Security Policy can be used to when identifying the critical data that has to be backed up.
Method: Scorecard
Evaluation: [(Size of critical data) / (Total size of data in the system.)] *100

71. What is the percentage of critical data that is frequently backed up?
Is there a frequent back up procedure for the classified data and operations and what is the efficiency of this procedure? A high level of percentage must be guaranteed in order to say back up procedures for critical files and operations is efficient.
Method: Scorecard
Evaluation: [(Size of critical files with an established backup frequency) / (Number of critical files requiring backup)] *100

72. What is the percentage of systems with an established contingency plan?
Having a plan is surely better than not having one, so the existence of a plan indicates a certain level of preparedness to expected external/ internal effects. But a contingency plan to be effective, it has to be documented well and distributed to the appropriate personnel.
Method: Scorecard
Evaluation: [(Num. of sys with a contingency plan)/ (Total Num. of Systems)] *100

73. Are the contingency plans being tested annually?
To understand the impact of a good implementation, it has to be tested over time. Regular tests make the plans better settled and easier to activate. Method: Checklist.
Evaluation: Yes (1), No (0).

74. What is the percentage of systems for which contingency plans have been tested in the past year?
If the organization has a contingency plan repository, which it should have, it must be reviewed periodically to test and readjust as appropriate the contingency plans.
Method: Scorecard
Evaluation: [(Num. of systems for which contingency plans have been tested annually)/ (Total number of systems with contingency plans)] *100

75. Are Risk Assessments performed and documented?
In corporation with contingency plans, risk assessment holds an important place; certain tests and vulnerability scanning have to be performed and documented in this action fpr better implementations.
Method: Checklist.
Evaluation: Yes (1), No (0).

76. Is there a "fail secure" system implemented
Does the system preserve the secure state in case of failure?
Method: Checklist.
Evaluation: Yes (1), No (0).

77. Are the equipment protected from power failures?
Power shortage creates a high level of risk according to the state of the occurence. Permanence of power supplies such as multiple feeds, ups or backup generator etc. can deal with this problem.
Method: Checklist.
Evaluation: Yes (1), No (0).

78. What is the number of incidents reported internally and/or to law enforcement?
I believe many companies do not report incidents to law authorities in order to protect company reputation. The FBI survey also supports this assumption. [CSI/FBI 2004] This is usually a managerial decision and security administrators can't do much about it. Still, I believe organizations should apply security metrics even to their most secret information in order to get realistic results.
Method: Scorecard.
Evaluation: Calculate the total number of incidents reported within the last period of time.

3.4.5 Configuration Check-Up

79. Is there a configuration Management Database that is actively maintained by the administrators?
A configuration management database allows officers to follow hardware and software implementations on the network. To be able to manage a network, administrators need to know it well.
Method: Checklist
Evaluation: Yes (1), No (0).

80. What is the percentage of systems with the latest patches installed?
Patch status can be addressed over certain vulnerability scanning tools or regular check ups; patch status verification is important to measure to see

the level of efficiency of patch management systems.
Method: Scorecard
Evaluation: [(Num. of Patched Sys)/ (Total Number of Systems)] *100

81. Are there any OS hardening standards being used?
Implementation of OS hardening is crucial in today's network systems as new vulnerabilities occurring everyday and hackers try to take advantage on weak systems.
Method: Checklist
Evaluation: Yes (1), No (0).

82. What is the percentage of systems with applied OS hardening standards?
This metric provides information on the efficiency of OS hardening standards' implementation. Hundred percent is expected as a result. Any systems that are non-compliant with the standards of course to be listed and issues should be addressed to fix the problems.
Method: Scorecard
Evaluation: [(Num. of Sys with OS hardening applied) / (Total Number of Systems)] *100

83. What is the percentage of computers with implemented automatic screen locking?
As a countermeasure against intruders and social engineering attacks from inside, automatic screen locking will provide effective security while a desktop is left unattended for a period.
Method: Scorecard
Evaluation: [(Num. of Desktops with auto-screen-lock) / (Total Number of Desktops)] *100

84. What is the percentage of computers that can not be booted else from hardware?
Booting from USB, CD-Rom or floppy to alternate the media may cause indefinite security flaws resulting in administrator privileges. Systems must be configured in order to prevent this action.
Method: Scorecard
Evaluation: [(Num. of Desktops can't be booted alternately) / (Total Number of Desktops)] *100

85. Are non-essential services disabled on servers?
Servers usually come with a variety of services and protocols, many of which are turned on by default; identifying common services and terminating the non essential services that create possible security vulnerabilities is security administrators' responsibility.

Method: Checklist
Evaluation: Yes (1), No (0).

