# Comparison of Recovery Requirements with Investigation Requirements for Intrusion Management Systems

By

Dilek TAPUCU ARPAÇAY

A Dissertation Submitted to the
Graduate School in Partial Fulfillment of the
Requirements for the Degree of

MASTER OF SCIENCE

Department: Computer Engineering
Major : Computer Software

İzmir Institute of Technology
İzmir, Turkey

June, 2002

We approve the thesis of **Dilek TAPUCU ARPAÇAY**

**Date of Signature**

............................................................ **28.06.2002**

**Asst. Prof. Dr. Tuğkan TUĞLULAR**
Supervisor
Department of Computer Engineering

............................................................ **28.06.2002**

**Assoc. Prof. Ahmet KOLTUKSUZ**
Department of Computer Engineering

............................................................ **28.06.2002**

**Asst. Prof. Cenk ERDUR**
Department of Computer Engineering

............................................................ **28.06.2002**

**Prof. Dr. Sıtkı AYTAÇ**
Head of Department

# ACKNOWLEDGEMENTS

Many people have made contributions to the development of this work. First, I would like to thank my thesis advisor Asst. Prof. Tuğkan Tuğlular Ph.D. for his guidance during the long process of the thesis. I would also like to thank Assoc. Prof Koltuksuz, Ph.D. for his valuable and continuous support.

I thank all my friends at IYTE for their friendship and support. I thank my family, for supporting me throughout my educational career.

# ABSTRACT

Computer systems resources and all data contained in the system may need to be protected against the increasing number of unauthorized access, manipulation and malicious intrusions. This thesis is concerned with intrusion management systems and specially with their investigation and recovery subsystems. The goals of these systems are to investigate intrusion attempts and recover from intrusions as fast as possible. In order to achieve these goals me should observe the fact that some of the intrusion attempts will be eventually successful should be accepted and necessary precautions should be taken.

After an intrusion has taken place, the focus should be on the assessment: looking at what damage has occurred, how it happened, what changes can be made to prevent such attacks in the future. In this thesis, requirements of investigation and recovery process are determined and related guidelines developed. The similarities and differences between these guidelines are explained.

# ÖZ

Bilgisayar sistem kaynaklarının ve sistemdeki tüm verilerin gittikçe artan sayıdaki yetkisiz erişime, ve kötü niyetli sızmalara karşı korunmaya ihtiyacı vardır. Bu tez çalışmasındada, Nüfuz Yönetim Sistemleri ve özel olarak onların soruşturma ve kurtarma alt-sistemleri dikkate alınmıştır. Bu alt-sistemlerin amacı sızma denemelerini araştırmak ve sistemi nüfuzdan olabildiğince çabuk bir şekilde kurtarmaktır. Bu amaca ulaşmak için bazı nüfuz denemelerinin başarılı olacağı kabulu yapılıp, gerekli önlemler alınmalıdır.

Nüfuz gerçekleştikten sonra; zararın ne olduğuna, nüfuzun nasıl yapıldığına ve yakın gelecekte benzeri nüfuzlardan korunmak için ne gibi değişiklikler yapılması gerektiğine bakılarak, zararın değerlendirilmesine odaklanılmalıdır. Bu tez çalışmasında, soruşturmanın ihtiyaçlarına ve sistemin eski durumuna getirilmesi süreçleri ortaya konulmuş ve ilgili kılavuzlar geliştirilmiştir. Ayrıca, kılavuzlar arasındaki benzerlikler ve farklılıklar açıklanmıştır.

# TABLE OF CONTENTS

# LIST OF FIGURES

# LIST OF TABLES

# Chapter 1

# INTRODUCTION

Computer systems and the information they store are valuable resources that need to be protected. An intrusion can be any irregular or adverse event that occurs on any part of the organization and deals with violations of an organization's computer usage policies. There are many different types of intrusions, which may include, malicious code attacks, probes and network mapping, denial of service, espionage, hoaxes and system and network intruders.

Simply detecting that an intrusion has occurred within a domain is only the first step of the solution to the security incident problem. It should be followed by determination of the focal point of the intrusion, and thorough analysis of all information pertaining to the victim. Moreover, the attack should be stopped from progressing, and it is necessary to assure that it will not happen again. Intrusion investigation and intrusion recovery is an integral part of intrusion management systems.

The main goal of intrusion management systems is to investigate intrusion attempts. Such an investigation aim to identify the perpetrator of an attack, the motivations of perpetrator and the means used in the attack. Moreover, investigation should collect and preserve evidence in such a way that it should be admissible in courts. Because of the nature of computers, collecting evidence and tracing perpetrators are not easy. For successful investigation, appropriate measures should be taken beforehand.

Another goal of intrusion management systems is to recover from intrusion incidents as fast as possible. To achieve this goal, the fact that some of the intrusion attempts will be eventually successful should be accepted and necessary precautions should be taken. The problem with recovery is that the last stored state of the information system may not be up-to-date and complete. In that case, a successful restoration is not possible and some information may be lost, which may increase the damage done by the intrusion. Therefore, the requirements of recovery process should be determined very carefully. In this thesis, the proposed work addresses the requirements of intrusion investigation, intrusion recovery and also implements practical guidelines.

Standards and guidelines specify technologies and methodologies to be used to assist users, systems personnel, and others in effectively securing their systems. Procedures normally assist in complying with applicable security policies, standards, and guidelines. They are detailed steps to be followed by users, system operations personnel, or others to accomplish a particular task and procedures established should provide thorough guidelines on what to do if a security intrusion is discovered. In addition, the procedures should compromise of roles and responsibilities, who to contact and when to contact someone.

In this thesis, guidelines and procedures serve as a guide to Information System Security Officer (ISSO) preparing proposed Intrusion Investigation Process and Intrusion Recovery Process for the conduct and management of their systems. Also this thesis explains a comparison of the requirements of investigation process with the requirements of recovery process.

Guidelines of investigation process are examined, and the procedures used by each are outlined. Intrusion recovery process is also examined, and procedures by each are outlined. The result of these study aid requirements should be determined and compared whether a correlation exists.

The remainder of the thesis is organized as follows. The second chapter provides background on computer crime, computer security, risk assessment, security policy and intrusion management. Chapter 3 examines the methodology of Intrusion Model and Intrusion Management System Model. Chapter 4 and 5 discusses Intrusion Investigation and Intrusion Recovery. Chapter 6 compares the investigation requirements with recovery requirements. The final chapter presents conclusions and suggestions for future work.

# Chapter 2

# BACKGROUND

With increased requirements for interconnection in today’s networks comes the increased vulnerability to abuse and misuse of computer systems. Typically, information protection architectures have focused on the management of access to sensitive or critical information assets. This approach has often been in conflict with the need to respond to breaches of access control. Most classical information protection approaches emphasize the prevention and protection aspects of data security, excluding the investigative requirements of responding to attempted and successful penetrations.

In this chapter, importance of computer security, risk assessment, security policy is discussed and the intrusion management is reviewed.

## 2.1 Computer Security

In a generic sense, security is "freedom from risk or danger" [Kangasluoma, 2001]. In the context of computer science, security is the prevention or protection against,

- access to information by unauthorized recipients,
- intentional but unauthorized destruction or alteration of that information
- denial of service [Oxford University Press, 1996].

Protection can be provided through any combination of various controls, such as physical (e.g., cipher locks on doors), personnel (e.g., clearances), procedural (e.g., use of passwords), or computer (e.g., file access control lists) mechanisms.

