Developing a Risk Management System for Information Systems Security Incidents

A Dissertation

Presented to

The Academic Faculty:

by

Fariborz Farahmand

In Partial Fulfillment

of the Requirements for the Degree of

Doctor of Philosophy in Computer Science

College of Computing

Georgia Institute of Technology

Developing a Risk Management System for Information Systems Security Incidents

Approved by:

Professor Shamkant B. Navathe, Georgia Tech

Professor L. Jean Camp, Harvard University

Dean Richard A. DeMillo, Georgia Tech

Professor Philip H. Enslow, Georgia Tech

Mr. William J. Malik, Sun Microsystems

Professor Gunter P. Sharp, Georgia Tech

November 2004

To my mother and sister

Acknowledgements

It is difficult to compress into a few lines my gratitude to a number of people who have directly and indirectly contributed to this dissertation. I am particularly indebted to the members of my advisory committee.

However, I would like to start by thanking Professor Philip Enslow, whom I consider the father of this research. I benefited greatly from his keen insights. His constant and outstanding support for this research, my career and my life has been far beyond the call of duty and will never be forgotten. I am deeply grateful for everything which he did for me.

I would like to express my sincere thanks to Professor Shamkant Navathe for accepting the principal advisor role for this research after Professor Enslow's retirement. It has been a great honor to work under his supervision and benefit from his advice. His deep and enlightening guidance led me to astonishing ideas for this research.

I would like to thank Professor Gunter Sharp for his unceasing help and assistance over many years. He not only worked with me on this research, but he coached me into becoming a researcher. I am grateful for the long hours of our association, his hard work, and being the engine of this research.

I would like to thank Dean Richard DeMillo for his invaluable comments and for showing me how to include industry and academic values into my Ph.D. research. I am also grateful to him for financial support, which included the awarding of a Georgia Tech Information Security Center Fellowship. His support allowed me to travel nationwide to do the interviews that are integral to my research.

Many special thanks to Harvard University Professor Jean Camp for advising this research externally. I deeply appreciate her excellent comments on my research and the attention and support that I received from her.

I wish to express my deep gratitude to Mr. William Malik for opening the doors to important interviewees who gave me their input. His support made the real world interviews and case studies of this research possible. His vision and outstanding computing professionalism was an asset to this research and my career.

I want to thank Mr. Chris Klaus for allowing me to discuss my research with him during many meetings. His mentorship has helped me greatly in my research and in my career. I would also like to thank Mr. Tom Noonan, who along with other members of Internet Security Systems helped me with my research.

Also, I would like to send my thanks to the unmentioned government and private sector officials whose extensive interviews contributed to the case studies of this research. I would also like to thank to Georgia State University Professor Jack Williams and his student Ms. Sue Smith for assisting me with my WestLaw case studies research.

I would like to thank Georgia Tech Librarian, Ms. Pat Johnston, for being a friend, for her research assistance and for helping me to edit this dissertation.

I would also like to thank Professor Richard LeBlanc who helped me to get established in the College of Computing and Professor Dan Colestock who also helped me when I first came to the College of Computing.

I am grateful to Ms. Mary Alice Isele for her support in dealing with non-Georgia Tech executives. Ms. Linda Williams made my life easier by helping me many times throughout my years at Georgia Tech's College of Computing.

Most importantly, I would like to thank my family and especially mother and sister whose unconditional love, passion and trust have been the inspiration for this work which has been dedicated to them. Their lifetime encouragement, patience, and sacrifice were the key for all of my achievements.

Table of Contents

List of Tables

List of Figures

Summary

The Internet and information systems have enabled businesses to reduce costs, attain greater market reach, and develop closer business partnerships along with improved customer relationships. However, using the Internet has led to new risks and concerns. This research provides a management perspective on the issues confronting CIOs and IT managers. It outlines the current state of the art of information security, the important issues confronting managers, security enforcement measure/techniques, and potential threats and attacks. It develops a model for classification of threats and control measures. It also develops a scheme for probabilistic evaluation of the impact of security threats with some illustrative examples. It involves validation of information assets and probabilities of success of attacks on those assets in organizations and evaluates the expected damages of these attacks. The research outlines some suggested control measures and presents some cost models for quantifying damages from these attacks and compares the tangible and intangible costs of these attacks. This research also develops a risk management system for information systems security incidents in five stages: 1- Resource and application value analysis, 2- Vulnerability and risk analysis, 3- Computation of losses due to threats and benefits of control measures, 4- Selection of control measures, and 5- Implementation of alternatives. The outcome of this research should help decision makers to select the appropriate control measure(s) to minimize damage or loss due to security incidents. Finally, some recommendations for future work are provided to improve the management of security in organizations.

Chapter 1

Overview of Research

The exponential growth of internet-based commerce is threatened by legitimate concerns over the security of a system that has a large number of potentially vulnerable components. Despite the potential rewards of conducting business on the Internet, some corporations have been slow to embrace this technology. Perhaps the most important reason for both businesses and consumers to refrain from establishing and participating in electronic commerce (e-commerce) is the potential for loss of assets and privacy due to possible security breaches in such systems. For example, a single, highly-publicized security breach can erode confidence in the business and not only damage the reputation of the firm, but can cause widespread repercussions in the e-commerce industry.

Chapter two of this dissertation provides a perspective of today's business and information security and explains:

- The state of the art of security practice in businesses
- The nature of security threats, how to deploy information security programs that thwart those threats, and
- The need for continually supervising the performance of information security managers to assure that they are properly maintaining and upgrading their systems.

Chapter 3 discusses the author's opinion about the cost of computer security incidents and explains:

- The cost of a computer security incident to an organization has to be measured in terms of the impact on their business. Hence, identical incidents occurring in two different companies of the same industry or other organizations, like government entities, could have different costs.
- The process of quantifying these costs
- Empirical analysis of the existing available literature, indicating that the greatest amount of damage in terms of the financial/market evaluation of companies is caused by the violation of data confidentiality, and
- Incidents such as intrusion, when confidentiality of data is not compromised, typically results in direct damage such as denial of service. The cost of this kind of attack is directly quantifiable, but it is not as costly and as hard to quantify as the damage caused by the potential loss or disclosure of confidential information from other attacks.

Lack of statistics from past information security incidents, makes the probability assessment of upcoming attacks a very complicated task. Chapter four discusses:

- Subjective probability assessment as a possible solution for estimating the likelihood of an event
- Some of the shortcomings of this approach, and a scope for this assessment, and
- A quantitative approach for estimating the probability of the information systems security incidents using specific examples.

Regardless of all the existing countermeasures, statistics show that chances of computer security system failure are still very high. The Internet Fraud Complaint Center, IFCC (a partnership of the National White Collar Crime Center and the Federal

Bureau of Investigation) reports that there were16,775 complaints of fraud for the Jan. 1, 2001- Dec. 31, 2001 period. These frauds have caused serious tangible and intangible losses to the companies and e-commerce industry as a whole and are on the rise. The Center for Emergency Response Team, CERT, at the Carnegie Mellon University, reported that they have received 2,437 vulnerability reports in 2001 compared with 3,784 vulnerability reports in 2003. In 2001, they handled 52,658 computer security incidents compared with 137,529 in 2003. Chapter five includes:

- A literature review on existing classifications of threats and countermeasures
- Threats are broken down into two components: 1- Threat agent, and 2- Penetration technique. A security breach is caused by a threat agent using a specific penetration technique to produce an undesired effect on the network.
- Threat agents are classified into environmental factors, authorized users, and unauthorized users, and
- Techniques are classified into physical, personnel, hardware, software, and procedural.

This research has developed a five-stage risk management system to identify, analyze and respond to information systems security incidents. This risk management system, which is explained in chapter six, includes:

- Resource and application value analysis
    - Determine the sensitivity of information
    - Estimate asset values
- Vulnerability and risk analysis
    - Identify vulnerabilities

        - Weigh vulnerabilities
        - Assess threat probabilities
- Computation of losses due to threats and benefits of control measures
        - Review risk
        - Identify control measures
        - Assess changes in threat probabilities
- Selection of control measures
        - Enumerate search procedure
        - Use mathematical programming approaches
- Implementation of alternatives
        - Develop and approve a plan
        - Implement control measures
        - Test and evaluate

A quantitative method for selecting control measure is also discussed in this chapter.

Chapter seven of this research explains the case studies:

- Evaluating the accuracy of findings from the literature review
- Analysis of the source, classification, and importance of threats to information systems, and
- Assigning effective control measures to confront these threats which were evaluated by experts

The methodology included meetings, telephone conversations and e-mails with company executives and government officers.

Chapter eight classifies the contributions of this research to the information security industry:

- Defining a minimal set of elements to be considered in an effective information security program
- Comparison of intangible and tangible cost of information security incidents
- Adaptation of subjective probability assessment to empirical data and applying it to information security
- Classification of threats and control measures to information systems, and
- Developing a five-stage risk management system.

Broader impacts of this research in solving technical and business issues of information security have also been discussed in Chapter 8.

Finally, Chapter nine proposes some approaches for tradeoff analysis between the cost of security measures, versus incident rate/reliability/safety measures. Chapter nine also proposes some methods for measuring the effectiveness of control measures.

Chapter 2

Information Security: Practice and Threats in Organizations

Federal Standard 1037C (1997) [27] defines information security as: "The protection of information against unauthorized disclosure, transfer, modification, or destruction whether accidental or intentional".

Information security is an area in which interest is mounting rapidly. It is becoming widely recognized that security is a fundamental aspect of any information system and warrants high attention beginning with system design and continuing throughout the product lifecycle. Failure to properly address security requirements leads not only to operational risks but also to prospects of outright product rejection by customers. Currently, organizations are struggling to understand what the threats to their information assets are and how to obtain the necessary resources to combat these threats. Acquiring the appropriate human and financial resources to offset the growing threats to information security continues to pose a challenge to many organizations. Information security includes many subjects, from high level principles and policy right down to the very detailed calculations in encryption algorithms.

Chapter two discusses the current state of the art in business information security practice. This is followed by a discussion on the nature of security threats and deploying resources in information security by business managers.

2.1 The State of the Art of Security Practice in Businesses

The vast majority of businesses deploy their information security programs in a piecemeal and poorly integrated fashion. In an ideal state, the security governance function is managed by a senior executive who reports on the overall state of the information security program to a committee of the senior leadership team. Once that program is established, the noteworthy elements of this report will be exceptions and upcoming changes to the initial report. The information security policy will be brief but comprehensive; not mixing procedural details or instructions for specialists with the general guidelines, goals, and expectations outlined for users. The information security architecture will translate policy directives ("we will keep customer information private") into detailed platform-neutral directives ("users must authenticate themselves with a unique password that is changed at least every 90 days").

Most organizations are running some form of "awareness program" to enable employees to become aware of the organizational security policies. The awareness program includes an introductory module for new hires covering the information security program as well as details on how to recognize and report a problem. Employees and contractors are given a second module covering updates to the information security program upon taking a new assignment, or after there are substantial changes in the environment. Every employee attends an update seminar of a few hours annually.

Information security products and tools are acquired through a formal Request for Proposal (RFP) process that is governed by an ongoing gap analysis assessing the variance between policy requirements and platform capabilities. Such tools are only deployed after a policy statement governing their use and goals is developed by the chief

information security officer, who also owns responsibility for the architecture. When an information security event is suspected, a cyber emergency response team (typically a virtual team made up of a few specialists in key IT areas) acts quickly to review logs, configuration information, and assess damage. Normal requests for access (new, changed, or deleted) are processed through an automated provisioning system. Password change requests are handled by self-service capabilities. Finally, as part of an annual audit, the entire information security program is revalidated against changes in the technology, marketplace, risk profile, work force demographics, and business structure.

Businesses typically deploy a subset of the elements of an effective enterprise-wide information security program. Large, publicly traded firms recognize some obligation to their investors and recognize the potential for: 1) Damage to their brand and reputation, 2) Legal and regulatory risk, and 3) Adverse financial consequences from an information security breach. The next tier of firms tends to be much less coordinated and much more informed with respect to their information security programs, relying on the talents of one or two information technology specialists who use their experience and contacts to deploy what, in their individual opinion, constitutes an appropriate set of control measures. The vast majority of smaller firms may do little or nothing to preserve or protect their IT environment. Spending on information security, not including disaster recovery, typically amounts to less than three percent of the IT budget, according to statistics developed by The Gartner Group. Those elements of the information security program that are deployed, find their funding justified only in response to a specific crisis such as: antivirus in response to a virus incident or firewalls in response to an internet deployment issue. An awareness and training program may feature one anecdote

concerning a recent problem that was dealt with after the fact rather than with a coordination policy devised before the problem occurred. As a result, there were no lessons learned to enrich the corporate culture. For the majority of businesses, there may be no awareness of the scope of the vulnerabilities they face, and often there may be no awareness of security breaches as they occur.

From business schools, professional managers learn what ought to be done to mitigate the risks of an information security breach, just as learning how to structure clear and effective management processes. However in the rough and tumble reality of day-to-day business, these lessons often get lost. It consumes resources to fully document procedures, review apparently completed work, deploy additional security measures, reset adequate default passwords, remove unused system ids, or apply patches to problems that have not been actually experienced.

Too often businesses focus on near-term tactical issues and ignore the strategic implications of such decisions. When a dominant firm in a particular geographic region or industry deploys an effective and integrated information security program, thereby lowering costs, reducing occurrences of unplanned outages, and enhancing brand and image, some competitors begin to see how such benefits could be theirs as well. Similarly, businesses understand that clearly documented processes allow for improvement in auditing, and training; but the reality is that few businesses actually document even their core procedures very well. Most managers understand that wasted time, effort, resources and product is costly; yet few are willing to invest the effort to perform a comprehensive survey of their processes to analyze and eliminate waste, redundancy, and delay. During the 1960s, American industry embraced the notion of

quality as a separate and distinct initiative. Major manufacturing firms designated senior managers as "Directors of Quality" and charged them with reducing product defects. These unfortunate individuals were totally ineffective because they lacked the organizational clout to modify existing business processes. The standard process of design, development, manufacturing and field maintenance continued unchanged. The finding from these failed initiatives was that quality is not an independent variable in the manufacturing process.

Eventually, we learned that quality is an aspect of the product development life-cycle. In other words, the quality of a manufactured object is an intrinsic element of the method of the object's manufacture. Quality is not like paint; it cannot be added on after the object is finished. Similarly, we are beginning to learn that information security is not a separate discipline from information technology. Information security is an aspect of how information technology is specified, designed, developed, deployed, and maintained. A comprehensive information security program has to be deeply integrated with the system throughout its lifecycle. The information security characteristics of an information technology environment are a consequence of its architecture, design, development, deployment, operations, and maintenance. Information security cannot be added on after an information technology environment is deployed. Information security is not a property of a product; it is a property of an environment.