86. Is there and organizationally accepted and approved encryption algorithm that is used in secure systems?
Usage of encryption standards, for implementations of communication and confidentiality of sensitive information is an important asset. Encryption mechanisms better be a widely known, secure one. Although this is hard to confirm, a government approved algorithm -like AES- is usually a better choice than an "home made" one.
Method: Checklist.
Evaluation: Yes (1), No (0).

87. What is the percentage of internal and external communication that is encrypted?
Is there an active usage of encryption mechanisms? What is the effectiveness of the system? If the external sites you communicate does not support encrypted, secure services and if most of your communication is based on this lines, then it does not matter how good implementation you have in-house. To evaluate the effectiveness of encryption measures, this metric is useful.
Method: Scorecard.
Evaluation: [(Total Num. of e-mails sent and received through un-trusted channels)/ (Total number of e-mails processed)] *100

88. Is the non-repudiation of origin guaranteed in communication systems?
This system ensures that the sender of the data can not successfully deny having sent the information. A method to ensure that a party that receives data/mail is provided with evidence of the origin of the information should be implemented (e.g. digital signatures, public key cryptography)
Method: Checklist
Evaluation: Yes (1), No (0).

89. Is the non-repudiation of receipt guaranteed in communication systems?
This system ensures that the recipient of the data can not successfully deny receiving the information. A method to ensure that a party transmits information during a data exchange provided with evidence of the receipt of the information should be implemented. (e.g. message report system)
Method: Checklist
Evaluation: Yes (1), No (0).

90. What is the percentage of portable devices with encryption capability for sensitive files?
The reason portable and mobile systems has to be protected is that portable systems are considered to be more vulnerable as they travel with their users

and there is a risk of being stolen or left unattended. All sensitive data files must be encrypted on this kind of devices.
Method: Scorecard.
Evaluation: [(Num. of mobile and portable devices with encryption capability)/ (Total number of portable and mobile devices)] *100

Chapter 4

Ending

4.1 Results & Comments on Quantifiable Metrics System

As a result of my studies and research, I can claim to have answered some of the questions and achieved the goal of my master Thesis Project. First of all, the question "Can we actually measure the level of IT security performance of an organization?" was answered, as yes, it is possible to measure IT security performance by implementing quantifiable metrics. It has been presented clearly that there is data that can be used for measurement, both provided by automated data sources and manual data collection. A well developed metrics system can actually be applied to these data to measure the performance level.

About the level of security performance, IT Security officers can, by looking at the results of measurements, analyze the metric system and decide whether they have implemented and managed the necessary aspects of security or not. Depending on the organization type and size, this metric system can help security professional define their network as "weak or good". The level of the security performance, as stated in the beginning of this thesis, is not a measurement to compare organization with other organizations. The aim is to continuously evaluate and validate IT Security performance with the quantifiable metrics. So, the security administrator can only make comments according to an organizations profile, which will sound like "Our security level is higher than the last year, the percentage of systems that are alerted for virus infection has reduced 10 percent". This will also answer the questions of "How does the security level of an organization change during periods?" Figure 4.1 is intended to give an example after the implementation of metrics program, and the analysis of the data gathered from quantifiable metrics; how should the trend (hopefully an improvement) will appear.

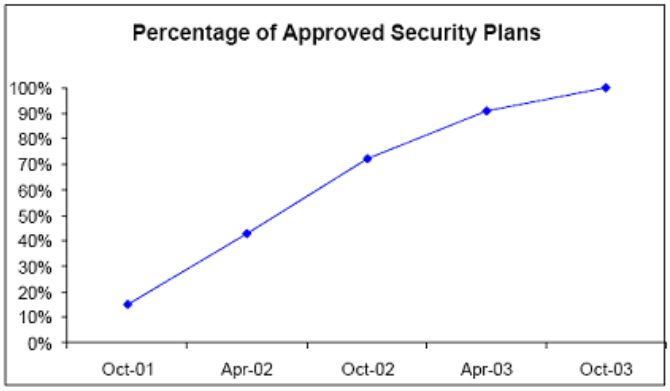

Figure 4.1: "IT Security Metric Trend Example", [NIST SP800-55]

Accountability, when added to Information Security's famous three aspects (confidentiality, integrity and availability) is sometimes even harder to achieve then others. To calculate the Return On Security Investment and to make it accountable in managers' eyes, security administrators can use quantifiable metrics. Results of a metrics system, can always be compared with the amount of investment on IT Security during the periods of time, providing a balance between how security improved by increasing the investment value on IT Security (or otherwise).