The objective of computer security is to improve protection of information and information processing resources. A critical component of the computer security is the risk assessment. The purpose of the risk assessment is to identify assets of the system, threats that could affect the confidentiality, integrity, or availability of the system, system vulnerabilities to the threats, potential impacts from threat activity, protection requirements to control the risk, and selection of cost effective security measures. Risk assessment is examined in Section 2.3.

For each asset, the basic goals of security are confidentiality, integrity and availability.

**Confidentiality** ensures that there is no deliberate or accidental improper disclosure of sensitive automated information [The Computer Security Handbook of CIT, 2002]. This means that the information in a computer system is accessible only by authorized parities. Authorized access includes printing, displaying, reading or knowledge that information even exists. Many computer systems store information that is highly sensitive, due to user privacy requirements (such as the secure storage of personal communications in electronic mail) or organizational secrecy requirements (such as private financial data or proprietary software). Threats to confidentiality allow an attacker to gain access to this information illicitly.

**Integrity** ensures that stored data and data in transit are not modified unintentionally or maliciously. In lay usage, information has integrity when it is timely, accurate, complete, and consistent. However, computers are unable to provide or protect all of these qualities. Therefore, in the computer security field, integrity is often discussed more narrowly as having two facts *data integrity* and *system integrity*. "Data integrity is a requirement that information and programs are changed only in a specified and authorized manner" [National Research Council, 1991]**.** System integrity is a requirement that a system "performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system" [National Research Council, 1991].

**Availability** is the property or process of ensuring that data held on a computer system is always available to those users or processes that are authorized to access the data. It thus involves protection against accidental loss or corruption of data (through adequate backup, for example) on the one hand, and the prevention of deliberate acts of sabotage, such as denial of service (DoS) attacks from the Internet.

## 2.2 Computer Security and Risk Assessment

Risk is the possibility of something-adverse happening. The purpose of the security risk is to identify combinations of threat, vulnerability, and impact (called risks) that deserve further attention. There are two elements of a risk analysis:

- Identifying the assets,
- Identifying the threats.

### 2.2.1 Identifying the Assets

One step in a risk analysis is to identify all the things that need to be protected. Some things are obvious like valuable proprietary information. *Pfleeger* [Rfc 1244] suggests one list of categories; this list is adapted from that source:

1- Hardware: CPUs, boards, keyboards, terminals, workstations, personal computers, printers, disk drives, communication lines, terminal servers, routers.

2- Software: source programs, object programs, utilities, diagnostic programs, operating systems, communication programs.

3- Data: during execution, stored on-line, archived off-line, backups, audit logs, databases, in transit over communication media.

4- People: users, administrators, and hardware maintainers.

5- Documentation: on programs, hardware, systems, and local administrative procedures.

6- Supplies: paper, forms, ribbons, magnetic media.

### 2.2.2 Identifying the Threats

Once the assets requiring protection are identified, it is necessary to identify threats to those assets. The threats can then be examined to determine what potential for loss exists. The following are classic threats;

- Unauthorized access to resources and/or information.
- Unintended and/or unauthorized disclosure of information.
- Denial of service.

Management is concerned with many types of risk. Computer security risk management addresses risks, which arise from an organization's use of information technology. This section is organized by the three phases of an ongoing risk management process: performing a risk assessment; addressing the mitigation of that risk; and level of risk determination.

### 2.2.3 Risk Definition

Risks are the resultant value derived from the mapping of known and perceived threats against known and perceived vulnerabilities. In qualifying the risks during the risk analysis process, a decision is made about which threats and vulnerabilities need to be controlled and managed. The application of security countermeasures should then be selected and applied against these specifically defined risks [National Research Council, 1991].

### 2.2.4 Functions of Risk Management

Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk [National Institute of Standards, 2001]. Each risk nominally goes through functions sequentially, but the activity occurs continuously, concurrently (e.g., risk are tracked in parallel while new risks are identified and analyzed), and iteratively ( e.g., the mitigation plan for one risk may yield another risk) throughout the project life cycle [National Research Council,1999]. The risk paradigm is shown in Figure 2.1. This figure shows the basic functions of managing risks; identify, analyze, plan, track, control and communicate.

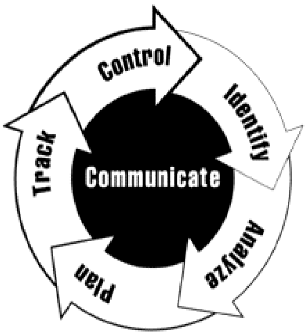

Figure 2.1 Risk Paradigm [National Research Council, 1991].

**Identify,** search for and locate risks before they become problems. Before risks can be managed, they must be identified.

**Analyze,** transform risk data into decision-making information. Evaluate impact, probability, and timeframe, classify risks, and prioritize risks.

**Plan,** translate risk information into decisions and mitigating actions (both present and future) and implement those actions.

**Track,** monitor risk indicators and mitigation actions, consists of monitoring the status of risks and the actions taken to alleviate them.

**Control,** correct deviations from planned risk actions. Risk control is a part of project management and relies on project management processes to control risk action plans, correct for variations from plans, respond to triggering events, and improve risk management processes.

**Communicate,** provide information and feedback internal and external to the project on the risk activities, current risks, and emerging risks. Communication happens throughout all the functions of risk management.

## 2.3 Risk Assessment Methodology

The output of risk management process is the residual risk and a determination whether this is at an acceptable level or whether additional security controls should be implemented to further reduce risk [National Research Council, 1991]. Risk is a function of the likelihood of a security event. To determine likelihood, threats to the system are analyzed in conjunction with the vulnerabilities present. This methodology is represented in Figure 2.2, the individual components are described in sections 2.3.1 through 2.3.4.

### 2.3.1 System Characterization

Characterizing the system establishes the scope of the risk management effort and provides information essential to defining the risk. In this step, boundaries of the system are identified, along with the resources and information that constitute it. Assets are classified as the following [National Research Council, 1991]:

- information infrastructure,
- hardware,
- data and information,
- system interfaces and connectivity,
- the processes performed by the system,

- the functional requirements of the system,
- users of the system,
- all applicable system security policies,
- system security architecture,
- the operating environment of the system,
- the information storage requirements of the system,

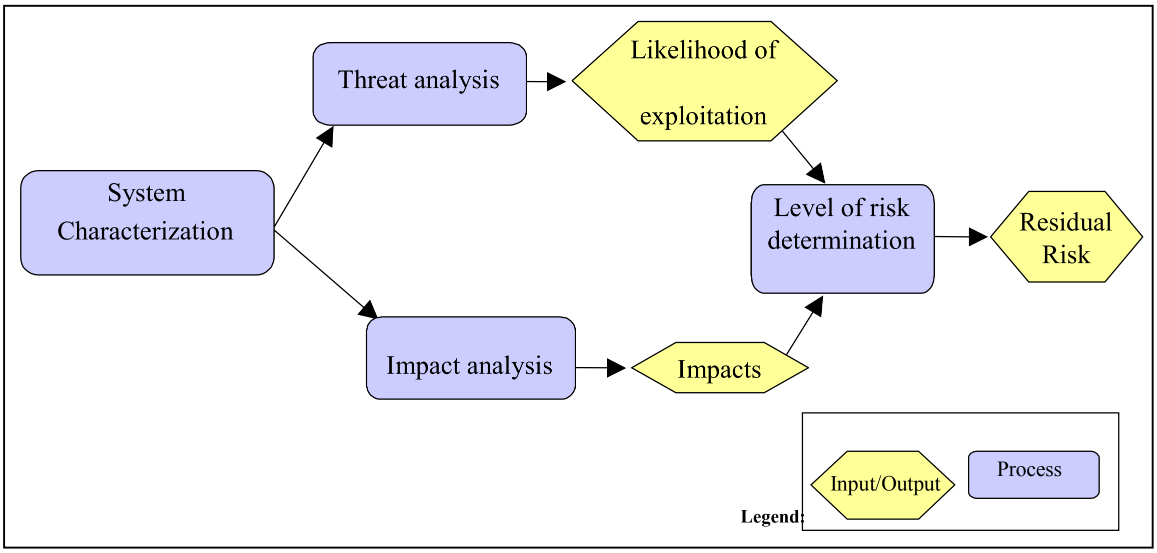

Figure 2.2 Risk Assessment Methodology [National Research Council, 1991].