2.2 The Nature of Security Threats

One useful model of the information security problem is to define three classes of objects. First, firms have intellectual property that represents value and therefore brings

risk of several forms to the firm. Second, that intellectual property is embodied in a technology environment that is imperfect which exhibits design flaws, trade-offs, defects and obscure documentation. Third, there is an individual, inside or outside the firm; who for some reason or another, wishes to exploit those technological or procedural weaknesses with the goal of damaging or transferring the value of that intellectual property. What kinds of individuals might do this? At a high level, there are two traits of some relevance.

First, the level of technical skill of the attacker, and second, the level of insider knowledge the attacker might have. An unskilled outsider may represent a low-grade threat; someone who might steal a laptop opportunistically and sell it. An unskilled insider actually represents a fairly significant threat. Because by knowing the procedures; such a person can exploit weaknesses in the design of a system without having to modify sophisticated algorithms.

Skilled outsiders (quadrant 1 in Figure 1) are the notorious hackers; of which there are only a few hundred in the world. However these individuals develop toolkits so hundreds of thousands of less skilled users can leverage the skill of the hacker to attack a broader range of sites. These individuals are dangerous, but until now most of their activities have been unguided. However, there is reason to believe that malevolent organizations are making contact with hacker groups to cultivate relationships. It is easy to believe that hackers are more likely to attack someone else; in fact, attacks are generally random and the technically skilled insiders (quadrant 2 in Figure 1) represent the most dangerous threat. However, they are rarely caught and represent a very small

population. Procedural remedies; surveillance, audit, job rotation and so forth; allow the firm to minimize it's exposure to this particular problem.

This could be shown graphically as a two × two matrix with skill level as the vertical axis, and inside knowledge as the horizontal axis shown in Figure 1. Quadrants three and four refer to low-skilled insiders and outsiders who are typically not involved in information security related incidents in a major way.

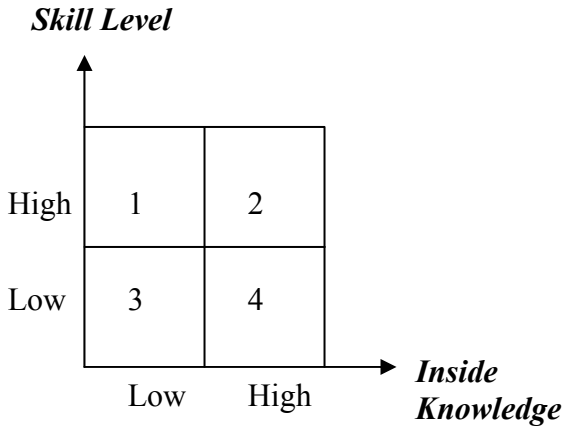

Figure 1- Skill Level- Insider Knowledge Matrix

In general, insiders (in quadrant two) are responsible for most financially significant information security problems. Federal Bureau of Investigation/Computer Security Institute, FBI/CSI, 2002 report which indicates that 78% of respondents to the survey have reported insider abuse of net access [54]. Therefore, firms must acknowledge that people with inside knowledge are a significant source of attacks, and structure their business processes and technology deployment to account for that fact.

2.3 Deploying Resources in Information Security

Unfortunately, most firms do not have a transparent, repeatable process for determining when or how to deploy resources (money, staff, and time). At the senior management level, information security is often perceived as simply another of the systems management disciplines, requiring either a code patch or a software tool to fix the underlying problem.

Such piecemeal approaches fail because they usually are driven by the haphazard occurrence, the most recent event, or the most recently publicized threat. A series of uncoordinated activities focused on fixing discrete problems alone, will leave gaps that will be exploited easily. Some larger organizations that have more experience with information security have chosen to deploy a comprehensive information security program. While there is no generally accepted model for such an initiative, the common elements are:

Governance – Translating business value and mission statements into principles relevant to information security

Policy – A clear, direct, concise high level statement of desired behavior and expected controls for users of an IT environment

Architecture – Translates the policy directives into platform neutral, low level actions (such as the ISO 7498-2 security functions)

Awareness and Training – Insuring that the staff are aware of management's expectations and procedures to follow

Technology – Selection, deployment, operation and continuing evaluation of tools to amplify the directives in the policy

Auditing, reporting and monitoring – Detection through an ongoing examination of the output from tools and processes for forensic and analytical purposes

Validation – As the environment changes, the prior steps are adjusted to maintain their relevance and effectiveness

Deciding how much to spend on an information security program should be driven by the magnitude of the risk the firm acknowledges. If the firm has developed some sense of the value of its intellectual property, then spending can be governed by attempting to mitigate the largest realistic risks first. While piecemeal approaches will always fail, approaches governed by both a comprehensive model like this (or the Control Objectives for Information and related Technology, COBIT, model, or the principles included in ISO 17799/BS 7799) as well as a sense of the magnitude of the risk the firm faces will make strategic sense over time.

Firms rarely overspend on information security. One approach, used by a few large financial institutions, is to marry the Software Engineering Institute's Capability Maturity Model, SEI CMM, with the processes outlined in the COBIT model, and assess the relative maturity of the organizational processes. This is described in the ISACA (Information Systems Audit and Control Association) web site http://www.isaca.org. The purpose is to develop a gap analysis that can help guide resource commitment, not by attempting to identify the most likely expensive risk (and address that), but by strengthening the weakest element of the information security program.

2.4 Security Standards and Overview of Common Criteria

Security standards ensure that individuals operate consistently to minimize risk and to make administration of systems and networks more efficient [66]. Standards can set a level of expectation that must be reached or exceeded in order to fulfill one's obligation or responsibilities. Standards can also have a large impact on implementation of security technologies. When standards have not been taken into consideration related to technology implementations, they may impact the amount of energy or support required to meet the security objectives of an organization and consequently have an impact on both cost and the amount of risk.

A literature review has identified the following organizations and groups which have contributed in developing standards for information security:

BSI: British Standards Institute

CERT: Computer Emergency Response Team

CSTC: Computer Security Technology Center

EDPAA: Electronic Data Processing Auditors Association

FACCI: Florida Association of Computer Crime Investigation

FIRST: Forum of Incident Response Teams

GASSP: Generally Accepted Systems Security Principles Subcommittee

HERT: Hacker Emergency Response Team

ICAT: Initiatives for Computer Authentication Technology

ICSA: International Computer Security Association

ISO: International Organization for Standardization

NIST: National Institute of Standards and Technology

NSA: National Security Agency

Information Assurance Technology Analysis Center

International Information Systems Security Certification Consortium

Network Security International Association

San Diego Regional Info Watch

The Common Criteria for Information Technology Security Evaluation, usually referred to as "CC", was initially developed in 1993 as an international standard to support developers, evaluators, and consumers of security products. The part of an IT system or product which should be evaluated, based on the CC, is called the Target of Evaluation (TOE) and has to fulfill different security requirements which are verified by an evaluation authority [68].

The security requirements of the CC are divided into security functional requirements (requirements on the product) and security assurance requirements (requirements on the process) and are structured into classes, which are described in the following section. All the members of a class share a common focus, while differing in coverage of security objectives. The functional requirements are realized in the functions of the system in order to achieve the security objectives of the TOE. The assurance requirements contain measures to be undertaken during development in order to keep the risk for weak points low. They are necessary for guaranteeing the confidence that the TOE meets its security objectives. The number and strictness of the assurance requirements to be fulfilled depends on the Evaluation Assurance Level (EAL) one has chosen for the TOE.

The following contains measures and products independent of a chosen EAL which are important for a development based on the CC. The listed products belong to the different assurance classes of the CC:

Security Target (class ASE)

The Security Target (ST) is the core document of system development based on the CC. It contains the security analysis for the TOE. First, the developers have to describe the TOE and its boundaries briefly in the ST. Additionally, they have to define the assets of the TOE and the threats against the assets. The ST also must contain the security objectives corresponding to the threats. In order to protect the assets, counter the threats and ensure the security objectives, the developers have to define control measures. These control measures are specified by the security technical requirements and the assurance requirements of a TOE. The functional requirements are chosen from the second part of the CC or are defined conformable to the CC. The assurance requirements result from the determined EAL. The ST is concluded with a TOE summary specification, describing the security functions of the TOE.

Configuration Management Plan (class ACM)

All assurance requirements concerning the configuration management should ensure that the integrity of the TOE is preserved. Developers have to write a configuration management plan that contains a description of the configuration management system used in the project.

Design and Representation (class ADV)

The assurance requirements about design and representation require correct and consistent specifications and designs on different levels of abstraction and formality (e.g., a semiformally specified high-level design).

Life Cycle Documentation (class ALC)

The assurance requirements for the life cycle support are important for the controlling of the development and maintenance of the TOE. For example, in this class there are requirements on the documentation of development tool usage.

Test Documentation (class ATE)

In this class all assurance requirements belong to test activities like test documentation, test depth and extent of testing. Test activities are used to validate that the TOE satisfies all security functional requirements defined in the ST.

Vulnerability Assessment (class AVA)

Activities concerning this class correspond to an analysis of the vulnerabilities (design-specific weaknesses) of a system.

Guidance Documents (class AGD)

The CC contains assurance requirements which refer to the content of the user and administration guidance. Both documents have to be understandable, consistent and complete. The aim is to show users and administrators how to operate with the system and its security functions in a secure manner.

Delivery and Operation Documentations (class ADO)

The CC contains assurance requirements to ensure the security during delivery, installation, start-up and operational use of the TOE.

The major strength of the CC Process is that it offers a common IT security language and attempts to measure both process and result. This also makes it a good candidate for predevelopment of certification and accreditation. However, there are several obstacles to the CC paradigm's long-term survival.

A lack of widespread government and commercial-sector use of CC evaluated products can be mentioned as an example. Literature review indicates that even among informed and concerned communities, many users do not care about evaluations; others, want a mark of approval but do not really care what the mark represents [35]. Another significant obstacle is the concern about the comparability and competency of evaluations. Conflicts between international harmonization and national investments could be especially significant if major European nations and the United States continue to follow increasingly divergent paths as they pursue the founding member nations who were able to work through their differences to produce the CC and the CC Recognition Arrangement (CCRA). Living with the results proves once again that "the devil is in implementation details".

Chapter 3

Costs Resulting from Information Security Incidents

3.1 A critical overview

A physical breach of security involves actual damage to, or loss of the computer hardware or media on which data are stored. A logical breach affects the data and software without physically affecting the hardware. Literature review reveals a stream of research on the cost of information systems security incidents [2, 8, 17, 20, 50, 65]. One of the problems with any logical breach of security is that the damage is invisible and its extent is unknown. This causes serious difficulties for managers to justify their investments on security. A simple approach for finding return on investment is calculating:

[(Change in revenue) + Cost saving)] / [(Investment)]

However, these parameters are hard to determine. Decisions about return on security investment will not start to make sense until one can replace these parameters with numbers. Literature review has also revealed that, by theoretical means, one can demonstrate that optimal level of investment in security-related activities should not exceed approximately one third of the potential expected loss [32].

It is also argued, that a cost effective analysis is the preferred alternative when costs and benefits are not commensurate [30, 49, 50]. Effectiveness is more tractable because it does not ask the price of events. Instead, it asks, "What is the most one can get for $X, given that he is inevitably going to spend $X?" In other words, it is about

maximizing the effectiveness of an expense in pursuit of a benefit not easily valued. Some factors which are considered in this approach are:

- Value linking- It is used to evaluate the combined effects of improving performance of a function and any consequential affect which results from a separate function.
- Value restructuring- It addresses the values associated with restructuring a job of a department function (it measures the value of productivity increases resulting from organizational changes)
- Innovation- It creates new functions within the business domain.

Although this approach is not the solution to analysis of investment on security and a replacement for traditional cost benefit approach, it directs security mangers in the right directions.

It has been suggested that a composite cost/benefit/risk methodology is appropriate for managers in their financial decision making [46]. To calculate Risk Score by this approach, one should multiply:

Consequences: Most probable result of the potential threat,

Exposure: The frequency of occurrence of the threat, and

Probability: Likelihood that threat sequence will follow to completion

Another factor to be calculated is the Prevention Score, which is the product of: Cost Factor (The cost factor of proposed control measures; a number between1-10), and Degree of Correction (The Degree of Correction that the proposed control measure provides for that threat). By dividing Risk Score into Prevention Score, one can calculate the Justification Rating. This Rating can be used as an index for managers in allocating

budgets to security threats. For example, a Justification Rating greater than 200 requires immediate correction; 100-200 requires attention as soon as possible, and less than 100 means that the threat should be eliminated, but situation is not an emergency.

The literature review also reveals a school of thought that promises economic reasoning as a solution to security issues of information systems [5, 55]. For example, the success of firewalls is not because of their effectiveness, but because auditors started demanding firewalls, and this fact could change the cost equations for businesses. The cost of adding a firewall incurred expense and user annoyance, but the cost of not having a firewall was failing an audit. This theory explains that monetizing security can solve business and technical problems for the information security industry. It provides information about both losses and product effectiveness, which are the prerequisites for the formation of a viable security market.

3.2 Insurance & Risk Mitigation

About 85 percent of the U.S. information infrastructure is controlled by the private sector. The private sector is highly influenced by the insurance industry, which plays a major role in decisions made by executives in the private sector. This research also considers the potential impact of insurance on decisions which managers make about information security incidents. Literature review reveals some attempts in identifying the role of the insurance industry in internet security [33, 56, 64].

Insurance companies claim that their coverage includes: 1- Web content liability, 2- Professional liability, 3- Network security third party liability, 4- Intangible/information property loss, 5- Loss of revenue, and 6- Cyber extortion [28].

However, the insurance companies' statements of paying claims for this coverage are questionable [33]. The insurance companies have also been questioned for their complicated policies [36]. The results of author's interviews with law enforcement agencies and executives in private sector also confirm that the private sector is willing to work with the insurance industry in protecting its information assets. However, ambiguity of policies and difficulties with pricing are a major burden to this partnership.

This author argues that a trade-off exists between the amount a firm should invest to protect against possible security breaches and the amount it should spend on cyber-risk insurance. For a given level of information value-vulnerability, higher levels of security protection will require lower levels of cyber-risk insurance and vice versa. When allocating resources to lower the overall risk exposure to an acceptable level, the trade-off between investing to reduce the probability of security breaches and investing in insurance to reduce the financial losses (should breaches actually occur) should be viewed in cost-benefit terms. This cost-benefit tradeoff between reducing the risk of security breaches and buying insurance will also affect the level of residual risk (that is, the remaining risk after taking steps to protect and insure against security breaches) deemed to be an acceptable level.

3.2.1 Liability Issues

Avoidance of legal liability is cited as a reason for improving information security [58]. Organizations often find themselves in possession of confidential or proprietary information belonging to third parties with whom they have no formal agreement. If that information should be somehow lost or stolen, thus causing injury to its original owner,

the organization may be liable. Under the strictures of tort law, the somewhat vague standard of the "reasonable man" is used to judge liability of negligence. In United States vs. Carroll Towing Company, 1947, Judge Learned Hand [42] articulated a formula that has gone on to become one of the defining tests of negligence.