4.2 Conclusion

What I found at the end of this research that, it is not easy to measure the performance level of IT Security. But if we are going to do it, we have to do it with quantifiable metrics and in a very wide spectrum covering all aspects of information security. I have tried to cover these areas with a holistic view and established my metrics for each section.

Today's best practices are informative for organizations, but the lack of a tool to measure overall IT Security performance was indisputable in IT Security Metrics area. Common Criteria is particularly developed for products but not for systems and the publications of NIST go no further than showing us the way. I hope this document to be helpful and in benefit of both academic and commercial organizations.

But then again, use of a tool like this, an evaluation methodology, contributes only to the repeatability and accountability of the results but is not by itself efficient. This evaluation must be done by expert IT Security administrators that have the ability of analyze and judgment over the system.

Some future work can be the application of this methodology, so that we can see actual results and measure the ease of use. The metrics developed here are based on real, existing values that are also specified in how to obtain these values; what is left is to actually apply the method. Unfortunately this is outside the scope of my project, as I have stated before, a metrics program must be applied constantly over time with a minimum of 1 year period, to see the change in system processes.

Bibliography

Publications

[**ITAA 2003**] Mark Uncapher, ITAA E-Letter, September 2003
Url: http://www.itaa.org/isec/pubs/e20039-07.pdf at 2004/12/02

[**ITAA 2004**] Information Technology association of America, "Information Security Awareness Test", USA 2004.
Url: http://www.itaa.org/infosec/gendoc.cfm?DocID=203 at 2004/12/03

[**ISSA 2004**] Information Systems Security Association; 'The Human Firewall Information Security" , USA 2004.
Url: https://www.humanfirewall.org/smi/ 2004/12/03

[**Mitnick 2002**] Mitnick, Kevin. "How to Hack People." BBC NewsOnline, October 14, 2002.
URL: http://news.bbc.co.uk/1/hi/technology/2320121.stm at 2004/10/11.

[**Marion 2000**] Marion, Rodger ; "The Whole Art of Dedution:Research Skills for New Scientists", Galveston, University of Texas, School of Allied Health Sciences; 2000.
Url: http://www.sahs.utmb.edu/Pellinore/intro_to_research/wad/wad_home.htm

[**Martins&Eloff 2001**] Martins A., Eloff Jhp, Measuring Information Security, Department of Computer Science Rand Afrikaans University; March 2001.
Url: http://philby.ucsd.edu/ cse291_IDVA/papers/rating-position/Martins.pdf

[**Nichols 2001**] Kevin L. Nichols, GIAC Security Essentials (GSEC) Certification Practical Assignment, "Implementing an Information Security Program", August 22, 2001.
Url: http://www.sans.org/rr/papers/48/452.pdf at 2004/10/12

[**OCTAVE 2003**] Alberts C., Dorofee A. Managing Information Security Risks "The OCTAVE Approach" Addison-Wesley Publishing 2003 — ISBN: 0321118863

[**Payne 2001**] Payne, Shirley C. A Guide to Security Metrics, SANS Security Essentials GSEC Practical Assignment Version 1.2e, July 11, 2001.
Url: http://www.sans.org/rr/papers/5/55.pdf at 2004/09/10.

[**Wiegers 1997**] Wiegers, Karl E., Article "Software Metrics: Ten Traps to Avoid", ProcessImpact.com, 1997.
Url: http://processimpact.com/articles/mtraps.html at 2004/10/18

Best Practices

[**BS7799 1995**] British Standard for Information Security, 1995
Url: http://www.bsi-global.com/Global/bs7799.xalter at 2004/09/01

[**BS7799.2:2002**] "Information Security Management BS 7799.2:2002 Audit Check List", Val Thiagarajan B.E.; SANS Institute, 2002.
Url: http://www.sans.org/score/checklists/ISO_17799_checklist.pdf at 2004/12/03

[**CCIMB 2004**] Common Criteria for Information Technology Security Evaluation, Version 2.2, Revision 256 CCIMB-2004-01-001; January 2004
Url: http://www.commoncriteriaportal.org/public/expert/index.php?menu=2 at 2004/08/20

[**ISO/IEC 17799:2000**] International Organization for Standardization , Code of practice for Information Security Management; 2000.
Url: http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html

[**NIST SP800-55**] Swanson M., Bartol N., Sabato J., Hash J., Graffo L., "Security Metrics Guide for Information Technology Systems" NIST Special Publication 800-55; July 2003.
Url: http://csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf at 2004/09/09.