### 2.3.2 Threat Analysis

Threat is expressed as a function of the likelihood that a given threat-source will successfully exploit a given vulnerability. Without a vulnerability that can be exercised, a threat-source does not present a risk [National Research Council, 1991]. In determining likelihood, one must consider vulnerabilities, threat-sources, and existing controls, as described below.

#### 2.3.2.1 Vulnerability Analysis

The goal in this step is to develop a list of the system flaws or weaknesses that could be exercised by the potential threat-sources. This step systematically evaluates the technical and non-technical weaknesses associated with the system [National Research

Council, 1991]. This information is collected via site surveys, interviews with personnel responsible for the system, network-scanning tools, and available system.

### 2.3.2.2 Threat - Source Identification

The goal in this step is to identify a threat-source, which is a human. A threat-source is defined as any circumstance or event with the potential to cause harm to an information system. Threat-source can either be intentional - a deliberate attack - or unintentional. A deliberate attack can be a malicious attempt to gain unauthorized access to an information system to compromise its integrity, availability, or confidentiality [National Research Council, 1991].

In order for a human to be a valid threat-source, motivation and the resources to carry out the attack must be present. Table 2.1 below presents an overview of the types of attackers, what their motivations might be, and the means by which they might carry out the attack.

Table 2.1 Human Threats.

| Threat-source | Motivation | Means |
|---|---|---|
| Hacker, cracker | Ego<br>Challenge<br>Rebellion | **System Intrusion**<br>Unauthorized system access |
| Criminal | Illegal Disclosure<br>Alteration<br>Monetary Gain | Crime/**Intrusion**<br>Fraudulent act |
| Terrorist | Blackmail<br>Exploitation<br>Destruction | **System Attack/intrusion** |
| Foreign Interests | Classified Information<br>Other government interests | **Intrusion**/penetration |
| Insider (disgruntled, negligent, or dishonest employee) | Intelligence<br>Revenge<br>Ego<br>Monetary Gain | **Intrusion,** computer abuse, unauthorized system access |

### 2.3.2.3 Control Analysis

During this step, the organization determines whether the security requirements collected during system characterization are being met by existing or planned security controls. Typically, the system security requirements are presented in matrix form where an explanation can be included that describes how the system's design or implementation does or does not satisfy the specific security control requirement. Security controls for the system can be extrapolated from the following sources:

- Security policies and guidelines,
- System operating procedures,
- System security specifications

**Technical controls** are those safeguards incorporated in computer hardware, software or firmware. Table 2.2 lists some of the technical controls used to mitigate risk.

Table 2.2 Examples of Technical Controls [National Research Council, 1991].

| Prevent | Detect |
|---|---|
| ▪ Access control mechanisms<br>▪ Antivirus software<br>▪ Identification & Authentication mechanisms<br>▪ Firewalls<br>▪ Encryption | ▪ Audit trails<br>▪ Intrusion detection systems |

**Operational controls** are those operational procedures and personnel and physical security measures established to provide an acceptable level of protection for computing resources. Table 2.3 lists some of the operational controls used to mitigate risk.

Table 2.3: Examples of Operational Controls [National Research Council, 1991].

| Prevent | Detect |
|---|---|
| ▪ Security awareness and training<br>▪ Disaster recovery, contingency, and emergency plans<br>▪ Background investigations | ▪ Security reviews and audits |

**Management controls** are those security measures that focus on the management of the system and the management of risk. By their nature they all fall into the "prevent" category. They include security reviews and assessments, risk assessments, and rules of behaviour.

### 2.3.3 Impact Analysis

The next major step in the risk assessment process is to determine the mission impact resulting from the threats (exercise of a vulnerability by a threat-source). The impact of a security event can be described in terms of mission impacts attributed to loss or degradation of the three-security goals confidentiality, integrity, and availability.

## 2.4 Security Policy

A security policy is a "formal statement of the rules by which people who are given access to an organization's technology, system and information assets" [Weise Joel, 2001]. The main purpose of a security policy is to inform users, staff and managers of their obligatory requirements for protecting technology and information assets [Rfc 2196]. The policy should specify the mechanisms through which these requirements can be met. Another purpose is "to provide a baseline from which to acquire, configure and audit computer systems and networks for compliance with the policy" [Charles R. Martin, 2001]. Therefore an attempt to use a set of security tools in the absence of at least an implied security policy is meaningless.

A security policy needs to have the acceptance and support of all levels of employees within the organization in order to be appropriate and effective. It is especially important that corporate management fully support the security policy process otherwise there is little chance.

Standards, guidelines, and procedures must complete policies. These must ensure that all operations are consistent with the intent of the security policies. The organization should undertake the definition of standards, guidelines, and procedures only after the development of security policies. Within this policies, guidelines, and procedures are established, appropriate parts of these procedures can be implemented in intrusion investigation process and intrusion recovery process. And these relations are described in Chapter 4 and Chapter 5.

## 2.5 Intrusion Management

Intrusion is defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network [Shah, 2001]. The intent of intrusion may include denial of service, access to confidential data, or compromise of existing data. While introducing the concept of intrusion detection in

1980, *Anderson* defined an intrusion attempt or a threat "to be the potential possibility of a deliberate unauthorized attempt to

- access information,
- manipulate information, or render a system unreliable or unusable" [Anderson, 1980].

It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. This field of research is called intrusion detection.

The intrusion management concept comes down to a specific set of priorities before and after an attack. After an attack has taken place, the focus should be on the assessment: looking at what damage has occurred, whether or not prosecution is merited, what changes can be made to prevent such attacks in the future.

The purpose of the Intrusion Management is to limit the possibility of a successful intrusion through effective preventive, quality management and detective process, and facilitating successful investigation of an intrusion or an intrusion attempt should either occur [Stephenson, 1999]. Starting in late 1996, the *Stephenson* began the process of developing a simple yet comprehensive information protection model. The Intrusion Management model is based upon the assumption that the ultimate goal of the information protection process must be three-fold. First, the process seeks to protect information assets from compromise. Second, the process must recognize that compromise is inevitable and that measures must be taken in advance to facilitate a means for investigating the compromise and recovering, managing and protecting the evidence of the compromise for future use in legal proceedings. Finally, the process must provide feedback that can speed response to a compromise and generate information that can be used to prevent similar compromises in the future [Stephenson, 1999]. Later in 2001 Tuglular improved this model as a policy-based management [Tuglular, 2001] and investigation of intrusions is added as a new layer. This new Intrusion Management Model is a four-step process, which is explained in Chapter 3; the steps are **prevention, detection, investigation** and **recovery.**

### 2.4.1 Prevention

Prevention is described as all of those underlying processes implemented to create a secure environment and to avoid threats against information assets by using policies, and standards. Those processes may be administrative, as in policies, standards and practices, or they may be technological as in the application of access control tools. The following steps should be taken in the intrusion avoidance layer:

- Analyze system configurations and vulnerabilities,
- Analyze, define, coordinate, implement and audit,
- Conduct virus detection, prevention, and elimination,
- Identify needs,
- Identify security holes,
- Perform risk analysis on all systems.