Let:

P = Probability of injurious event

L = Gravity of the resulting injury

B = Burden, or cost, of adequate precautions

then, the accused party is negligent if and only if $B < PL$

The cost of avoiding an accident, and the expected cost of the accident, must be compared at the margin by measuring the costs and benefits of small increments in safety and stopping investing in more safety at the point where another dollar spent would yield a dollar or less in added safety. Thus, the threat of legal liability creates an incentive for organizations to collect the necessary data to justify their information security policies with credible assessments of risk.

Competitive market forces are probably the last great engines of change that will force companies to protect their information assets efficiently. Regardless of the risk-management strategy pursued, whether it is an annual loss expectancy assessment, scenario analysis, best practices, or some other strategy, the marketplace will ultimately govern whether that strategy was an efficient use of resources. Those companies that secure their assets cost-effectively will gain a competitive advantage over those who do not. Thus, businesses that over-protect will have spent too much on security, and those that under-protect will suffer greater losses as a result of ensuing security breaches [53].

3.2.2 Information Systems Disasters

An information system disaster can be defined as: "An event which causes the loss of the communication services, or of a significant part of it, or of systems, communications or applications for a length of time which prevents the impacted organization from achieving its mission or which imperils the business" [38]. The impact may be felt in a number of different ways:

- Existing customers may transfer business elsewhere, and prospects may not be converted into new customers.
- New business is strangled; even loyal customers quickly become disaffected and hard-won market share drops.
- The organization's image and credibility may be damaged beyond recovery.
- Cash flow goes into reverse as creditors seek immediate payment and debtors defer settling bills knowing that credit control systems are not available to purse them.
- With the loss of production and financial control systems, costs run out of control.
- Inventory costs mount and inventory management becomes erratic.
- The share price may slump, reducing collateral and making the company susceptible to bank action such as withdrawing loans.

According to the Gartner Group, two out of five companies that experience a catastrophe, or an extended system outage never resume operations; and of those that do, one-third go out of business within two years [21].

In the era of information systems and distributed computing, most businesses no longer have the luxury of several days to fix a problem. In fact, most critical

applications, like those used in e-commerce and customer service, usually require continuous availability or the recovery of data and critical applications in minutes and at worst, several hours. Some organizations go so far as to stipulate that no transaction can be lost in the event of failure.

These facts lead us to the conclusion that every company must be prepared for recovering from possible disasters. The object of disaster recovery is not to eliminate risk, but to manage it. A disaster recovery plan should comprise several elements:

- Immediate reaction procedures
- Restoration of the computing infrastructure
- Restoration of the applications
- Resumption of business processing under emergency arrangements
- Restoration of the permanent computing service.

It is also mentioned that the best planning looks to diversification as a strategy for protecting an organization even with a direct disaster hit [46]. Diversification does not mean creating back ups and hot sites, but creating an infrastructure for control and coordination. This would enable all assets allocated to disaster recovery to be used all of the time and to be reallocated in the event of a disaster.

3.2.3 Working with the Insurance Industry

Traditionally, companies are willing to work with insurance companies to deal with risks of running their businesses. The following are mentioned as the criteria of insurability of internet risks [34]:

- Fortuitousness. This criterion demands that the event causing the case be unknown and not subject to influence at the time of conclusion of the contract. On the Internet, damages mainly result from deliberate attacks of third parties or technical defects. However, the possibility of the intentional creation of a damage event by the insured to get insurance benefit may never be ruled out. In order to eliminate the incentive for the insured to intentionally cause damage, or to neglect security measures, insurers apply specific obligations and components in the contract.
- Unambiguousness. This stipulates that the event (the damage occurrence) as well as the amount of damages be ratable in an objectively verifiable way. In practice, the exact interpretation of occurrence of damage and the amount of damages that must be compensated by the insurance benefits require many insurance clauses. These clauses have to be agreed upon by the signatories before the conclusion of the insurance contract.
- Estimability. This criterion represents the problem of insufficient knowledge. For internet risks there is not enough statistical data upon which to base the decision to assess the damage. An insurer, who has to estimate the average amount of damages, as well as the probability of the occurrence of the event, will judge subjectively. Likewise, the decision as to what extent a risk is basically insurable for the risk bearer will be subjective.
- Independence. This refers to positively correlated risks. These should be excluded so as to ensure a process of fortuity of the insured damage events of the business in force. Negatively correlated risks are preferable and therefore not

considered any further. Sufficient stochastic independence of the single risk is the central prerequisite for the effect of a collective portfolio balance. If the majority of the insured suffered damages at the same time, then the individual cases no longer represent independent events. Virus attacks, shortcomings or bugs of widely spread software can be cited as examples which cause highly correlated damages. Denial of service attacks can also entail an accumulation of damages. Such accumulation of damage, endanger the solvency of the insurer, which means that high payments are due all of a sudden; far exceeding the individual capacity limit of the insurer.

- Size. The criterion of size refers to the highest possible risk of damage in an individual occurrence. The size of the risk to be insured is a criterion that can be quantified with great difficulty only. This is due to the fact that the insurability depends on the underwriting capacity of the insurance industry, or the underwriting policy of the insurer. However, the maximum damage can always be restricted by limiting the coverage. In addition, the insurer can extend the underwriting capacity by means of re-insurers.

In response to Dr. Grzebiela's concerns in working with insurance companies in dealing with risks of information systems security incidents, and in some cases disasters, this author identifies three approaches to be taken by managers [22]:

1- Accepting the risk as a cost of doing business; some do and some do not. For example, some companies accept the risk of someone eavesdropping on credit card transactions and they only provide encryption if the customers request it.

2- Transferring the risk entirely to an insurance company. There are a large number of well-established insurance companies that insure internet risk, despite the mentioned difficulties: AIG, Cigma Property and Casualty, ICSA, J & H March, LIoyds, Reliance National/NRMS, Zurich Financial Services Group.

3- Accepting some of the risk and transferring its proportionate cost to the cost of implementing control measures and expected cost of the incidents

This research recommends the third approach as the most cost effective one in working with the insurance industry. Implementing effective control measures not only reduces the probability of information systems incidents and possible disasters, but will have a tremendous impact on lowering the premiums and transferring the remaining risks to insurance companies. In upcoming sections, this research provides some methodologies to assign probabilities of incidents, evaluating their costs and choosing cost-effective control measures in confronting these threats.

3.2.4 Limiting Cases

If the probability of the occurrence of an incident is considered as one out of one, meaning that a specific threat will definitely occur, then the benefit of a control measure will be reflected in its effectiveness in reducing the damage. This approach is used in the risk management system presented later. Another viewpoint is to define a shorter time period of interest so that the probability of the threat occurring is less than one out of one.

3.3 Cost of an incident

Dr. DeMillo and Dr. Dobkin explained that**: "**…The design of systems sufficiently secure with respect to such penetrators will perhaps never be achieved. One can only hope that the cost of compromise [benefits of penetration vs. cost of protection] will increase to exceed the possible benefits that could be derived from such a compromise [18]".

Every company, no matter what size, must be able to understand the financial costs involved when its security is breached. But what is a loss? Cohen [16] states that: "A complete list of things that can go wrong with information systems is impossible to create. People have tried to create comprehensive lists, and in some cases have produced encyclopedic volumes on the subject, but there are potentially infinite numbers of different problems that can be encountered, so any list can only serve a limited purpose".

The cost of a computer security incident to an organization has to be measured in terms of the impact on the business; hence identical incidents in two different organizations of the same industry or business type could have different costs. The impact may well be financial, in forms of immediate costs and losses as was briefly explained before, but much more serious are the hidden costs. For example, a computer security incident might damage an organization in terms of the following intangibles:

- The brand image, public reputation and goodwill in the market place
- The financial value of business transactions
- Public and customer confidence in the accuracy of business transactions
- Public and customer confidence in the fraud-resistance of business transactions
- The ability to maintain revenue cash flow in a timely manner
- The ability to resolve disputes beyond reasonable doubt

- The ability to meet the requirements of regulators

In this section, we discuss how identical incidents can have different impacts on different companies; an approach for quantifying costs of incidents, and; the importance of intangible damages that can be caused by an incident.

3.4 Variability of Losses Resulting from Similar Exploitation

When a firm experiences an information security problem, the consequences to the firm can vary dramatically from instance to instance. When two firms experience the same incident, one may be able to contain the damage, while the other may not. One may have effective backup procedures allowing the evidence to be used for a prosecution, while the other may face a difficult choice between resuming operations (by refreshing the environment) or supporting an investigation (by allowing systems to be sequestered, check-pointed, and analyzed). One firm may have an effective liaison with its information security vendors and outsourcers, while the other may not. One may have properly tuned intrusion detection tools and able staff, while the other may not. One may have rigorous screening of candidates for key positions, while the other may not. One may have an effective awareness program, while the other may not. One may truly support the culture of security, while the other may only provide occasional support, but no enduring commitment.

Even with similar overall structures, firms never have similar configurations at the detailed, operational level. As a result, an incident may barely impact one firm while another similar firm may be overwhelmed with consequential damage. This happens often when firms experience a virus attack. Seemingly minor configuration differences

may allow a particular virus to spread rapidly in one firm, while a similar firm notes the event but does not suffer greatly from it.

Following a privacy violation, one firm might face vigorous prosecution from authorities in one jurisdiction, while a similar firm in another jurisdiction might not face any investigation at all.

The simple fact is that the consequences from an information security breach are contingent on a vast number of factors, many of which are not under the control of the firm experiencing the breach.

3.5 Quantifying the Cost of Security Incidents

Before quantifying the damage that can be caused by an incident, managers should know the value of the assets of the organization that are exposed to the threat. Logical and physical assets can be grouped into the following categories:

1- Information − documented (paper or electronic) data or intellectual property used to meet the mission of an organization.

2- Software − Software applications and services that process, store, or transmit information.

3- Hardware − Physical devices for computing, communications and storage

4- People − The people in an organization who posses skills, knowledge, and experience who are difficult to replace.

5- Systems − Information systems that process and store information (systems being a combination of information, software, and hardware assets, and any host, client, or server being considered a system).

For example, the cost of downtime per hour caused by a denial of service attack can be computed by measuring the loss in the following categories:

- Productivity

  (Number of employees impacted) × (Hours out) × (Burdened hourly rate)

- Revenue

  Direct loss, lost future revenues

- Financial Performance

  Credit rating, stock price

- Damaged Reputation

  Customers, suppliers, financial markets, banks, business partners, etc

- Other Expenses

  Equipment rental, overtime costs, extra shipping costs, travel expenses, etc.

This author, with the assistance of his colleagues at the Georgia State University, has also reviewed the cybercrime cases through Westlaw. Westlaw is West's online legal research service. It provides quick, easy access to West's vast collection of statutes, case law materials, public records, and other legal resources, along with current news articles and business information. The following searches found the most useful cases for this study: "18 u.s.c." /2 1030 /s fraud; "18 u.s.c." /2 1030 /p evaluation /p damages; "18 u.s.c." /2 1030 /p damages; computer /1 crime /p fraud; computer /1 crime /p fraud /p damages. Information such as case holding, facts, nature of company, type of incident, category of incident, total amount of damage, number of victims, income of victims, and statements made by expert witnesses, were analyzed from more than twenty cases. The result of these cases were similar to results of the Incident Cost Analysis and Modeling

Project, ICAMP, [15] where thirty information security incidents from universities across the nation were investigated. This author [25], and the final report of ICAMP, both acknowledge that the value of intangible damages in many cases could be considerably more than the tangible damages, such as downtime cost. However, despite their importance, they are missed in investigations because of the difficulty of calculating the intangible cost.

In the category of assets, one through five mentioned above, information assets are the most difficult group to assess. Information values can be derived by looking at three cost areas [19]. The first is replacement costs, which occur whenever information resources are destroyed, damaged, contaminated, or physically stolen. These costs are a function of readily discernible marketplace variables, including costs to purchase, transcribe from public resources, collect and reconstruct data. The second area is unavailability costs, which accrue whenever information resources are not available for a period of time; either because they were destroyed or stolen, or because they were sufficiently damaged, or contaminated as to be partially or completely useless. Those costs are estimated by considering time intervals beginning from the point in time when the asset becomes unavailable and ending at the point when it becomes available. They can include: staff overtime; attrition and training; idled staff; facilities and resources; inability to pay bills or pay clients; deliver products and services; lost interest or borrowed money; costs of using alternative resources; potential for fraud and abuse; legal, regulatory, civil, and criminal properties; litigation expenses; and reduced market share, customer goodwill, credit rating, and stock values. The third area is disclosure costs resulting from braches of confidentiality. Costs in this category could result from

lost market share or competitive advantage, blackmail, legal, regulatory, civil and criminal penalties, litigation expenses, and impact on credit rating and stock values. An information asset could be subject to losses in multiple categories. The associated costs are added if they represent distinct losses.

One approach to combining tangible and intangible losses is to use scoring tables, as shown in Tables 1 and 2:

Table 1- Example of a scoring table for intangible damages

Intangible Damage	**Valuation Score**
Embarrassment restricted to within the project or work site	1
Embarrassment spread to other work areas of operating group or division	1-3
Embarrassment spread throughout the enterprise	3-5
Public made aware through local press coverage	5-7
Adverse national press	7-9
Major stock price impact/bankruptcy	10

Table 2-Example of a scoring table for financial losses

Intangible Damage	**Valuation Score**
Under $1M	1
Between $1Mand $4M	1-3
Between $4M and $16M	3-5
Between $16M and $64M	5-7
Between $64M and $256M	7-9
Between $256M and $1B	10

Table 1 defines valuation scores for intangible damages that might be caused by an incident, and Table 2 shows the financial loss table for these valuation scores. The values found in the tables could be derived from meetings with experts from the various departments and business units within the company. For example, one can assign the valuation score of one to an attack to a company's intranet. With the probability of 0.2, the expected intangible damage of such an attack for the company with the gross annual revenue of $1billion, will be $200,000. To select cost-effective control measures, one may calculate the total expected damage of 220,000 by adding the intangible damage and the $20,000, which is the direct cost of the downtime of the network valuation scores. These valuation scores will be described in Section 6-2-4.

Calculating the Expected Cost of an Incident

The expected cost of an incident can be defined as:

$$EC = \sum_{i=1}^{n} AP_i \times C_i$$

Where EC is the total expected cost of the incidents, AP_i the assessed probability of the occurrence of incident i, and C_i the cost for damage caused by incident i. For example, an unauthorized person might access the credit card numbers of clients of a financial institution. This can cause total tangible and intangible losses of $15 million to the institution. A probability of 5 percent for the occurrence of this threat results in an expected damage of: $15,000, 000 × 0.05 = $750,000.

It is difficult to come up with exact probabilities of information security incidents. Therefore, there is a need for a practical methodology to quantify such probabilities. This research has outlined a procedure for evaluating possible losses due to security incidents

based on the use of questionnaires and answers given on scales of "very high" to "very low." This procedure can form part of an overall risk assessment model that enables security managers to allocate resources in the most effective manner, as presented in upcoming sections.