[**NIST SP800-27**] Gary Stoneburner, Clark Hayden, Alexis Feringa; "Engineering Principles for Information Technology Security (A Baseline for Achieving Security)", Revision A, NIST Special Publication 800-27 Rev A; June 2004.
Url: http://csrc.nist.gov/publications/nistpubs/800-27/sp800-27.pdf at 2004/09/09.

[**NIST SP800-42**] John Wack, Miles Tracy, Murugiah Souppaya; "Guideline on Network Security Testing" NIST Special Publication 800-42, October 2003

Url: http://csrc.nist.gov/publications/nistpubs/800-42/NIST-SP800-42.pdf at 2004/11/10.

[**NIST SP500-172**] "Computer Security Training Guidelines", November 1989.

[**OSSTMM 2003**] Pete Herzog, "Open Source Testing Methodology Manual"; Institute for Security and Open Methodologies, 23 August 2003.
Url: http://isecom.securenetltd.com/osstmm.en.2.1.pdf at 2004/11/12.

[**SSE-CMM 2003**] Systems Security Engineering Capability Maturity Model, (SSE-CMM Ver. 3)
Url: http://www.sse-cmm.org/model/ssecmmv2final.pdf at 2004/09/13.

Surveys

[**CSI/FBI 2004**] CSI/FBI Computer Crime and Security Survey; Lawrence A. Gordon, Martin P. Loeb, William Lcyshyn and Robert Richardson, 2004 .
Url: http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2004.pdf at 2004/10/11.

[**ISS 2002**] 2002 Information Security Survey, KPMG; url at 2004/09/20
Url: http://www.kpmg.com/microsite/informationsecurity/iss_seclea_meaandrep.html

Web Sites

[**commoncriteriaportal.org**] The official web site for the Common Criteria Project. The document an be found under "Official CC/CEM Versions" link.

[**secmet.org**] The Official Site for the Security Metrics Consortium which targets to define the quantitative metrics for industry, corporate and vendor adoption.

[**insecure.org/nmap**] Site for the free open source utility for network exploration or security auditing.

[**gfi.com/lannetscan**] Site for GFI's commercial network security scanner tool LanGuard.

[**nessus.org/**] Official site for the Nessus Open Source Vulnerability Scanner Project.

[**atstake.com/products/lc/**] Site for the password recovery and auditing application by @stake.

[**openwall.com/john/**] John the Ripper is an OpenWall project password cracker. It's primary purpose is to detect weak passwords.

[**oxid.it/cain.html** This site refers to a password recovery tool dedicated to Windows operating systems.

Literature Overview

[**Anderson 2002**] Anderson, Ross , Security in Open versus Closed Systems, Cambridge University, England; 2002.
Url: http://www.ftp.cl.cam.ac.uk/ftp/users/rja14/toulouse.pdf at 2004/09/08

[**Cambra 2004**] Cambra, Rich; GIAC Security Essentials Certification (GSEC), "Metrics for Operational Security Control"; July, 2004.
Url: http://www.giac.org/practical/GSEC/Richard_Cambra_GSEC.pdf at 2004/10/18

[**Faile 2000**] GIAC Security Essentials (GSEC) Certification Practical Assignment, "Security Outsourcing"; Jonathan S. Faile December, 2000.
Url: http://www.sans.org/rr/papers/37/223.pdf at 2004/10/11.

[**Foundstone 2003**] Foundstone Strategic Security, Information Security Metrics - Using Foundstone's FoundScore to Assign Metrics and Measure Enterprise Risk, 2003.
Url: http://www.foundstone.com/resources/whitepapers/wp_securitymetrics.pdf

[**Gulati 2003**] GIAC Security Essentials (GSEC) Certification Practical Assignment, "The Threat of Social Engineering and Your Defense Against It"; Radha Gulati , Sans Institute, 2003
Url: http://www.sans.org/rr/papers/51/1232.pdf at 2004/10/11.

[**Robinson 2004**] Chad Robinson; "Collecting Effective Security Metrics" April 9, 2004.
Url: http://www.csoonline.com/analyst/report2412.html at 2004/12/10

[**Johnson 2001**] GIAC Security Essentials (GSEC) Certification Practical Assignment, "Successfully Managing Cyber Security"; James B. Johnson September 12, 2001
Url: http://www.sans.org/rr/papers/37/224.pdf at 2004/10/11.

[**Katzke 2003**] Dr. Katzke, Stuart , First Workshop on Information-Security System Scoring & Ranking, Information Assurance Solutions Group/ National Security Agency, 2003.
Url: http://www.acsac.org/measurement/ proceedings/wisssr1-proceedings.pdf

[**Lau 1998**] Lau, Oliver, The Ten Commandments of Security , Computers & Security, 17 (1998) pp. 119-123, Marburg, Germany, 1998