### 2.4.2 Detection

Intrusion detection refers to the process of identifying attempts to penetrate a system and gain unauthorized access. If audit trails have been designed and implemented to record appropriate information, they can assist in intrusion detection. Although normally thought of as a real-time effort, intrusions can be detected in real time, by examining audit records as they are created, or after the fact (e.g., by examining audit records in a batch process). The goals are listed below;

- Monitoring and analyzing both user and system activities,
- Assessing system and file integrity,
- Ability to recognize patterns typical of attacks,
- Analysis of abnormal activity patterns,
- Conduct, coordinate and oversee network intrusion detection and analysis.

### 2.4.3 Investigation

Intrusion investigation involves determining whether or not an intrusion has occurred, and if one has occurred, determining the nature of the intrusion, tracing and abuses followed in a manner that facilitates appropriate responses. The following steps should be taken in the investigation phase:

- Collect, analyse, and preserve evidence and related data,
- Determine whether or not an event is actually an intrusion

- Determine scope of intrusion,
- Isolate the attack and determine how it was executed,
- Support legal investigations,
- Report all evidence to management,
- Tracking user policy violations,
- Understand the extent and source of an intrusion.

### 2.4.4 Recovery

This phase ensures that the system is returned to a fully operational status, and also the intrusion and vulnerabilities that allow re-entry to the system are eliminated. The following steps should be taken in the recovery phase:

- Asses damage and retore services,
- Document findings and make recommendations,
- Locate the most recent clean back up,
- Validate the system. Once the system has been restored, verify that the operation was successful and the system is back to its normal condition.

# Chapter 3

# METHODOLOGY

In this chapter, two distinct states of intrusion management system are described. The first state is comprised of *proactive* states driven by avoidance and detection layers. This state is controlled by the attacker. The attacker controls the intrusion time, and can take as much time or as little time as necessary to either cause or effect all the steps in the intrusion. The second one is the *reactive* states controlled by the defender with investigation and recovery layers in the intrusion management system. The defender with any positive actions commencing only after an action by the attacker has been detected. This means that, reactive states are implemented when the proactive states for the attack has failed. This state helps to identify the damage that was caused and the vulnerabilities that were exploited in the attack, determine why it took place, repair the damage that was caused by it.

Both states work together to develop security policies and controls to minimize attacks and the damage caused during them. In this section both the reactive and proactive states are explained.

## 3.1 Assumptions for Thesis Work

The identification of the intrusion is the evaluation of the scope and impact of the problem. It is important to correctly identify the boundaries of the intrusion in order to effectively deal with it. In addition, the impact of an intrusion determines its priority in allocating resources to deal with the event. Without an indication of the scope and impact of the event, it is difficult to determine a correct response [Rfc 1244].

The attacker usually performs extensive surveillance on the system, frequently mapping the network to find area to enter. Once the surveillance is completed, the attacker attempts intrusions. The exact point of the attack is to

- determine and analyze all information pertaining to the victim,
- actually stop the attack from progressing,
- assure that it will not happen again.

For the purposes of this thesis model, an intrusion management system capable of detecting break-ins, penetrations, and other forms of computer abuse has been proposed. The initial state of data is completely known at the beginning of the computation, in computer system and intrusion is detected with damage. It has been accepted that the priorities for sensitive data are changed according to these phenomena assumptions could be categorised into three classes;

1. The first category in applying computer security is to establish the relevant minimum standards required by policy for the system. Protective measures to meet the required security standards can then be selected.
    - the elements of the security policy that describe how intrusions are handled,
    - that the attack is serious enough, or complex enough, that standard security procedures are unlikely to be sufficient ,
    - the defender is usually in a reactive state,
    - specific assets of the system are identified such as information, service, programs.

2. The next step in applying computer security is to assess the threat levels for confidentiality, integrity and availability for the system and detect intrusions with some mechanisms.
    - network intrusion detection systems or host intrusion detection systems are available,
    - monitoring the network to detect illegitimate traffic,
    - monitoring individual computer systems for evidence of illegal access.

3. In this category assessment should seek to establish the potential damage of a successful attack in order to provide a cost basis for justifying security measures.
    - trusted data is available,
    - back-ups run regularly,
    - enable logging for system level,
    - daily reviews of security logs,
    - set up log archiving facility,

- transaction logs,
- transaction auditing,
- implement file integrity.

### 3.2 Defender Timeline

In this section defender timeline shows the major parts of the reactive states. After the attack has completed, the defender performs damage assessment to ascertain where the damage occurred, how the attack happened. The defender then selects optimum strategy to investigate and recover operation of the attacker. The main goal in analysing and understanding the nature of the timelines is to drive portions of the defender timeline closer with attacker timeline.

**Before intrusion** take the necessary steps to recover the system and sensitive data against the known attacks.

1- Security policy and procedures must outline steps to take in the event of a damage

- Identify backup points,
- Determine the required schedule of availability of system,
- Determine the schedule of database backup operations compatible with the operating schedule and provide the required data protection.

2- Data priorities must be defined to save data than to save system software and hardware.

**Priority One:** Protect classified and/or sensitive data. Prevent exploitation of classified and/or sensitive systems, networks or sites. Inform affected classified and/or sensitive systems, networks or sites about intrusion [Rfc 1244].

**Priority Two:** Protect other data, including proprietary, scientific, and managerial and other data, because loss of data is costly. Prevent exploitation of other systems, networks or sites and inform affected systems, networks or sites about successful intrusion [Rfc 1244].

**Priority Three:** Prevent damage to systems (for example, loss or alteration of system files, damage to disk drives, etc.). Damage to systems can result in costly down time and recovery [Rfc 1244].

**Priority Four:** Minimize disruption of computing resources (including processes). In many cases it is better to shut a system down or disconnect from a network than to risk damage to data or systems. Sites must evaluate the trade-off between shutting down and disconnecting, and staying up [Rfc 1244].

3- Start by backing up the system

- To monitor all sensitive actions,
- □□□□Determine the real threats,
- Focus on theoretical threats ,
- Determine known vulnerabilites,
- Use intrusion detection systems to determine if the security perimeters are being damaged.

**After intrusion occurred** and damage detected investigation and recovery processes start. The defender performs damage assessment. Collect information for better understanding of happened. Manage the volume of data, communications, and processing in system.

In order to determine the cause of the damage it is necessary to understand what resources the attack was aimed at and what vulnerabilities were exploited to gain access or disrupt services. Review system logs, audit logs, and audit trails. These reviews often help in discovering where the attack originated in the system and what other resources were affected. It is very important that the damage be repaired as quickly as possible in order to restore normal business operations and any data lost during the attack. The organization's Intrusion Recovery Plans and procedures (discussed in Chapter 5) should cover the restore strategy. The Intrusion Recovery Team should also be available to handle the restore and recovery process and to provide guidance on the recovery process.

Understand the extent and source of an intrusion. Implement strong reactive strategies to detect and then correct any damage. The defender can then select optimum strategy to recover operation of the system.

- Analyse and correlate logs from multiple source and determine what the intruder did,
- Check file integrity, system to ensure that which files were changed in an attack,
- Discover what weaknesses were exploited (for future prevention),
- Take steps to prevent further incursions,

- There appears to be no damage to data, but evaluating systems must be carefully to ensure no traces remain,
- If the attacker is actively damaging data, taking time to further establish the pattern of activity is going to be harmful.