3.6 Analysis of Cost of Security Breach Announcements

The relationship between information system security and market valuations can be traced to the trust placed by customers and partners who do business with the firm through the Internet. Customer and partner trust assume more significance in electronic commerce transactions because of concerns related to data privacy. A security incident can irrevocably damage the trust and confidence required to build a long-term relationship with customer and partner. Dissatisfied customers can switch to competitors that are just a click away. Thus, a perception of low security can have a profound financial impact on the firm. Security problems may also signal to the market a lack of concern for customer privacy and poor security practices within the firm. These signals in turn lead investors to question the long-term performance of the firm. In efficient capital markets, investors are believed to revise their expectations based on new information in announcements. Investor confidence is reflected in stock prices. If security breaches are expected to reduce future cash flows, capital markets would respond unfavorably to announcements of security breaches by driving stock prices down.

This author has also explained the relationship between:

- Confidentiality of data
- Trust, and
- Some initiatives made by the U.S. government to establish such a relationship

This author also addresses the challenges of establishing these relationships [23]. Personal data protection is based on the defense of the right of privacy. This is a key concern for internet users, who may be wary of the possible misuse of their personal data by companies or institutions. Accordingly, it is essential for any organization wishing to enhance its credibility with potential consumers or users, to establish an effective data protection policy and to show a clear interest in respecting relevant regulations. Providing confidentiality of data is crucial in building trust for citizens to interact with the government via the Internet.

As an effort to build this trust and provide data confidentiality, the U.S. government has created several interrelated initiatives [9]. The first is the creation of a public-key infrastructure (PKI) through the government-wide Access Certificates for Electronic Services (ACES) program. The Federal Bridge Certification Authority (FBCA), which enables interoperability among PKI domains, and the e-authentication, which begins by providing authentication services to 22 U.S. e-government initiatives, are other U.S. government plans for assuring data confidentiality. PKI seems to be a proper security model for e-government transactions and for overcoming the lack of trust for on-line transactions, however, there are still some challenges.

First, in order to develop an interoperable government wide system, agency PKIs will have to work seamlessly with each other, yet current PKI products and implementations

suffer from interoperability problems. Ensuring the ability of agency PKIs to process certificates from all potential sources in a consistent manner will require that application software, certificates, and related infrastructure conform to some minimum standards.

Second, because full-featured organizational PKIs are rare in some countries, like New Zealand, it is not yet known how well this technology will operate as its use grows (http://www.e-government.govt.nz/). New Zealand government agencies have only limited experience with PKI, and much of it is based on pilot projects or relatively small-scale applications. Some examples in the New Zealand government are the Treasury Crown Financial Information System net, CFISnet, with some 200 certificates, including one user in each government agency, and New Zealand Health Information Service, NZHIS, with 400 certificates.

Third, adoption of the technology may be impeded by the high cost associated with building a PKI and enabling software applications to use and maintain it. These costs can easily add up to millions of dollars.

Fourth, an effective PKI at any level within the government will require well-defined policies and procedures for ensuring that an appropriate level of security is maintained on an ongoing basis. Establishing such policies will require resolution of a number of sensitive issues in areas such as governance, management of policies and standards, privacy protection, encryption key recovery, and how employees will be expected to identify themselves and secure their electronic PKIs.

Finally, as with any security technology, the success of a PKI implementation will depend on how well people interact with the system and how well the system is

implemented. Thus, agencies will be faced with the challenge of training and involving both users and system administrators in the adoption of a significant new technology.

This author has conducted personal interviews with law enforcement agencies dealing with computer crime and with executives from financial institutions dealing with security issues. In addition, this author did a literature review of cases prosecuted by the Department of Justice including the evaluation of damages and financial awards [24]. This review provides a significant negative market reaction to information security breaches involving unauthorized access to confidential data; but no significant market reaction when the breach does not involve access to confidential data [11]. This finding is actually consistent with the findings from the 2002 CSI/FBI Survey, which suggests that among information security breaches, the most serious financial losses were related to theft of proprietary information. This is also consistent with the recently prosecuted computer cases by the Computer Crime and Intellectual Property Section, CCIPS, of the Criminal Division of the U.S. Department of Justice. According to CCIPS, 91% of the cases that have been prosecuted under the computer crime statute, 18 U.S.C. 1030, are the cases related to the violation of confidentiality of information. As an example of these cases, in November 2001, two former Cisco Systems, Inc., accountants were sentenced to 34 months in prison for illegally issuing almost $8 million in Cisco stock to themselves. This author has sorted the information provided by the 2002 CSI/FBI Survey according to the percentage of detected attacks by respondents, and mapped these attacks into our three dimensional model as expressed in Table 3.

These findings reveal that breaches involving unauthorized access to confidential information are quite different than attacks that do not involve access to confidential

information. Once confidential information has been accessed in an unauthorized manner, the value of such a strategic asset may be permanently compromised. For example, a firm's customer list may be an important proprietary asset. Once this list has been accessed without authorization, others may be able to use the list for marketing and other purposes. This may permanently impair the list's value to the firm that created and owned it. In the cases of breaches that do not involve unauthorized access to confidential information, the underlying assets generally relate to operations.

While the firm may lose the ability to use these assets for some period of time, the loss is usually temporary. Consider the case of a denial of service attack. During the attack, the firm may not be able to conduct operations, take customer orders, reservations etc. Once the attack ends, and any necessary system changes are made, the firm can resume operations; and the value of its operating system is not permanently impaired. Findings provide some limited support for a negative stock market reaction to the widely reported information security breaches. This means that, customers, stockholders, and other stakeholders would probably be willing to accept some types of information security breaches, such as denial of service attacks, as a routine risk and a normal cost of doing business. As an example, this author has calculated the tangible cost for break-in using buffer overflow attacks against Web servers from real incidents in five different companies as follow:

Total productivity lost

Total downtime; time to access and repair damage: 49 hours

Total productivity lost: 49 hours × 30% time users lost ×500 users = 7,350 hours

Cost of downtime (Total productivity lost × percentage of staff) × hourly rate

Employees with annual salary of $20,000

(7,350 hours × 55% of staff) × $10 per hour → $40,425

Employees with annual salary of $30,000

(7,350 hours × 30% of staff) × $15 per hour → $33,075

Employees with annual salary of $45,000

(7,350 hours × 15% of staff) × $22.5 per hour → $24,806

Total cost for downtime→ $98,306

This total cost for downtime seems to be very low compared with damages of millions of dollars in cases where violation of data confidentiality occurred.

The literature review also indicates that compromised firms, on average, lose approximately 2.1% of their market value within two days after the event; while security vendors gain an average of 1.36% from each such announcement [14]. It also shows that negative average impact associated with an announcement decreases with the size of the firm and this suggests that smaller firms are penalized more than larger firms. This result for the managers of small firms serves as a reminder of the importance of security for survivability of these firms. However, the authors do not present detailed data, and thus it is not possible for readers to draw conclusions about the absolute loss of market values. Although the market penalizes all firms for security breaches, internet firms are penalized more compared with conventional firms. A possible explanation for this effect is the

greater dependency by the firms on the Internet to generate revenue. Firms that solely depend on the Internet as a revenue-generating mechanism pay higher prices in case of a security breach than firms that have multiple-sale channels.

Table 3- Combination of agents, techniques, security measures, and percentage detected in 2002 (Using the data from 2002 CSI/FBI survey)

Attack	**Agent**	**Threat**	**% Detected**	Security Measure
Virus	Unauthorized	SW	85	Data Integrity
Insider Abuse of Net Access	Authorized	SW & Personnel	78	Authentication & Access Control
Laptop	Unauthorized & Authorized	Physical & Personnel	55	ALL five Measures
Denial of Service	Unauthorized	SW	40	Authentication & Access Control
System Penetration	Unauthorized	SW & HW	40	Authentication & Access Control
Unauthorized Access by Insiders	Unauthorized	Personnel	38	Authentication & Access Control
Theft of Proprietary	Unauthorized & Authorized	SW & procedural	20	Authentication & Access Control
Financial Fraud	Unauthorized & Authorized	Procedural	12	Authentication & Access Control
Telecom Fraud	Unauthorized	SW & HW	9	Authentication & Access Control
Sabotage	Unauthorized & Authorized & Envr.	HW & Physical	8	Access Control
Telecom Eavesdropping	Unauthorized	HW	6	Data Confidentiality
Active Wiretap	Unauthorized	HW	1	Data Confidentiality & Data Integrity

This research also tried to investigate the long-term impact of the announcement of a security breach on firms by comparing the stock value of the victimized firms with their industry indexes. A sample of eight companies: Boeing, First Data Corp, McGraw-Hill, Yahoo, Ebay, Egghead, Raytheon, and Northwest Airline, who had suffered from a publicized security breach were chosen. The stock values of these companies, on the day of the incident, two days, 7 days, one month, one quarter, two quarters, three quarters,

and four quarters, before and after the incident, were recorded from the Standards and Poor's publications [59, 60, 61]. These numbers were also compared with the trend of their related industries in that period of time. However, because of the lack of data points and insufficient information, it was concluded that one cannot draw a definite conclusion about the impact of public announcement of security breaches on firms with such an approach.

Chapter4

Probability of Security Incidents

4.1 Subjective Probability Assessment

In practical terms, the evaluation of security risks eventually leads to subjective assessment supported by guidelines or some risk assessment system. This research provides a methodology by which the process can be made more systematic.

Estimating the probability of attacks caused by humans using subjective evaluation can be complex. One should consider the following factors:

1- Motive. How motivated is the attacker? Is the attacker motivated by political concerns? Is the attacker a disgruntled employee? Is an asset an especially attractive target for attackers?

2- Means. Which attacks can affect the critical assets? How sophisticated are the attacks? Do likely attackers have the skills to execute the attacks?

3- Opportunity. How vulnerable is the computing infrastructure? How vulnerable are specific critical assets.

4.2 Possible Pitfalls of Subjective Analysis

This author wishes to warn managers of some cognitive biases that stem from the reliance on judgmental heuristics, which may occur in subjective analysis. The origins of these pitfalls can be classified into three types:

Representativeness. In the representativeness heuristic, the probability that for example Bob is a hacker, is assessed by the degree to which he is representative of, or similar to, the stereotype of a hacker. This approach for estimating probability can lead to serious errors, because similarity, or representativeness, is not influenced by several factors that should affect determining of probability.

Availability. There are situations in which people look at the frequency of a class or the probability of an event by the ease with which instances or occurrences can be brought to mind. For example, one may access the risk of disclosure of information among financial institutions, by hearing about such occurrences from one's acquaintances. Availability is a useful clue for assessing frequency or probability, because instances of large classes are usually recalled better and faster than instances of less frequent classes. However, availability is affected by factors other than frequency or probability. Consequently, the reliance on availability can lead to biases.

Adjustment and anchoring. In many situations, people make estimates by starting from an initial value that is adjusted to yield the final answer. The initial value, or starting point, may be suggested by the formulation of the problem, or it may be the result of a partial computation. In either case, adjustments are typically insufficient. That is, different starting points yield different estimates, which are biased toward the initial values.

In spite of these pitfalls, this author believes that subjective analysis can be employed usefully in information security assessment, even when quantitative data is not available or a formal process description is not required [26]. Previous attempts to

quantify the likelihood of attacks provide examples of the ability of subjective analysis without quantitative data [51, 65].

4.3 Scope of Subjective Analysis

Among information security experts, there appears to be no agreement regarding the best or the most appropriate method to assess the probability of computer security incidents. There does exist, however, a hierarchy of approaches such as checklists and scenario generation techniques that require the user to have only a minimum knowledge of information system security [70]. To have a well-defined scope for the checklist, one can follow the formats that are provided by British Standards [7], or the National Security Agency [37].

The National Security Agency, suggests the following eighteen areas for information security assessment, which is more comprehensive than the British Standards:

- Information security documentation
- Identification and authentication
- Account management (establishment, deletion, expiration)
- Session control management (access control lists, files, directions, servers, remote dial up, Internet services)
- External connectivity
- Telecommunications
- System security administration
- Auditing

- Virus protection
- Contingency planning
- System maintenance procedures
- Configuration management
- Back up policies
- Labeling
- Media sanitization/Disposal
- Physical/Environmental controls
- Personnel security
- Training and awareness

4.4 Probability Assessment

To derive an overall likelihood rating that a potential vulnerability may be exploited, these governing factors should be considered: threat-source motivation and capability; nature of the vulnerability; and existence and effectiveness of current controls

The likelihood that a potential vulnerability could be exploited by a given threat-source can be described as high, medium, or low. In defining these likelihoods, this author follows the likelihood determination by NIST [63]:

High likelihood. The threat-source is highly motivated and sufficiently capable; and controls are ineffective in preventing penetration.

Medium likelihood. The threat-source is motivated and capable; but controls are in place that may impede a successful attack.

Low likelihood. The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede the attack.

One can also use these qualitative ratings to assign values for a quantitative evaluation to use in developing a checklist; for example: high likelihood at 0.9, medium likelihood at 0.5, and low likelihood at 0.1. We can also use a more detailed scale such as: very high, high, medium, low, and very low, and use 0.9, 0.7, 0.5, 0.3, and 0.1, respectively, for these likelihoods.

The checklist can be written in a question format and should allow three possible answers: "yes", "no", or "not relevant". Questions should be asked in a way that a "yes" answer mean that the control exists and a "no" answer means that the control does not exist. A control is relevant when both the asset to be protected and the threat exist.

For example, one critical element to evaluate data integrity can be, "Is virus detection and elimination software installed and activated?" A subordinate question for the above question could be, "Are virus scans automatic?" The answer to this question might be "yes", "no", or "not relevant". A metric for this evaluation can be the percentage of systems with automatic virus scanning, which can help gauge the risk exposure caused by known viruses.