In addition defender gathers the attacker's evidence. Intrusive evidence can be found in files and other data areas created as a routine function of the computer's operating system. Passwords, Internet activity, and temporary backup files are examples of data that can often be recovered and examined. There are components of files that may have evidentiary value including the date and time of creation, modification, deletion, access, user name or identification, and file attributes. However, the loss or compromise of data (especially classified or proprietary data) is usually not an acceptable outcome.

## 3.3 Overview of Intrusion Management System Model

Intrusion Management System Model is independent of any particular system, application environment, or type of intrusion, thereby providing a framework for a general-purpose intrusion management system, which is shown in Figure 3.1. This model has four main components and each one is described.

### 3.3.1 Avoidance & Prevention

Information security begins with avoidance and prevention. Intrusion prevention utilizes authentication, encryption and firewall etc. to protect system from being attacked and compromised. In this layer the important point is to determine what ISSO needs to protect, and how to protect it.

General security goal is to

- Prevent intrusions,
- Try to reduce the number of possible intrusions,
- Detect quickly any intrusions that did occur.

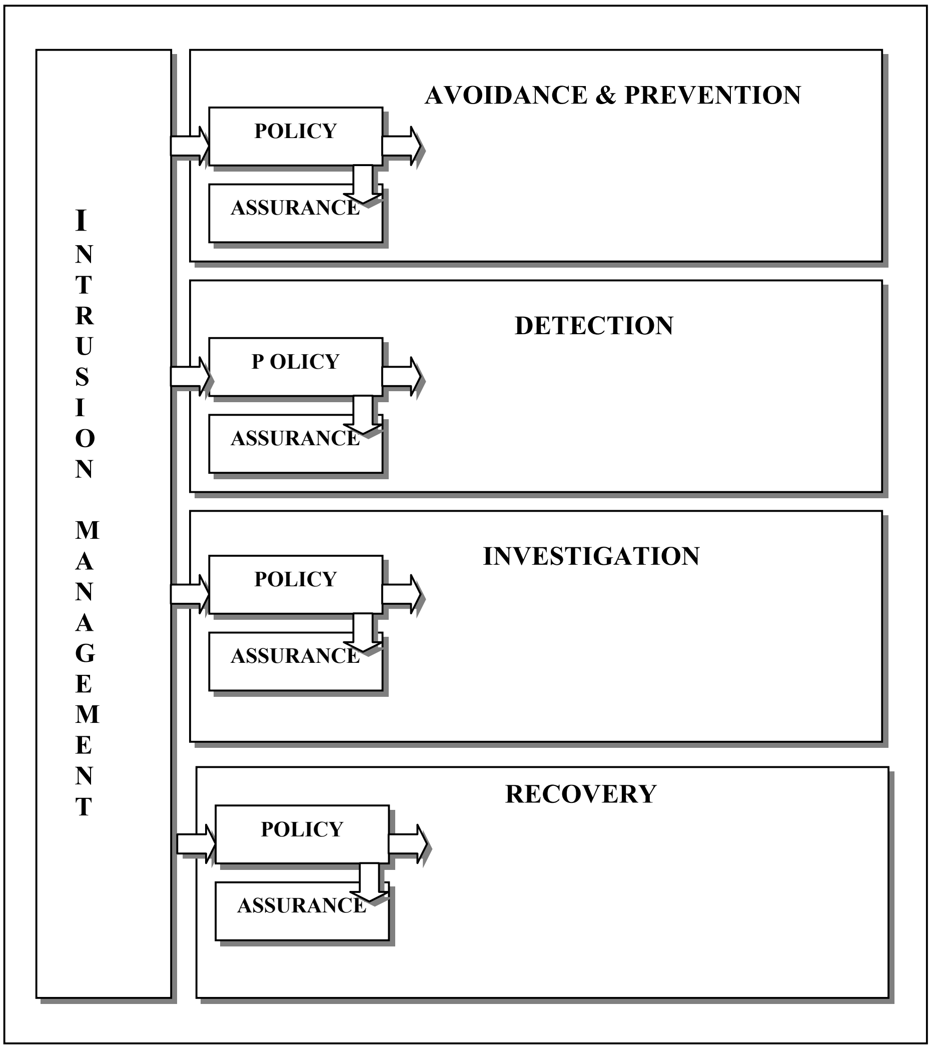

Figure 3.1 Intrusion Management Model.

Trying to reduce the number of intrusions would have to be accomplished by providing secure mechanisms for end users to access their computer systems and then educating those users and their system administrators about the proper usage of those secure mechanisms. Some of them are shown in Figure mechanisms 3.2.

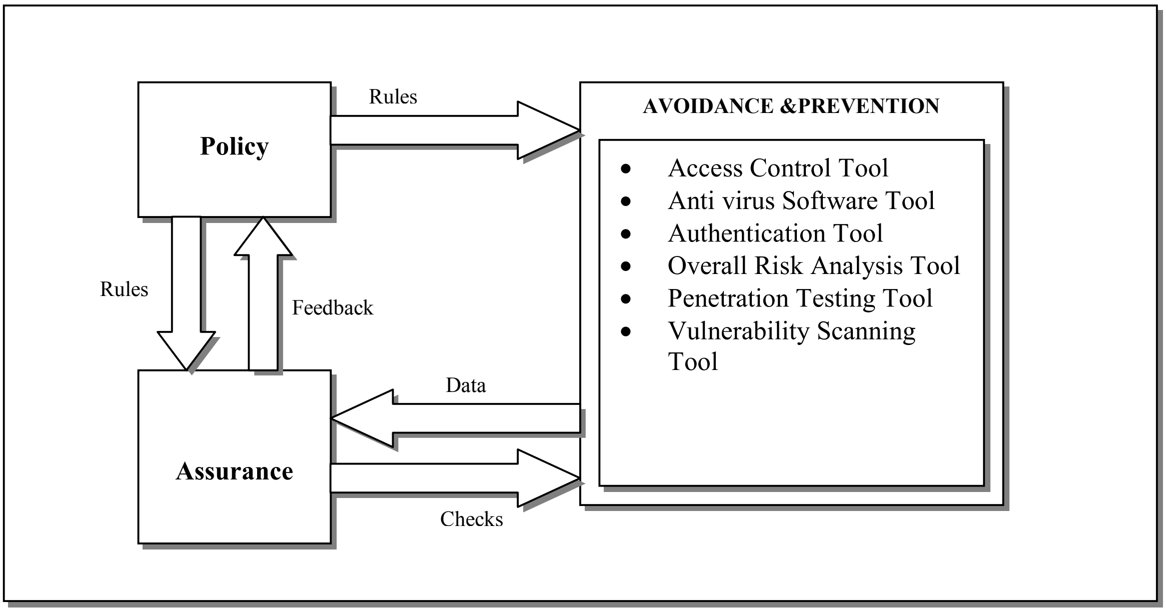
Policy
Rules
AVOIDANCE &PREVENTION
• Access Control Tool
• Anti virus Software Tool
• Authentication Tool
• Overall Risk Analysis Tool
• Penetration Testing Tool
• Vulnerability Scanning Tool
Rules
Feedback
Data
Assurance
Checks

Figure 3.2 Intrusion Model in Avoidance & Prevention Layer.

### 3.3.2 Detection

Policies and procedures allow to detect when, where and how an intrusion has taken place. Additional hardware and software are required for intrusion detection. Intrusion Detection Systems (IDS) attempt to detect intrusion through analyzing observed system or network activities. There are commercial packages used for detection, some of them are shown in Figure 3.3.