Assessing probability:

In this section, we propose a procedure by which quantitative answers to a detailed security questionnaire can be compiled into an overall vulnerability measure. Conducting the survey with the checklist, we can assess the vulnerability of each system under examination by defining the following parameters and calculations:

N (VH): Number of questions with very high importance

N (H): Number of questions with high importance

N (M): Number of questions with medium importance

N (L): Number of questions with low importance

N (VL): Number of questions with very low importance

NR (VH): Number of relevant questions with very high importance

NR (H): Number of relevant questions with high importance

NR (M): Number of relevant questions with medium importance

NR (L): Number of relevant questions with low importance

NR (VL): Number of relevant questions with very low importance

NN (VH): Number of "no" answers to relevant questions with very high importance

NN (H): Number of "no" answers to relevant questions with high importance

NN (M): Number of "no" answers to relevant questions with medium importance

NN (L): Number of "no" answers to relevant questions with low importance

NN (VL): Number of "no" answers to relevant questions with very low importance

NP: Normalized probability

IP: Index of probability

SWP: Sum of probability weights

JP: Justified probability

MW: Maximum weight

AP: Assessed probability

We would have:

$$NP = \frac{\left[NR\ (VH) / N\ (VH) \times 0.9 + NR\ (H) / N\ (H) \times 0.7 + \cdots + NR\ (VL) / N\ (VL) \times 0.1\right]}{\left(0.9 + 0.7 + 0.5 + 0.3 + 0.1\right)}$$

$$I\ P = 1/NP$$

$$SWP = NN\ (VH) \times 0.9 + NN\ (H) \times 0.7 + NN\ (M) \times 0.5 + NN\ (L) \times 0.3 + NN\ (VL) \times 0.1$$

$$JP = SWP \times IP$$

$$MW = N\ (VH) \times 0.9 + N\ (H) \times 0.7 + N\ (M) \times 0.5 + N\ (L) \times 0.3 + N\ (VL) \times 0.1$$

$$AP = JP/MW$$

For example, the checklist for the area of integrity may include 20, 40, 50, 30, and 15 questions in a scale of importance of very high, high, medium, low, and very low; and only 10, 30, 40, 24, and 12 may be relevant to the specific vulnerability regarding integrity. If we have 7, 25, 36, 20, and 9 "no" answers (meaning control does not exist), respectively, following the proposed method; we obtain an assessed probability of AP = 0.88. This would imply that there is an 88% chance of a data integrity violation. The assessed probability is a number between zero and one, with zero representing an incident that definitely will not occur and one representing an incident that definitely will occur.

Chapter 5

Classification of Security Threats in Information Systems

Before we analyze the security threats and develop a scheme or a methodology to optimally allocate resources and deploy control measures against these threats, we need a good classification scheme for threats. A taxonomy to be used in this research can be defined as follows:

"Any taxonomy that is used to price security failures should be deterministic and complete. No security failure should be left unclassified and no security failure should fall into more than one classification" [10].

In general, categorizing a phenomenon makes systematic studies possible. In particular, an organized classification of threats to e-commerce can help managers to build systems that are less vulnerable. An established classification would also be useful when reporting incidents to incident response teams. Lindqvist [43] recommends the following properties for the classification for information security:

- The categories should be mutually exclusive that is every specimen should fit in at most one category. And collectively exhaustive, that is every specimen should fit in at least one category.
- Every category should be accompanied by clear and unambiguous criteria defining what specimens are to be put in that category.
- The taxonomy should be comprehensible and useful, not only to experts in security, but also to users and administrators with less knowledge and experience.

- The terminology of the taxonomy should comply with established security terminology; something that is not always easy to define.

5.1 A Review of Existing Taxonomies

Literature review has identified many attempts in the classification of security threats.

The taxonomy developed by the Naval Research Laboratory [41], classifies each security flaw according to genesis (caused intentionally or inadvertently), time of introduction (during development, maintenance, or operation), and location (software or hardware).

The taxonomy developed by Neumann and Parker [48], categorizes computer misuse techniques into nine classes (that are ordered from the physical world to the hardware and software and from unauthorized use to misuse of authority, etc). This classification seems to cover most of the known techniques covering external attacks as well as unauthorized users misusing their privileges. However, it has some shortcomings in assigning an intrusion to one class or another, or both.

The DARPA's Intrusion Detection Evaluation Taxonomy [44], classifies attack types into four groups: 1- Denial of Service, 2- Remote to Local (an attacker who gains access to victim's machine), , 3- User to Root (a local user on a machine is able to obtain privileges normally reserved for the UNIX root or super user), and 4- Surveillance/Probing. This taxonomy uses a reasonable, but not exhaustive, set of attacks with a limited set of actions performed as a part of each attack This taxonomy also uses a simple network topology, and a non-restrictive security policy.

Schummacher and Ghosh [57] have defined systematic, communication, physical, personnel, application, performance, design correctness; as the components, and privacy, integrity, accountability, reliability, connectivity, recovery, liability, and uncertainty, as the attributes of the information security. Pflegger [52] also groups the potential threats to a network into seven categories: wiretapping, impersonation, message confidentiality violations, message integrity violations, hacking, code integrity, and denial of service.

This author's opinion is that these taxonomies, although they address the most important computer security threats, either do not cover all of them or do not allow them to be considered independently.

5.2 A Model for Threat Classification and Control Measures

We consider threats to a network system from two points of view: 1- Threat agent, and 2- Penetration technique. A threat is manifested by a threat agent using a specific penetration technique to produce an undesired effect on the network.

Threat Agents

Threat agents are classified into environmental factors, authorized users, and unauthorized users.

Environmental Factors: Although it is common sense, one should remember to account for environmental factors. Some areas are more prone to certain environmental influences and natural disasters than others. Some types of disasters, such as fire, are not geographically dependent, while others, such as tornadoes and floods, can be anticipated on a more regular basis in specific areas. In addition to the natural disasters, attention

should be paid to the danger of mechanical and electrical equipment failure and the interruption of electrical power.

Authorized users: Authorized users and personnel engaged in supporting operations can be considered as potential threats when they exceed their privileges and authorities or commit errors, thus affecting the ability of the system to perform its mission. Personnel granted access to systems or occupying positions of special trust, and having the capability or opportunity to abuse their access authorities, privileges, or trusts, should be considered as potential threats.

Unauthorized users: An unauthorized user can be anyone not engaged in supporting operations that, by design, attempts to interrupt the productivity of the system or operation either overtly or covertly. Overt methods could include outright acts of sabotage affecting hardware and associated equipment. Covert methods are more subtle efforts of destruction, which could be accomplished through the manipulation of software, both systems and application.

Techniques

Techniques can be classified into physical, personnel, hardware, software, and procedural including:

Physical: Physical penetration implies use of a physical means to gain entry into restricted areas such as buildings, compound rooms, or any other designated areas.

Personnel: Penetration techniques and methods generally deal with the subverting of personnel who are authorized some degree of access and privilege regarding a system, either as users or operators. Operators could include system-analysts, programmers, input/output schedulers, etc. They can be recruited by a threat agent and used to

penetrate the system, operation or facility, or they themselves can become disaffected or motivated to mount an attack.

Hardware: Attacks can be mounted against hardware for the purpose of using the hardware as a means of subverting or denying use of the system. A physical attack against the equipment, a bug implanted within a hardware controller, or an attack against the supporting utilities, are means of subverting the system by using the characteristics of the hardware. Hardware, as used in this category, generally includes any piece of equipment that is part of the system, (i.e., the mainframe, peripherals, communications controllers, or modems). It also includes indirect system support equipment, such as power supplies, air conditioning systems, backup power, etc.

Software: Software penetration techniques can be directed against system software, application programs, or utility routines. Software attacks can range from discreet alterations that are subtly imposed for the purpose of compromising the system, to less discreet changes intended to produce results such as destruction of data or other important systems features.

Procedural: Authorized or unauthorized users can penetrate the system due to lack or inadequacy of controls, or failure to adhere to existing controls. Examples of procedural penetration include former employees retaining and using valid passwords, unauthorized personnel picking up output, and users browsing without being detected due to failure to diligently check audit trails.

At a more detailed level, the ISO 7498-2 Standard [39], lists five security control measures to combat these threats: 1) Authentication, 2) Data Confidentiality, 3) Access Control, 4) Data integrity, and 5) Non-repudiation. This classification is widely

accepted among computer security experts, and this author also recommends them as good control measures.

Authentication. Authentication is the binding of an identity to a subject [4]. The external entity must provide information to enable the system to confirm its identity. This information may come from one or more of the following:

1- What the entity knows, such as passwords or confidential information

2- What the entity has, such as a card

3- What the entity is, such as fingerprints or retinal characteristics

4- Where the entity is, such as in front of a particular terminal

The authentication process consists of obtaining the authentication information from an entity, analyzing the data, and determining if it is associated with that entity. Kerberos and X.509 are some examples of authentication applications which are widely used in securing networks. Kerberos is an authentication protocol based on conventional encryption that has received widespread support and it is used in a variety of systems [62]. X.509 specifies an authentication algorithm and defines a certificate facility. The latter enables users to obtain certificates of public keys so that a community of users can have confidence in the validity of the public keys. This facility is employed as a building block in a number of applications.

Data confidentiality. Confidentiality is the concealment of information or resources. Data can be gathered by many means such as tapping wires, planting bugs in output devices, sifting through trash receptacles, monitoring electromagnetic radiation, bribing key employees, inferring one data point from other values, or simply requesting

the data. Because data are often available in a form people can read, the confidentiality of data is a major concern of information security.

All the mechanisms that enforce confidentiality require supporting services from the system. The assumption is that the security services can rely on the kernel, and other agents, to supply correct data. Thus, assumptions and trust underlie confidentiality mechanisms. Pretty Good Privacy, PGP, and Secure/Multipurpose Internet Mail Extension, S/MIME are examples of mechanisms for providing confidentiality and authentication for electronic mail.

PGP is an encipherment program widely used to provide privacy for electronic mail throughout the internet and to sign files digitally. It uses a certificate-based key management infrastructure for user's public keys. S/MIME is very much like PGP; its difference is the method of key exchange. Basic PGP depends on each user's exchanging keys with all potential recipients and establishing a ring of trusted recipients. S/MIME uses hierarchal validated certificates, usually represented in X.509 format, for key exchange. Thus, with S/MIME the sender and the recipient do not need to have exchanged keys in advance as long as they have a common certifier they both trust. S/MIME works with a variety of cryptographic algorithms, such as Digital Encryption System, DES, and Advanced Encryption System, AES.

Access control. Access control mechanisms support confidentiality of information. One access control mechanism for preserving confidentiality is cryptography, which scrambles data to make it incomprehensible. In the context of network security, access control is the ability to limit and to control the access to host systems and applications via communication links. To achieve this control, each entity

trying to gain access must first be identified, or authenticated, so that access rights can be tailored to the individual.

Data integrity. Integrity refers to the trustworthiness of data or resources, and it is usually phrased in terms of preventing improper or unauthorized change. Integrity includes data integrity (the content of information) and origin of integrity (the source of data). Integrity mechanisms fall into two classes: prevention mechanisms and detection mechanisms.

Prevention mechanisms seek to maintain the integrity of data by blocking any unauthorized attempt to change the data or any attempt to change the data in unauthorized ways. Detection mechanisms do not try to prevent violations of integrity; they simply report that the data's integrity is no longer trustworthy. Detection mechanisms may analyze system events, user or system actions, to detect problems or more commonly, may analyze the data itself to see if required or expected constraints still hold. The mechanisms may report the actual cause of integrity violation (a specific part was altered), or they may simply report that the file is now corrupt.

Working with integrity is very different from working with confidentiality. With confidentiality, the data is either compromised or it is not; but integrity includes both the correctness and the trustworthiness of the data. The origin of data, how and from whom it was obtained, how well the data was protected before it arrived at the current machine, and how well the data is protected on the current machine, all affect the integrity of the data.

Non-repudiation. Non repudiation prevents either sender or receiver from denying a transmitted message. Thus when a message is sent, the receiver can prove that the

message was in fact sent by the alleged sender. Similarly, when a message is received, the sender can prove that the message was in fact received by the alleged receiver.

These security measures, along with agents and techniques, are shown in Figure 2. One can use this figure to classify threats (agents and the techniques) to information systems and security measures to confront these threats. For example, access control is one of the security measures to confront the threats that may be caused by an unauthorized user through software. In total, there are $5 \times 3 \times 5$ combinations of threat techniques, agents, and control measures; however not all of these combinations are applicable. For example, non-repudiation cannot be a security measure for the threats caused by environmental factors or by a procedural technique. This three-dimensional demonstration of threat agents, techniques, and security control measures can be used for a better quantitative assessment and management of security risk. Figure 3 shows virus, denial of service attack, and insider abuse of net access as an example of threats and recommended control measures in the model.

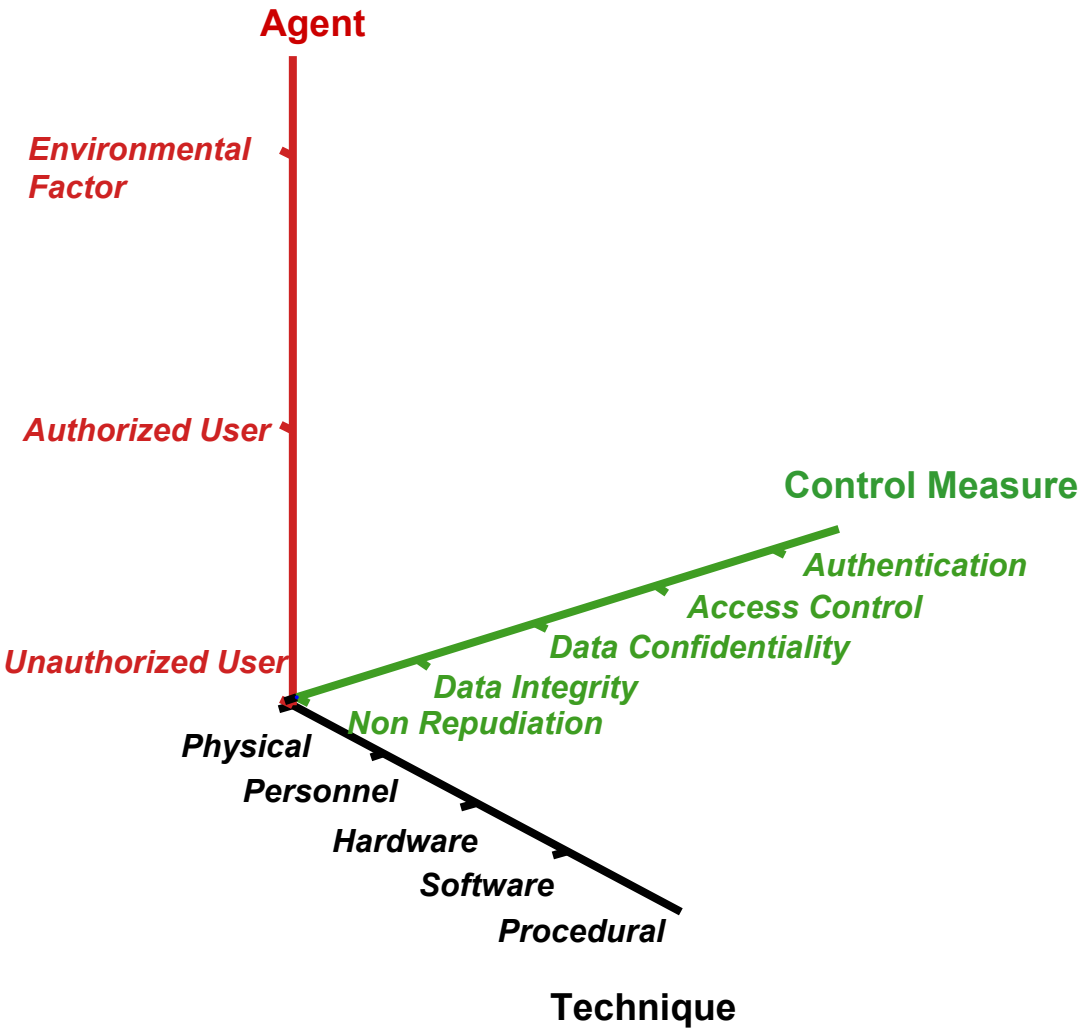

Figure 2- Combination of agents, techniques, and control measures

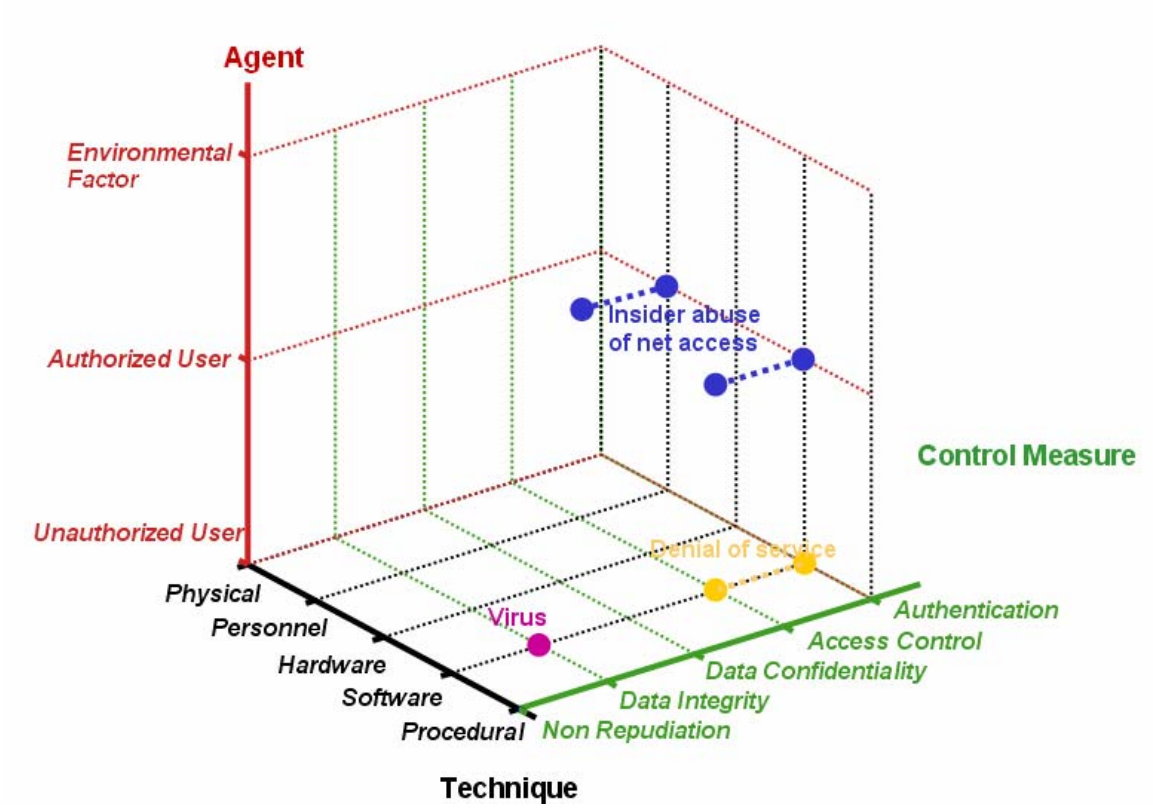

Figure 3- Virus, denial of service attack, and insider abuse of net access in our classification

Chapter 6

Developing a Risk Management System

6.1 A Critical overview

Risk can be defined as: "The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets", and vulnerability can be defined as: "A weakness of an asset or group of assets which can be exploited by a threat" [40].

Risk assessment is the process for determining whether existing or proposed safeguards are adequate to protect information resources from likely threats [19]. It involves identifying assets to be protected, threats to those assets and the likelihood of threat occurrence. Risk assessment also identifies vulnerabilities that could be exploited, losses that could result from an attack, and safeguards that are or could be installed. The objective is cost-effective safeguards; that is, safeguards that cost no more than the expected level of loss from an attack.

Information security incidents are adverse events that cause losses to business; therefore, information security is a risk management application, with the intent to manage the cost of information risk to the business. Literature review has identified a stream of research on risk assessment of information systems security incidents [1, 3, 6, 12, 47, 58]. Specific methods for undertaking information security risks analysis fall into two categories, quantitative and qualitative.

Quantitative methods

The quantitative approach assumes that it is possible to associate a level of risk with each hazard identified and attempts to calculate the value of the likely damage should the risk become reality. The focus is the production of an Annual Loss Expectancy (ALE), figure which is calculated for each threat by establishing two factors [67]:

1- Its probability of occurrence over a specified time period

2- The amount of loss that would be incurred

These quantities are multiplied to obtain the estimated ALE which is compared with the cost of suitable control measures. The philosophy here is that, if the cost of a control measure is less than the calculated ALE, then implementing the control measure would be a cost-effective solution, otherwise alternative solutions should be considered.

Qualitative methods

The qualitative approach assesses risks on the basis of the capability to identify threats and vulnerabilities correctly. Unlike the quantitative approach, precise values are not sought and risks are expressed in terms of descriptive variables such as “high”, “medium”, or “low”; the rationale being that the consequences of some types of loss, such as corruption or modification of data, cannot be expressed in terms of monetary value or discrete events.

Comparison of Quantitative and Qualitative methods and choosing an appropriate method

The calculation of an ALE is a method which has been used by insurance companies for some time; and at present, the majority of quantitative computer security risk analysis methods use this technique. However, unlike insurance risks which focus on losses arising from insurance claims, system security risks are of a more involved nature which can only be evaluated by considering a complex combination of possible consequences. Moreover, system security risks are not readily specified in purely monetary terms. Potential losses are often related to factors such as corporate goodwill or other non-monetary assets. For example, the extent of loss in customer confidence following a security breach is extremely difficult to quantify before the event. Not only it is difficult to put a precise financial value to a wide range of threats, but it is common for people to be unwilling to assign a monetary measure at all in situations where threats have a social impact, for example disclosure of health information.

The advantages of quantitative methods lie in their ability to relate expenditure to threat value in percentage terms and to direct resources proportionally [13]. However, even though a single figure such as the ALE is an easily perceived summary of the cost of the threats, it must be recognized that it is derived from data and probabilities which frequently do not have a strong empirical basis [29]. Problems arise when too much faith is placed in what appear to be exact and precise figures as the probabilities and data used in this type of approach are often not very accurate.

A major advantage of the qualitative approach is the time and expense required to make the assessment. The quantitative approach usually requires an in-depth and

extensive study of the system/organization in order to establish threats and vulnerabilities, to determine probabilities and to obtain cost figures. In nearly all cases, such a study is a time consuming effort and is characterized by fairly extensive surveys including many people in the organization. On the other hand, qualitative methods can usually be completed in less time with a smaller number of personnel as they do not require the same type of data collection and mathematical calculations. However, care must be taken when attempts are made to compare qualitative values such as high, medium, and low risks. One manager's perception of a high risk could be considered a low risk by another manager. It is suggested that when deciding which approach to use, the following factors could be taken into consideration [69]:

- Cost- How much is the organization willing to spend?
- Appropriateness- Organizations must select the most appropriate risk analysis method for their particular environment.
- Adaptability- Methods must relate to the current working practice.
- Completeness- It must be ensured that the method encompasses all possible risks.

Paying close attention to the second factor (i.e., appropriateness) is important for decision makers in organizations. The following can be suggested as steps for measuring suitability in selecting a risk management approach. For measuring suitability, one must:

1- Establish a set of criteria that describe a method's suitability.

2- Define the suitability criteria in terms of related attributes.

3- Specify metrics that describe presence of the attributes.

4- Make a quantitative statement of the appearance of a suitability criterion by determining the ratio of actual occurrences of a metric to the number of possible occurrences. This should be done for each criterion.

5- Use the derived quantitative values for each of the criteria to evaluate and compare the variety of methods and tools available to the organization.

The following seven criteria are also suggested as the suitability criteria:

1- Consistency- Given a particular system configuration, results obtained from independent analysis will not significantly differ.

2- Usability- The effort necessary to learn, operate, prepare input, and interpret output is generally worth the results obtained.

3- Adaptability- The structure of the method or tool can be applied to a variety of computer system configurations and the inputs can easily be updated as they periodically change.

4- Feasibility- The required data is available and can be economically gathered.

5- Completeness- Consideration of all relevant relationships and elements of risk management is given.

6- Validity- The results of the process represent the real phenomenon.

7- Credibility- The output is believable and has merit.

This research uses a combination of qualitative and quantitative methods in developing a risk management system for information system security incidents which is explained in the following section.

6.2 A Risk Management System

This research has developed a five stage risk management system to help managers to identify vulnerabilities to the information systems of their companies, to evaluate the existing security measures in place, and to select the most appropriate and cost-effective control measures. This risk management system is shown in Figure 4.

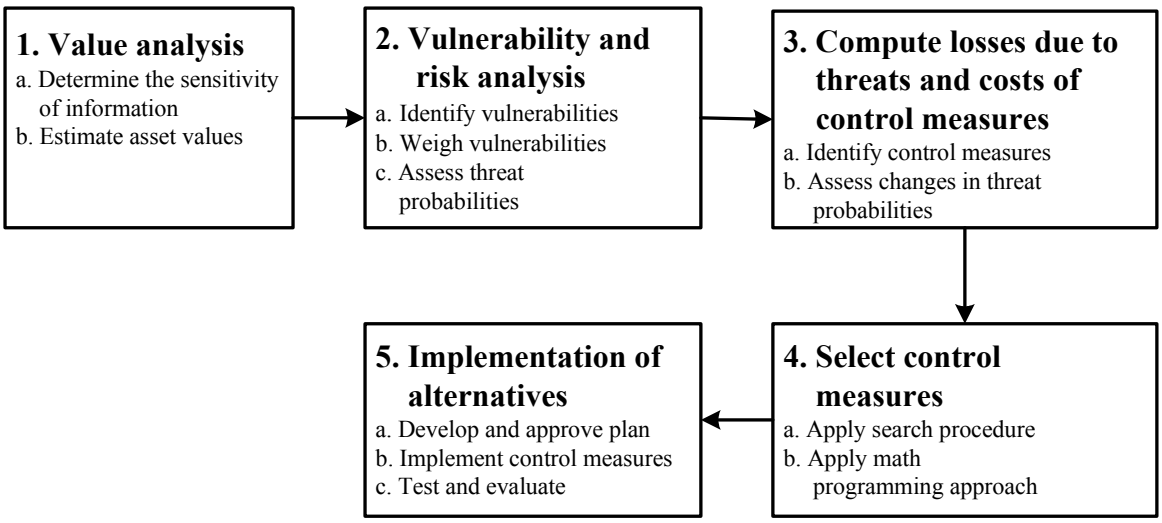

Figure 4- The proposed risk management system

The five stages of our risk management system are:

6.2.1 Resource and Application Value Analysis

This can be done in two phases: First, determine the sensitivity of information handled. The objective is to relate each application to sensitivity level based upon the most sensitive type of data processed (e.g., privacy, asset/resource, proprietary). This analysis provides the framework for subsequent analysis, so its detail and accuracy are important. Second, estimate the asset value of automated resources providing support such as physical facility, equipment, supplies and software.

6.2.2 Vulnerability and Risk Analysis

This analysis is in three parts: 1- Identification of vulnerabilities: Weakness or flaws in the design, implementation, or operation of the security controls of a facility, system or operation must be identified; whether through analysis of the security controls alone, or as causal factors directly related to a previously identified threat. 2-Weighting of vulnerabilities**:** Vulnerabilities just identified, should be considered in relation to each other and arrayed according to seriousness and potential degree of exploitability. And, finally, 3- Assess threat probabilities: In this step, probabilities of threats are documented. This has been discussed in Section 4-4.

6.2.3 Computation of Losses due to Threats and Benefits of Control Measures

Losses due to threats and benefits of control measures can be computed by defining a control measure(s) at an appropriate level. For a control measure at a given level, there is the cost of the control measure, its effectiveness, expected damage caused by the threat, probability that the threat occurs, expected benefit of the control measure, expected loss attributed to the control measure set, etc. Assessing changes in threat probabilities can be reflected in f_{ij}: effectiveness of control measure i on threat j, which will be used in the calculations.

6.2.4 Selection of Control Measures

At this stage, the system chooses a control measure and level to minimize total cost. Enumerating search procedures and mathematical programming approaches can be used at this stage. For this selection we will use a search through the solution space. To select control measures, we use the following parameters and calculations:

i : i th control measure; i = 1…….I

j: j th threat; j = 1……..J

C_i: Cost of control measure i

f_{ij}: effectiveness of control measure i on threat j (Assuming independent control measures)

l_j: expected damage caused by threat j

P_j: probability that threat j occurs

B_i: Expected benefit of control measure i

L: Expected loss of a set of control measures (expected losses left "uncontrolled" by control measures)

C: Cost of control measures

TC: Total cost of control measures and losses

vj: Valuation score

The procedure is:

1- Measure the expected loss due to the occurrence of the threat:

$$l_j = P_j \times v_j$$

2- Compute the benefit of control measures:

$$B_i = \sum_{j=1}^{J} l_j \times \left\{ 1 - \prod_{i=1}^{I} \left(1 - f_{ij} \right) \right\}$$

3- Compute the total expected loss for control measures:

$$L = \sum_{j=1}^{J} l_j \times \prod_{i=1}^{I} (1 - f_{ij})$$

4- Compute the total cost of control measures:

$$C = \sum_{i=1}^{I} c_i$$

5- Compute the total expected cost for each set of control measures:

$$TC = C + L$$

The goal is to minimize TC by selecting control measures

As an example of using this system, assume there are five possible threats: 1) Virus, 2) Insider abuse of net access, 3) Denial of service, 4) System penetration, and 5) Authorized access by insiders. Access control is evaluated as a possible control measure. There are three access control options: 1) Discretionary Access Control (DAC), $250K, 2) Mandatory Access Control (MAC), $300K, and 3) Role based Access Control (RBAC), $500K. There is the following information presented in Tables 4 and 5:

Table 4- Threat, probability, and expected cost

Threat Number	**Probability of Occurrence**	**Expected cost (K$)**
Virus	0.3	1000
Insider abuse of net access	0.1	4000
Denial of service	0.1	3000
System penetration	0.2	5000
Unauthorized access by insiders	0.5	1000

Table 5- Effectiveness of control measures (CM) by type of Threat

Threat / CM	**Virus**	**Insider abuse of net access**	**Denial of service**	**System penetration**	**Unauth. access by insiders**
DAC	0.1	0.1	0.2	0.1	0.1
MAC	0.5	0.5	0.6	0.4	0.6
RBAC	0.8	0.9	0.7	0.7	0.6

Considering this information, and also the cost of implementing control measures, the outcome of the system will be:

- The minimal total cost computed with the given probability vector of threats and threats vs. control measures as $1,190,000
- The initial minimal cost of implementing RBAC as $500,000 and the control measure which is selected would be RBAC

6.5 Implementation of Alternatives

This stage can be done in three phases. The first phase is developing and approving a plan. To develop a plan, it is necessary to establish priorities for implementation. Generally, control measures should be implemented according to severity of the undesirable effect being countered, as determined by the preceding analysis. Using this as the basic criterion, other influences can be brought into consideration. Once the plan is developed, it must be reviewed and approved by senior management. The second phase is implementation of control measures**.** Once the planning documents have been completed, action can commence on the implementation of the control measures. The third phase is testing and evaluation of control measures**.** Sensitive systems, with the strongest security requirements, should have a formal test and evaluation of significant control measures immediately prior to and during initial implementation. The purpose of testing and evaluation is to ascertain, with reasonable assurance, that the proposed control measure produces the desired effect and will not result in undesirable side effects.