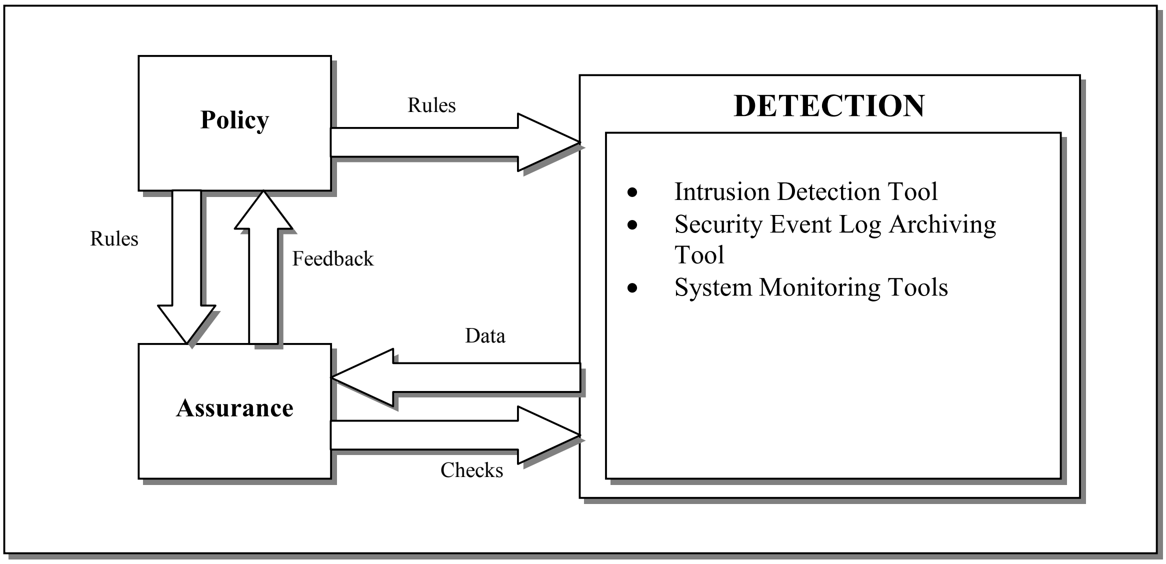
Policy
Rules
DETECTION
• Intrusion Detection Tool
• Security Event Log Archiving Tool
• System Monitoring Tools
Rules
Feedback
Data
Assurance
Checks

Figure 3.3 Intrusion Model in Detection Layer.

### 3.3.3 Investigation

Policies and procedures are used to define how to react an intrusion, in order to ensure that the intrusion does not happen again, and that the vulnerability used to gain access to the system is eliminated. Tools and techniques, which are shown in Figure 3.4 for identifying perpetrators, tracing them back, and supporting prosecution need to be developed.

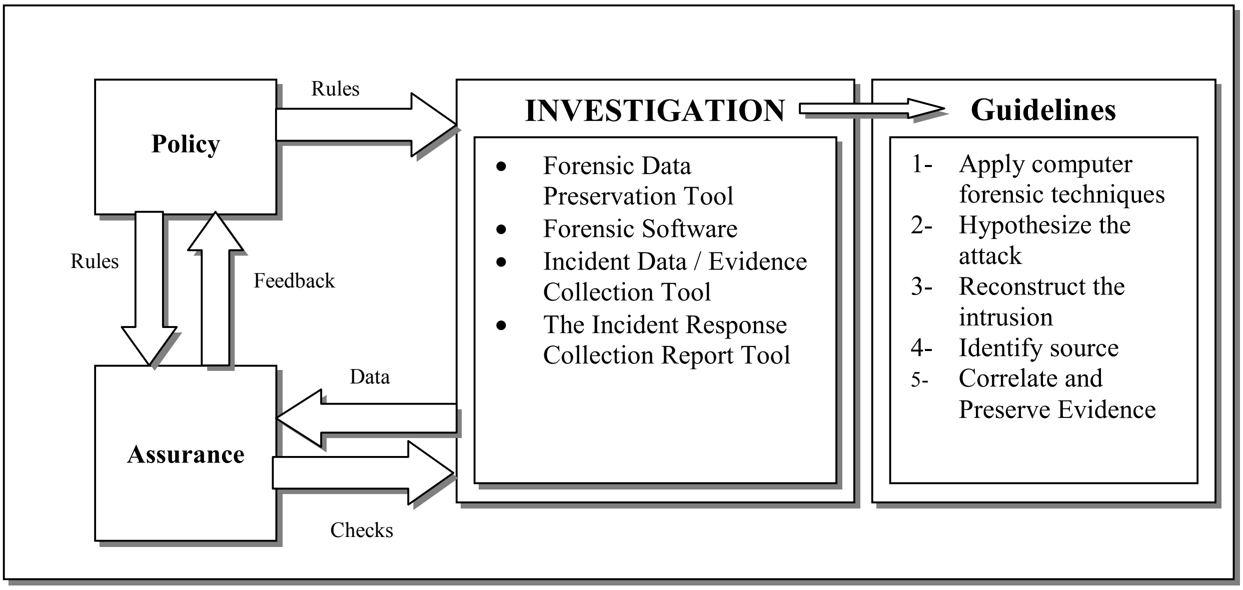
Policy
Rules
Rules
Feedback
Assurance
Data
Checks
INVESTIGATION
Guidelines
Forensic Data Preservation Tool
Forensic Software
Incident Data / Evidence Collection Tool
The Incident Response Collection Report Tool
1- Apply computer forensic techniques
2- Hypothesize the attack
3- Reconstruct the intrusion
4- Identify source
5- Correlate and Preserve Evidence

Figure 3.4 Intrusion Model in Investigation Layer.

### 3.3.4 Recovery

Policies and procedures define how to recover the system after an attack. Recovery and reconstitution techniques, both manual and automatic, are needed to determine what damage has been caused and to which systems, how to limit further damage, and how to bring systems back to a secure and usable state.

- Determine if intrusions are continuing and, if possible, determine the source of the intrusion,
- Identify and close access points,
- Identify what has been accessed, destroyed or altered,
- Assist in recovering data from network backups,
- Recommend revisions to security facilities, policy and procedures,
- Implement revised computer technology security policy and procedures.

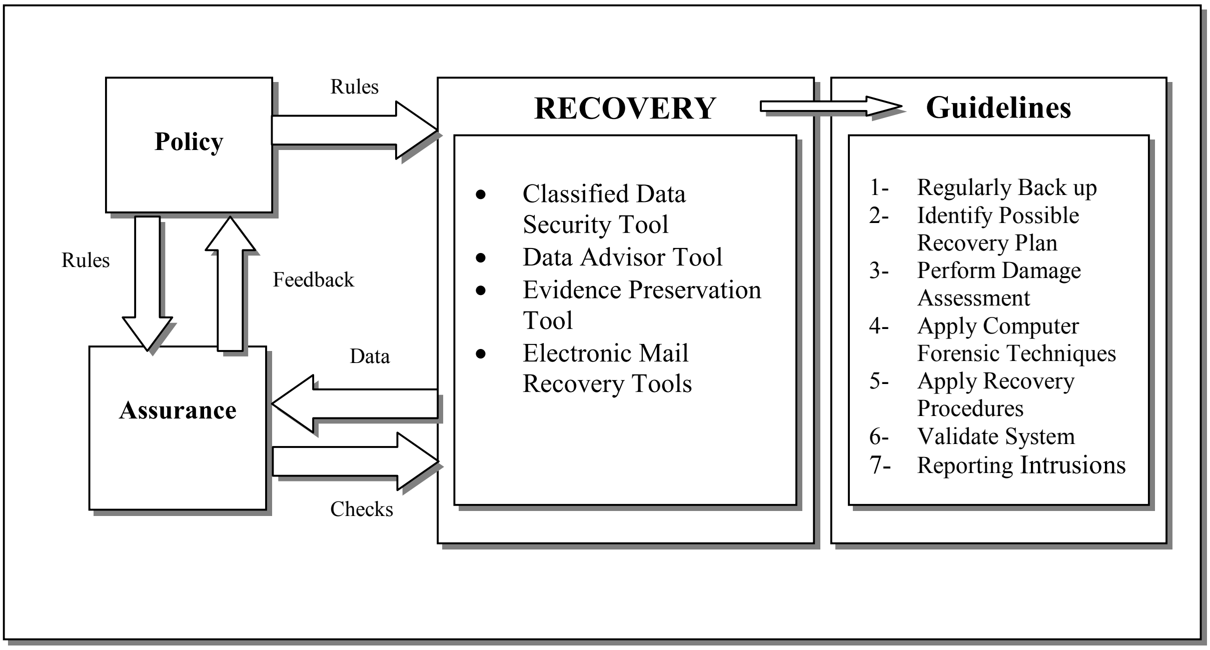
Policy
Rules
Rules
Feedback
Assurance
Data
Checks
RECOVERY
• Classified Data Security Tool
• Data Advisor Tool
• Evidence Preservation Tool
• Electronic Mail Recovery Tools
Guidelines
1- Regularly Back up
2- Identify Possible Recovery Plan
3- Perform Damage Assessment
4- Apply Computer Forensic Techniques
5- Apply Recovery Procedures
6- Validate System
7- Reporting Intrusions