This system is intended to help managers in: identifying business assets, recognizing the threats, assessing the level of business impact that would ensue if the threats were to materialize, analyzing vulnerabilities, and, finally, selecting the control

measure and suggesting an implementation plan. This procedure is our first attempt at defining this rather complex problem. The following extensions are under consideration:

- Incorporating more robust solution techniques for large, real-life problems,
- Differentiating control measures by implementation techniques
- Considering the effects resulting from combinations of control measures
- Performing sensitivity analysis with respect to the inputs, such as probabilities of expected threats.

Current work includes a refinement of the system to incorporate actual field data collected from security-conscious e-commerce companies and further validation.

Chapter 7

Case Studies

Chapter seven describes the case studies of this research which was done in 4 steps:

1. Identifying sources of information
2. Developing the questionnaire
3. Analyzing/evaluating the usefulness of answers
4. Testing and confirming the results at the second round

At this stage of the research, six information security experts participated. They are from: 1- A consumer advertising service, 2- A law enforcement agency, 3- An information security consulting service, 4- A network service provider, 5- An online payment service, and 6- An educational service auditor. Four experts participated in round one and two experts, who had contributed in round one, as well as one additional expert, participated in round two.

7.1 First Round of Interviews

The following are the thirteen questions and the answers to the first round of four case studies:

Question 1- What do you think would be the most important threat(s) to the information system of your company?

Case1- "The most important threat that we face would be disclosure of customer data.

Because of certain aspects of our business model, we see lots of customer-provided confidential data, and associate with it certain information that those customers prefer to keep private. The second most important threat would be the loss of company proprietary data."

Case 2- "Virus, Outside intrusion, Denial of Service."

Case 3- "Intransigent IT Security teams, Disgruntled Employees, External Hacking, Improper password security, Hardware failures."

Case 4- The application

Question 2- How many times have you experienced this type of threat(s)/incident(s) during the last 12 months?

Case1- "We have not had this happen in the last 12 months. We regularly place certain aspect of our intellectual property at customer sites."

Case 2- "Virus, One major attack per month average. Intrusion: one every 6 months average. DoS, no major attacks yet."

Case 3- "Intransigent IT Security teams: one, but increasingly likely and debilitating. 6 months of meetings, etc. to resolve."

"Disgruntled Employees: External Hacking: one"

"Improper password security: one (posted on a public website!!!)"

"Hardware failures: numerous, but no known data loss."

Case 4- "We receive an average of 10,000 application specific attacks a day"

Question 3- If the threat has not yet occurred, how long do you think it will be (in months) before you suffer such a threat?

Case1- "We would expect to see such an attack occur within the next 24 months or so."

Case 2- "DoS in next 12 months."

Case 3- "NA"

Case 4- "Within months to two years"

Question 4- What type of damages did this/these threat(s) cause? (or would likely cause)?

Case 1- "If such an attack were to take place, substantial, but not irreparable damage to the company brand would occur. The damage would be dependent on the publicity surrounding the access".

Case 2- "Virus: shutdown systems, caused rebuilds. Intrusions: Notification cost, outside consulting costs, re-design costs."

Case 3- "A lot would depend on what may have been taken, proprietary information, intellectual properties, etc. For example a bank lost several credit cards, identity theft, and the bad guy(s) actually were able to charge around $10.00. But when this became public the banks stock feel over 3 points. This lose could have been in the 100's of 1000's. "

Case 4- "We have had one successful application incident that defaced our homepage with profanity. I'm more concerned with what's to come than what we have experienced to date. My concerns lie in someone using our application to access

privileged information, planting files on web servers and phasing our customer base."

Question 5- Is/are this/these threat(s) more likely to be caused by unauthorized or authorized users by using software techniques?

Case 1- "Authorized users of the system are unlikely to cause these problems, because they are mostly external and minimally motivated to engage in these behaviors. Unauthorized attackers are much more worrisome."

Case 2- "Unauthorized users"

Case 3- "Could be both. In addition social engineering could also be used."

Case 4- "Unauthorized users are our focus for now but the authorized users are still of concern."

Question 6- What control measure(s) did you have in place that failed to stop the threat?

Case 1- "N/A"

Case 2-"Virus. Scanners. (No signatures, old signatures). Break-in (passwords, firewalls, IDS systems)"

Case 3- "NA"

Case 4- "There are no control measures in place to counter an application threat."

Question 7- What type of control measure do you use for this/these threat(s) that do not fall in the category of access control, authentication, data confidentiality, data integrity, and non-repudiation services?

Case 1- "Source code analysis and intrusion detection systems."

Case 2- "Background checks"

Case 3- "This would not apply to us. We respond after the fact in most cases. If we are consulting we would set up some kind of secure server and/or disaster recovery solution.

Case 4- "We are looking into an application firewall and application auditing software for the developers and security team to help mitigate our exposure."

Question 8- According to the CSI/FBI Survey, attacks which can cause the most serious financial damages are: theft of propriety information, financial frauds, and viruses. Do you think this/these attack(s) are more likely to be caused by unauthorized or authorized users by using software techniques?

Case 1- "Your use of the phrase "by software techniques" is not clear, but we think that unauthorized external users are the biggest threat. This is somewhat caused by the unusual nature of the data we carry for customers."

Case 2- "Techniques? Financial fraud is almost always an insider job, usually with authorization. Viruses are from unauthorized outsides."

Case 3- "I believe currently, by far maybe even up to and over 70%, employees cause the most damage. They of course would be using the company's software products."

Case 4- "Because we are a .com company with all employees online at all times with little restriction, unauthorized users are presently our biggest threat. Employees are always exposed to unauthorized users nefarious techniques."

Question 9- Which combination of control measures do you prefer?

Case 1- "Effective ones!"

Case 2- "Policies and processes. Security Architecture including access control and proactive methods (Virus scanning). Encryption for storing of sensitive data."

Case 3- "First of all you need policies. Then you would need some kind of hardware and/or software monitoring devices. If probable cause is present, you could take control by using a keystroke monitoring device, with the proper authority."

Case 4- "Access control and web application security testing and assessment software."

Question 10- How would you rate the effectiveness of these control measures? For example, to what degree did this/these control measure(s) reduce the probability of the threat or the actual cost of the damage?

Case 1- "Unfortunately, measuring the effectiveness of most of our defensive measures is difficult."

Case 2- "I am sure that they reduce the risk. Difficult to determine how much. Good data back up policies reduce the cost to recover."

Case 3- "If the employee knows they are monitoring his status, etc., it could be very effective."

Case 4- "Out of 1 to 10? I would rate it the measures a 7"

Question 11- In some cases, using stronger control measures can cause dissatisfaction of clients, e.g. using stronger encryptions cause delay in response time. What is the maximum response time to a mouse click, in seconds, that you consider acceptable for your web-based customers?

Case 1- "Our web-focused service is intended for occasional, batch-focused use, and clients understand that after certain actions, our processing time may be from minutes up to days."

Case 2- "Cost of encryption in terms of cycles used or mouse click response time is very low. Main dissatisfaction is in the area of passwords and authentication. i.e. must change password every 60 days or requirement to have multiple passwords"

Case 3- "Probably not our companies issue"

Case 4- "Zero to 25 seconds"

Question 12- In making financial decisions, do you consider the intangible damages of an incident to your company, e.g. negative impact of announcement of a breach on stock market or on clients? If so, what metrics/evaluation criteria do you use to calculate these costs?

Case 1- "Our current methodologies are very informal"

Case 2- "Reputation risk is a major concern. Difficult to quantify. I have thought about equating the cost of reputation damage to the cost of advertising. We spend XX dollars to advertise our brand. If it is damaged then we need to spend YY additional to bring the image back to where it was. Therefore the cost of the attack was equal to the cost of the additional advertising. Other cost is the manpower cost to manage the incident."

Case 3- "NA"

Case 4- "The intangible of a service not being offered online has been calculated but the negative impact of a breach on clients has only been briefly discussed."

Question 13- Will you consider transferring risks to an insurance company? If so, do you find their policies and coverage reasonable?

Case 1- "As much as possible"

Case 2- "Currently looking to purchase Cyber insurance. There are still a number of items to be determined such as deductibles, what is covered. First party coverage vs. third party coverage. This will probably be a big area in the next few years."

Case 3-"This is a somewhat new field, cyber insurance. Some large insurance companies are beginning to write cyber insurance policies under some strict guidelines. But your question is not something we do but we certainly would consult with companies about this. Even to the point of doing a cyber assessment for them. As to the insurance companies we would do a cyber assessment for them either before or after they write the policies. We would look for different vulnerabilities and other such items."

Case 4- "At this point in time, no."

7.2 Summary of the Answers in the First Round

The following summarizes answers in the first round:

- All the respondents listed disclosure and theft of proprietary information as a major threat.

- Virus, DoS, disgruntled employees, improper password security, hardware failures were also mentioned as threats.
- None to one major attack per month and average of one intrusion every six months.
- All the respondents said they expect at least one major attack during the coming twelve to twenty four months,
- The damage of such an attack would first depend on publicity of the attack, and second on costs of system downtime, notification, consulting, and re-design.
- Unauthorized users were identified as the source of the most important threats to an organization which can be caused by software techniques.
- Most respondents could not describe what exact control measure they had in place. Some listed scanners for viruses, and passwords, firewalls, IDS systems for break-ins.
- Background checks were mentioned as a control measure which is not included in our model.
- All respondents mentioned access control as the most effective control measure for a threat. Respondents were not able to evaluate the effectiveness of the control measures, except for one respondent who estimated 70% effectiveness as an overall effectiveness for the control measures..
- All respondents reported dissatisfaction of users on using passwords and authentication and a 25 second tolerance by users for completing a transaction were reported.

- All respondents emphasized the need for a formal methodology in evaluating intangible damages. Only one respondent provided an approach for evaluating damages to reputation,
- Although most of the respondents were interested in transferring risks to insurance companies, they had concerns about issues such as: lack of formal methods for damage assessment, deductibles, covered items, and above all, confusing policies.

7.3 Round Two and Summary of the Results

At the second round we asked the following questions to expand on and to verify the responses given in round one:

In our first round of interviews with information security experts, we found the following as the top 3 important threats to information assets (ranked in order of importance):

1- Theft of proprietary/ disclosure of information
2- Virus
3- Denial of service attacks

1- Do you agree with this order? If not, what order do you suggest?

2- Do you agree that a company may experience these attacks as following:

Theft of proprietary/ disclosure of information: Rarely to once a year

Virus: Once every 3 months

Denial of service: Once a year

3- Do you agree with the following control measures for these threats and their effectiveness:

For theft of proprietary/ disclosure of information threats control measures can be listed as:

Perimeter router

Multiple intrusion detection systems

Access control

Firewall

System Log

For virus:

Access control

Virus scanners

For Denial of Service attacks:

Access Control

Firewall

Proactive methods such as application software

If so, what are the effectiveness of these control measures? What other control measure(s) do you suggest for these threats and what do you estimate the effectiveness of this control measure?

All of the respondents agreed with the following ranking of threats in the order of importance:

1- Theft of proprietary/ disclosure of information

2- Virus/worm attacks

3- Denial of service attacks

One expert said:

"I agree, number one could be very costly to a business,

while two and three can be managed to a degree"

All of the respondents said that frequency of theft of proprietary information, or disclosure of information, was estimated to be more than just once a year. It was also stated that under several circumstances most of these attacks did not receive publicity. Virus attacks are expected by respondents on a daily basis.

The following is a sample comment by one expert:

"I think you are correct in your response, only because this is about how often the above incidents are reported. The first incident is very rarely reported, while the second is known due to the publicity that is reported throughout the industry. As to a DoS attack, with better security and equipment, we don't hear from the victims as much as we used to. This may also be due to the fact that Internet providers are more proactive in stopping DoS attacks"

The following control measures were approved as effective control measures:

For the theft of proprietary/ disclosure of information threat:

- Perimeter router
- Multiple intrusion detection systems
- Access control
- Firewall
- System Log

(Encryption, IDS, separation of duties, and web content filtering were also suggested by some respondents)

For virus:

- Access control
- Virus scanner

(Inline IDS was also recommended)

For denial of service:

- Access control
- Firewall
- Proactive methods such as application software

(Application firewall running alongside the perimeter routers, border routers, and bandwidth shapers were also suggested by some respondents)

The results of the research also indicate that stronger control measures can cause dissatisfaction on the part of clients and the maximum response time to a mouse click should be les than 25 seconds.

The following is a sample comment by one expert regarding selecting the effective control measures:

> *"I agree 100 percent; the stronger the control measures, the more dissatisfied the client. People are very impatient, and their time is very valuable. Client's days are very busy and complicated, and in order to generate a good work product, they cannot be frustrated by security controls that have been put in place. Installing complicated security measures, slows down the system, and*

distracts the client. As to a reasonable time, I do not know, but we both know the faster the better"

Chapter 8

Contributions and Conclusions

This research addresses some of the security issues faced by an organization engaged in e-commerce as well as some useful information for managers to deal with these issues. This research provides the state of the art of information security practice.

It explains how firms determine where to deploy resources in information security and how costs of similar incidents can vary from one company to another. Therefore, it is difficult to "standardize" a procedure or to come up with a single universal model to apply in estimating the costs of measures and the damages due to breach of security. Governance, policy, architecture, awareness and training, technology, auditing, reporting and monitoring, and validation are recommended as a minimal set of elements to be considered in an effective information security program.

The next area of contribution is a comparison of tangible with intangible costs reported from information security incidents. This research, through a comprehensive literature review, personal interviews, and case studies, concludes that the impact of an information system security incident on an organization, may well be financial, in terms of immediate costs and losses; however, long term intangible damages may prove to be more serious. Damage to the brand image, public reputation, goodwill in the market place, public and customer confidence in the accuracy of business transactions are some examples of intangible damages from disclosure of confidential data. These intangible

damages could result in millions of dollars, compared to hundreds of thousands of dollars damage from attacks to network services

The third area of contribution of this research is the adaptation of subjective probability assessment to empirical data and applying it to the information security area. Acquiring data for information security incidents is difficult because of the negative impact of the announcement of a security breach on an organization. This research suggests subjective probability assessment as an alternative. It is suggested to use the NIST's guidelines for ranking threats, to use NSA's 18 areas of information security assessment, and finally to use checklists for vulnerability assessments which can lead an organization to estimate probabilities of the occurrences of incidents.

This research addresses some of the shortcomings of existing classifications of threats to information systems and their control measures and considers threats from two points of view: 1- Threat agent, and 2- Threat technique. Threat agent could be environmental factors, authorized users, and unauthorized users; threat (penetration) technique could be personnel, physical, hardware, software, or procedural. Providing authentication, access control, data confidentiality, data integrity and non-repudiation services are presented as control measures to these threats.

This research developed an overall risk management system for security managers to enable them to allocate their resources in the most effective manner and to select the most effective control measure. This system consists of five parts: 1- Resource and application value analysis, 2-Vulnerability analysis, 3- Computation of losses due to threats and benefits of control measures, 4- Selection of control measures, and 5- Evaluation of implementing alternatives.

This research, through a comprehensive literature review, case studies, and personal interviews, has identified the order of importance of threats to information systems of organizations as follows:

1- Theft of proprietary/ disclosure of information

2- Virus/worm attacks

3- Denial of service attacks

Respectively, this research identifies perimeter router, multiple intrusion detection systems, access control, firewall, and system logs as control measures for the first threat; access control and virus scanners for the second threat; and finally, access control, firewall, and proactive methods as effective control measures for denial of service attacks.

This research has developed broader impacts of solving business problems of information security by:

- Making information-related losses public would create the necessary conditions for the formation of an economically efficient information security market. These conditions currently do NOT exist.
- Publishing dollar loss information would create clear cost-justification for use of effective security solutions.
- Assisting executives in the private sector and insurance agents in their assessments. Insured losses would create incentives for improvement of information security practices and technologies. Furthermore, loss of information would provide a monetary unit by which the effectiveness of practices and technologies could be measured.

This research has also developed broader impacts of solving technical problems of information security:

- The financial and legal system is already set up to deal with issues of financial liability; but, it is not yet set up to deal with problems of loss and liability. If security problems can be made into financial and legal problems, the financial and legal systems can stop imposing artificial and counterproductive constraints on the way technology is designed and built.
- Insuring information security losses, and making information about product effectiveness public, will create incentives for technology improvement and metrics which can be used to measure improvement.

Chapter 9

Future work

One of the objectives of this research is to assist managers in choosing appropriate control measures for security threats. As explained in previous sections, this research assigns five control measures to threats to information systems. Future work would involve choosing control measures for each threat. The level of control measure, (L), effectiveness (E), and cost (C) of control measure will also be introduced. In the equations presented in Section 6-2-4, the joint effectiveness of the control measures have been considered. To be practical, real numbers have to be inserted in this control measure (L, E, C) variable. The numbers will be estimated by interviewing security managers. This result will then be used in our five-stage risk analysis system as in Table 6.

Table 6- Threat-control measure relation, effectiveness values by level

		Authentication	Access Control	Data Confidentiality	Data Integrity	Non Repudiation
Unauthorized User	Software					
	Hardware					
	Procedural					
	Personnel					
	Physical					
Authorized User	Software					
	Hardware					
	Procedural					
	Personnel					
	Physical					
Environmental Factor	Software					
	Hardware					
	Procedural					
	Personnel					
	Physical					

Another area of future research is a tradeoff analysis between the cost of security measures-the incident rate-reliability as a measure of safety. A multi-objective optimization approach could be used here to find the Pareto set of solutions.

Measuring the effectiveness of control measures can be accomplished in a three-stage process:

1- A comprehensive list of available control measures, along with information about the cost of acquiring, managing, and maintaining each control measure, needs to be developed.

2- For each incident identified, information needs to be collected about which control measure was/were in use at the time of the incident, which control measure was bypassed, and/or defeated.

3- How much time and effort were required to bypass and or/defeat the control measure in place?

Bibliography

[1] Alberts, C., Dorofee, A., *Managing Information Security Risks, The Octave Approach*, SEI Series, Addison Wesley, 2003.

[2] Anderson, R., "Why Information Security is Hard- An Economic Perspective", *17th Annual Computer Security Applications Conference*, Dec. 2001.

[3] Bennett, S.P., Kailay, M.P**, "**An application of qualitative risk analysis to computer security for the commercial sector**",** *Eighth Annual IEEE Computer Security Applications Conference*, Nov.-4 Dec. 1992, pp.64–73.

[4] Bishop, M., *Computer Security, Art and Science*, Addison Wesley, 2003.

[5] Blakley, B., "The Measure of Information Security is Dollars", *Workshop of Economics and Information Security*, May 2002.

[6] Blakley, B., McDermott, E., Geer, D., "Information Security is Information Risk Management", *Proceedings of the 2001 workshop on New security paradigms*, 2001, pp. 97-104.

[7] British Security Standard, BS 7799, *British Standards*, 1999.

[8] Butler, S. A., "Security Attribute Evaluation Method: A Cost-Benefit Approach", *Proceedings of the 24th international conference on Software engineering*, ACM, May 2002, pp. 232-240.

[9] Caloyannides M. et al., US E-Government Authentication Framework and Programs, *IT Professional*, IEEE, Vol.5, Issue 3 , May-June 2003, pp. 16 – 21.

[10] Camp, L.J., and Wolfram, C., Pricing Security , *Proceedings of the CERT Information Survivability Workshop*, Boston, MA Oct. 24-26, 2000, pp. 31-39.

[11] Campbell, K., Gordon, L. A., Loeb, M. P., Zhou, L., "The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market", *Journal of Computer Security*, Vol. 11, 2003, pp. 431-448.

[12] Campbell R. P., Sands, G. A., " A Modular Approach to Computer Security Risk Management", *1979 National Computer Conference*, AFIPS Conference Proceedings, June 1979, pp. 293-303.

[13] Carter R., "The Threat to Computer Systems-Learning the Rules of Risk", Accountancy, 1987.

[14] Cavusoglu, H., Mishra B., Raghunthan S., "The Effect of Internet Security Breach Announcements on Market Value of Breached Firms and Internet Security Developers", Ph.D. Thesis, The University of Texas at Dallas, Feb. 2002.

[15] CIC Security Working Group, Incident Cost Analysis and Modeling Project, University of Michigan, 1997.

[16] Cohen, 1997, http://citeseer.nj.nec.com/lee00toward.html

[17] Cohen, F., "A Cost Analysis of Typical Computer Viruses and Defenses", *Computers & Security*, Vol. 10, 1991, pp. 239-250.

[18] DeMillo, R., Dobkin D. P., "Recent Progress in Secure Computation", *The IEEE Computer Society's Second International Computer Software and Applications Conference*, Nov.1978, pp. 209–214.

[19] Denning, D., *Information warfare and Security*, Addison Wesley, 1999.

[20] Dobson, J., "Messages, Communication, Information Security and value", *Proceeding of the New Security Paradigms Workshop*, IEEE, Aug. 1994, pp. 10-18.

[21] Eklund, B., "*Business Unusual*", netWorker, Vol. 5, Iss. 4, pp. 20-25.
Eschellbeck,G., *"*Active Security- A Proactive Approach for Computer Security Systems, *Journal of Network and Computer Applications*, No. 23, 2000, pp.109-130.

[22] Farahmand, F. and Navathe, S.B., *A Security Risk Management Model for Electronic Commerce and Security*, in preparation, 2004.

[23] Farahmand, F., Navathe, S. B., Sharp Gunter P.*,* Enslow, P. H., Data Confidentiality in E-Government and E-commerce*", Proceeding of The 2004 International Conference on Security and Management, SAM'04*, Las Vegas, 2004.

[24] Farahmand, F., Navathe, S. B., Sharp Gunter P.*,* Enslow, P. H., Managing Vulnerabilities of Information Systems to Security Incidents, *ACM ICEC 2003*, Pittsburgh, Sept. 2003.

[25] Farahmand, F., Malik, William J., Navathe, S. B., Enslow, P. H., "Security Tailored to the Needs of Business"*, Proceeding of the ACM CCS BIZSEC, Oct. 2003*.

[26] Farahmand, F., Navathe, S. B., Enslow, P. H., Electronic Commerce and Security – a Management Perspective, *ISS/INFORMS Seventh Annual Conference on Information Systems and Technology*, San Jose, 2002.

[27] Federal Standard 1037C, 1996, cited in joint Chiefs of Staff, Information Assurance; Legal, Regulatory, Policy and Organizational Considerations, 3rd ed., U.S. Dept. of Defense, Sept. 17, 1997.

[28] Freeman, "Cyber Risk Management and National Strategy to Secure Cyberspace", *The Open Group Conference Proceeding*, Feb. 2003.

[29] Gardner, P. E., "Evaluation of Five Risk in Aiding Management Decisions", *Computers & Security*, Vol. 8, Iss. 6, Oct. 1989, pp. 479-485.

[30] Geer, D. E., "Making Choices to Show ROI", *Secure Business Quarterly*, Vol. 1, Iss. 2, 2001, pp. 1-3.

[31] Ghosh, A. K., Swaminatha, T. M., Software Security and Privacy Risks in Mobile E-Commerce, *Communications of the ACM*, Feb. 2001, Vol. 44, No. 2, pp. 51-57.

[32] Gordon L. A., Loeb, M. P., *"Return on Information Security Investments"*, *Strategic Finance*, Nov. 2002.

[33] Gordon, L. A., Loeb, M. P., Sohail, T., "A Framework for using Insurance for Cyber-Risk Management", *Communications of the ACM*, Vol. 46, No. 3, March 2003, pp. 81- 85.

[34] Grzebiela, T., "Insurability of Electronic Commerce Risks", *Proceeding of the 35th Hawaii International Conference on System Sciences, HICSS'02*, Volume 7, Jan 2002.

[35] Hearn, J., "Does Common Criteria Paradigm Have a Future", *IEEE Security and Privacy*, 2004, pp. 64-65.

[36] Held, G., "Hacker Insurance-Will You Ever See A Payout?", *International Journal of Network Management*, Vol. 11 , Issue 2, March-April 2001, pp. 73 – 74.

[37] Henning, R. R., Security Service Level Agreements: Quantifiable Security for the Enterprise? *ACM Proceedings of the 1999 Workshop on New Security Paradigm*, Sep. 1999, pp. 54-60.

[38] Hiles, A., "Surviving a Computer Disaster", *Engineering Management Journal*, Dec. 1992, pp. 271-274.

[39] ISO, Information Processing Systems- Open Systems Interconnection-Basic Reference Model, Part 2: Security Architecture, *ISO 7498-2, 1989*.

[40] ISO/IEC TR 13335-l, "Information technology - Guidelines for the management of IT Security - Part 1: Concepts and models for IT Security", ISO/IEC, 1996.

[41] Landwehr, C. E., et. al, A Taxonomy of Computer Program Security Flaws, with Examples, Naval Research Laboratory, Nov. 1993.

[42] Law 1947, United States vs. Carroll Towing Company, 159 F.2d 169, 173 (2d Cir. 1947).

[43] Lindqvist, U., and Jonsson, E, How to systematically classify computer security intrusions**,** *IEEE Symposium on Security and Privacy*, 1997, pp. 154 –163.

[44] Lipmann, R., et. al, The 1999 DARPA off-line Intrusion Detection Evaluation, *Computer Networks*, Vol. 34, 2000, pp. 579-595.

[45] Miguel, J., "A Composite Cost/Benefit/Risk Analysis Methodology", *Computer Security, IFIP*, 1984, pp. 307-311.

[46] Nemzow, M., "Business Continuity Planning", *International Journal of Network Management*, Vol. 7, 1997, pp. 127-136.

[47] Neumann , P., "*Computer-Related Risks*", Addison-Wesley, 2000.

[48] Neumann, P. G., and Parker, D. B., A Summary of Computer Misuse Techniques. *Proceedings of the 12th National Computer Security Conference*, Oct. 1989, National Institute of Standards and Technology/National Computer Security Center, pp. 396-407.

[49] Orlandi, E., "The Cost of Security", *Proceeding of the 25th Annual IEEE International Carnahan Conference on Security Technology*, Oct. 1991, pp. 192 – 196.

[50] Orlandi, E., "*Computer Security Economics*", ICCST, 1989, pp. 107-111.

[51] Pate-Cornell, E., and Guikema, S., "Probabilistic Modeling of Terrorist Attacks: A System Analysis Approach to Setting Priorities Among Countermeasures, *Military Operation Research"*, October 2002.

[52] Pfleeger, C. P., Security in Computing, *Prentice Hall*, 1997.

[53] Posner, R. A., *Economic Analysis of Law*, 4th edition (Boston: Little, Brown & Co., 1992), pp. 164.

[54] Power, R., Computer Security Issues & Trends, *2002 CSI/FBI Computer Crime and Security Survey*, Vol. VIII, No. 1, Spring 2002.

[55] Schneier, B., "No, We Don't Spend Enough", *Workshop of Economics and Information Security*, May 2002.

[56] Schneier, B., "Insurance and the Computer Industry", *Communications of the ACM,* Vol. 44, No. 3, 2001, pp. 114-115.

[57] Schummacher, H., J., and Ghosh, S., A Fundamental Framework for Network Security, *Journal of Network and Computer Applications*, 1997, pp. 305- 322.

[58] Soo Hoo, K., "How much is Enough? A Risk Management Approach to Computer Security", *Workshop on Economics and Information Security*, University of California, Berkeley, May 16-17, 2002.

[59] S & P, Industry Surveys, Standards and Poor's, McGraw-Hill, 2002.

[60] S & P, Industry Surveys, Standards and Poor's, McGraw-Hill, 2001.

[61] S & P, Industry Surveys, Standards and Poor's, McGraw-Hill, 1999.

[62] Stalling, W., "Network Security Essentials", Prentice Hall, 1999.

[63] Stonebumer, G., Goguen, A., and Feringa, A., Risk Management Guide for Information Technology Systems, *NIST Special Publications 800-30*, 2001.

[64] Tang, F. F., et. al, "Using Insurance to Create Trust on the Internet", *Communications of the ACM*, Vol. 46, No. 12, Dec. 2003., pp. 337- 344.

[65] Tarr, C.J., Cost effective perimeter security**,** Security and Detection, *European Convention on Security and Detection*, 1995, pp. 183 –187.

[66] Tudor, J. K., Information Security Architecture, "An Integrated Approach to Security in the Organization", Auerbach, 2000.

[67] Turn R., "Security and Privacy Requirements in Computing", *ACM Fall Joint Computer Conference*, 1986.

[68] Vetterling M., Wimmel G., "Secure Systems Development Based on the Common Criteria: The PaIME Project", *ACM, SIGSOFT,* Nov. 2002, pp. 129-138.

[69] Wong, K., Watt, S., Managing Information Security: A Non-technical Management Guide, Elsevier Advanced technology, 1990.

[70] Wood, Charles C., et. al. *Computer Security; A comprehensive Control Checklist*, John Wiley & Sons, 1987.