Figure 3.5 Intrusion Model in Recovery Layer.

The remaining chapters of this thesis present a study that addresses to some of the concerns facing intrusion response. In Chapter 4, intrusion investigation is examined, investigation policy, guidelines and tools are summarized. In Chapter 5 similar study is made for intrusion recovery. In chapter 6 intrusion investigation and recovery guidelines are compared with each other.

# Chapter 4

# INTRUSION INVESTIGATION

Intrusion investigation and intrusion recovery are the integral part of intrusion management, intrusion response and reactive strategy. If avoidance and detection layers cannot reasonably prevent something, investigation layer wants to detect the problem as early as possible and minimize the damage.

Once the analysis is complete, Information System Security Officer (ISSO) must introduce some form of counter-measure to counter-act the effects of the attack and restore the system to a safe state [Nikhil, 2000].

The overall goal of intrusion investigation is to answer the related questions of "what happened", "how did it happen", "what is suspected", "what actions were taken", "who was contacted as a result" and "what evidence of the intruders activities was located".

## 4.1 Goal

The goal of this section is to provide knowledge about the procedures to conduct a computer intrusion investigation. It will also describe generic computer forensic procedures, tools and techniques related to investigative process to ensure that ISSOs and System Administrators are aware of the evidentiary requirements for preserving and analysing computer evidence to support investigation and prosecution.

According to *Rosenblatt* [Stephenson, 1999], the investigation of a computer intrusion has six goals,

1- To understand how the intruder is entering the system

2- To obtain the information you need to justify a trap and trace of the phone line the intruder is using

3- To discover why the intruder has chosen the victim's computer

4- To gather as much evidence of the intrusion as possible

5- To obtain information that may narrow your list of suspect or at list suspects, or at least confirm that the intruder is not a current employee

6- To document the damage to the victim caused by the victim in investigating the incident and determining the amount of damage to its computer.

## 4.2 Scope

Investigation is used to determine the origin of the attack, and corrective action should be taken as appropriate. The scope of the intrusion investigation process is to determine cause and effects of an attack, and to identify, examine and preserve potential electronic evidence. Electronic evidence refers to the entire range of information stored in or generated by computers [Strydom, 2001].

Methods of gathering electronic evidence includes:

- imaging,
- specialised soft/hardware,
- utilising existing data,
- monitoring [Strydom, 2001].

"Computer forensics involves the preservation, identification, extraction, and documentation of computer evidence stored in the form of magnetically encoded information (data)" [Lunn, 2001], and the study of computer technology as it relates to the law. The objective of the forensic process is to learn as much about the suspect system as possible. This generally means analyzing the system by using a variety of forensic tools and processes.

Computer forensic tools and techniques have become important resources that are used in intrusion investigations. These techniques are described as;

### 1. On-line inspection

1.1 Clone the disk and copy: Copy the data to a remote host for later investigation.

1.2 Process Investigation

- view the running process environment,
- view process opening file,
- to trace a process system calls and signals.

1.3 Collect Network Information

- the host network connection,
- to list the open port,
- to trace a host,
- to trace the MAC.

**2. Off-line inspection**

- check the MAC time (modify, access and status changed time stamp),
- check the log files (syslog, messages, secure , mail, wtmp, utpmp, lastlog.

**3. Recovery and exam of removed files** (not from back up tape)

- view the removed file name in the directory,
- calculate its inode position .

By using these technique computer forensic tools;

- Protect the computer system during the forensic examination against alteration, damage, data corruption and virus introduction,
- Find and record currently active files, deleted yet remaining files, encrypted files, hidden files and password-protected files,
- Recover deleted files reveal the contents of hidden files, temporary and swap files used by both the application programs and the operating system also access the contents of password protected, encrypted files and analyze all potentially relevant data found in special areas of a disk. This includes ‘unallocated’ space on a disk, 'slack' space in a file,
- Report an overall analysis of system, relevant files, discovered file data.

### 4.3 Roles & Responsibilities

This section outlines the roles and responsibilities of the individuals involved in the intrusion investigation activities in the organization. Intrusion Investigation Team must have a fundamental understanding of information systems. The team members must possess skills and knowledge relevant to computer security. The members of the team must understand how computers, operating systems, databases, and computer networks function, and must have a basic understanding of the various concepts at work in these areas (e.g., computer organization, distributed computing, database architecture and administration, network architecture and protocols, etc.). And they must also have the imagination and deductive skills to solve cases. In the table at the below each member is described with their roles and responsibilities.

Table 4.1 Roles and Responsibilities.

| Role | Scope | Responsibilities |
|---|---|---|
| **System Administrator (Director)** | To give answers directly to top management | • Carry out incident response activities<br>• Answer directly to top management |
| **Lead Investigator** | To give reports to the System Administrator | • Prepare an intrusion report s<br>• Give briefing any findings and/or determinations<br>• Interface with law enforcement |
| **Forensic Technicians** | To carry out intrusion response tasks at the direction of the Lead Investigator | • Analyze that evidence<br>• Report on their findings |
| **Evidence Handler** | To protect all evidence gathered during the intrusion | • Receive any evidence that is collected by Forensic Technicians<br>• Check evidence into and out of protective custody |
| **Legal Adviser** | To provide guidance consistent with all applicable state and federal laws | • To provide guidance consistent with all applicable state and federal laws |
| **ISSO** | To develop an Intrusion handling capability within their organizations | • Delegate responsibilities and authority for implementing this guideline, to include designation of System Managers.<br>• Review occurrence reports<br>• Ensure training programs which are established for system user<br>• Overall leadership and decision-making during an intrusion |
| **System Users** | To work with work definitions | • To run applications |
| **Computer Incident Response Team** | To resolve all intrusions | • Identify computer security incidents<br>• Receive intrusion reports from system administrator, lead investigator and legal adviser<br>• Log all reports<br>• Prepare a report of findings and perform a post intrusion review |

## 4.4 Intrusion Investigation Process

The leading hindrance to a successful investigation is lack of complete, timely, reliable information about the attack and attacker. The organization's Computer Incident Response Team (CIRT) should undertake investigations of security intrusions, whether they are successful or simply strong attempts. The CIRT should be trained and prepared to initiate a formal investigation, present result to management, support litigation or criminal prosecution if necessary, and ensure that fed back into the Intrusion Management process [Stephenson, 1999].

An effective investigation process;

- identify causes,
- identify problem,
- recommend corrective action,
- provide information that can be used as a preventive tool,
- provide management with data about intrusions,
- provide information that can be used to investigate the need for actions,
- all investigation must be documented and preventative controls put in place.

This process begins with the intrusion investigation team members determining the bounds of investigation in accordance with the organization's policy. All of the necessary tools and functions are integrated into investigation process and allowing the examiner to multitask, manage the evidence more effectively and build a case. Investigation process steps are described as follows;

*Step: 1 Review investigation policy and procedures*

The first step is to assess the situation. What is the severity level of the intrusion? Who will be involved in the investigation? Who is responsible for determining future actions? The more such questions have been addressed in advance by the adoption of a written security policy, the more quickly and accurately the effects of the damage [Matuszak, 2001].

A- Locate the policy that addresses Intrusion Investigation Guideline.

- It should define roles and responsibilities; System Administrator, Lead Investigator, Forensic Technicians, Evidence Handler, Legal Adviser

- It should name a plan of action: Intrusion Investigation procedures

B- Locate the Intrusion Investigation Procedures

- It should state what to do, when, and by whom.

C- Evaluate the situation

- Is the intrusion urgent, what is the damage, is continued operation possible?

*Step: 2 Collect information*

Initial assessment consists of inventory of all potentially affected systems. An important first step is determining if a perpetrator still has control of the any relevant computer. If they are still logged on, an important decision is to decide whether to terminate the user; leaving the intruder on the system may provide a better opportunity of profiling and ultimately identifying and apprehending the attacker. If, on the other hand, the investigator decides to lock the user out and disconnect the system from the network, they can often limit the damage to what the malicious user has already accomplished [Matuszak, 2001]. Record everything;

- Observations, Hypothesis, Ideas, Assumptions, Date and Time, Actions taken.

*Step: 3 Take appropriate action*

If it is clear that an intrusion has occurred, create an image backup of the affected hard drives. An image backup will contain information that is not accessible from file systems, such as deleted files. If an image backup is not feasible, check for suspicious activity in audit trails and logs, network traces, any change dates on files and directories, changes to startup files or the registry, new users or groups or members added to groups.

After the initial assessment is complete, protect the system by physically disconnecting from the network and shutting down the operation system to minimize the effects of the attack and to allow for the examination of the system. Notify all employees to change their passwords immediately. The following kinds of information can greatly accelerate the investigation process:

- connection logs
- user authentication logs
- general system logs
- application audit logs

- database audit logs
- file access/modification time-stamps [San Diego Supercomputer Center, 1997].

The steps of investigation process actions are detailed in the intrusion investigation guidelines.

### 4.4.1 Intrusion Investigation Policy

One of the first steps by any concerned intrusion investigation process should be to formulate a security policy that has approval from the highest levels of management. Policies are later translated standards and guidelines and also into actions, directives and consistent security behaviours. Intrusion investigation policy is explained below.

***Intrusion Investigation Policy***

*Goal :* Collect, preserve and submit evidence of the intrusion.

*Scope :* Intrusion.

*Roles & Responsibilities:* Security Manager is responsible for proper execution of the following guidelines.

*Description of Life-Cycle:* Develop hypotheses, Refine/Eliminate hypothesis, Determine the correct hypothesis using the evidence.

*Guidelines:*

1 Apply computer forensic techniques

2 Hypothesize the attack

3 Reconstruct the intrusion

4 Identify source

5 Correlate and Preserve Evidence

### 4.4.2 Intrusion Investigation Guidelines

The aim of intrusion investigation guideline is to provide System Administrators (sysadms) and ISSOs with a general knowledge of the procedures for conducting a computer intrusion investigation. In a plain and approachable manner, this guideline covers a generic method for the application of intrusion investigation. The main part of the guideline addresses goals, scope, roles & responsibilities and describes process issues fundamental to investigating computer investigation, and detail a procedure for doing search and information discovery of logical computer evidence. Investigation process guidelines are explained below.

***Intrusion Investigation Guidelines***

*No :* **Intrusion Investigation Guideline - 1**

*Title :* ***Apply computer forensic techniques*** (Stephenson 1999)

*Goal :* Determine if a security intrusion actually occurred.

*Scope :* Victim Environment.

*Roles & Responsibilities:* Security Officer is responsible for proper execution of the following procedures.

*Description of Life-Cycle:* Collect background information, Collect evidence, Assess damage.

*Procedures:*

1.1 Describe the computer system including peripherals
1.2 Discover all files on the subject system
1.3 Recover all (or as much as possible) of discovered deleted files
1.4 Access (if possible and if legally appropriate) contents of protected or encrypted files
1.5 Analyze all relevant data found in special (and typically inaccessible) areas of a disk
1.6 Print out a listing of all possibly relevant files and discovered file data
1.7 Print out an overall analysis of the subject computer system
1.8 Track and document damage caused by the intrusion

*No :* **Intrusion Investigation Guideline - 2**

*Title :* ***Hypothesize the attack*** (Stephenson 1999)

*Goal :* Figure out how the attack occurred.

*Scope :* Access routes, logs, known exploits.

*Roles & Responsibilities:* Security Officer is responsible for proper execution of the following procedures.

*Description of Life-Cycle:* Construct various hypotheses.

*Procedures:*

2.1 Map all access routes into the victim computer
2.2 Analyze the attack theoretically
2.3 Test the hypothetical routes to the victim and users with access
2.4 Analyze logs
2.5 Evaluate known exploits in this system
2.6 Construct hypothesis

*No :* **Intrusion Investigation Guideline - 3**

*Title :* ***Reconstruct the crime*** (Casey and Seglem 2002)

*Goal :* Reconstruct the crime by performing the actions of the attacker.

*Scope :* Hypotheses.

*Roles & Responsibilities:* Security Officer is responsible for proper execution of the following procedures.

*Description of Life-Cycle:* Follow the steps of the attacker, Compare results, Eliminate unmatching hypothesis.

*Procedures:*

3.1 Create a timeline of events

3.2 Check the hypothesis

3.3 Refine/Eliminate the hypothesis

3.4 Examine alternative scenarios

*No :* ***Intrusion Investigation Guideline - 4***

*Title :* ***Identify source*** (Casey and Seglem 2002)

*Goal :* Examine victim and intermediate computers to identify the attacker.

*Scope :* Files, logs, accounts, services, tools.

*Roles & Responsibilities:* Security Officer is responsible for proper execution of the following procedures.

*Description of Life-Cycle:* Find clues that indicates the source.

*Procedures:*

4.1 Examine critical files

4.2 Merge all logs and look for clues

4.3 Check for unauthorized accounts and unauthorized services

4.4 Examine communication connections

4.5 Look for changes to files, critical file deletions, unknown new files

4.6 Look for hacking tools

*No :* ***Intrusion Investigation Guideline - 5***

*Title :* ***Correlate and Preserve Evidence*** (Romig 2002)

*Goal :* Construct Evidence Relationships.

*Scope :* Evidence.

*Roles & Responsibilities:* Security Officer is responsible for proper execution of the following procedures.

*Description of Life-Cycle:* Order the evidence, Find out missing evidence.

*Procedures:*

5.1 Find out functional and temporal correlations

5.2 Eliminate inappropriate evidence

5.3 Determine missing evidence

5.4 Contact law enforcement immediately if decision is made to prosecute the attacker

Figure 4.1 shows common parts of intrusion investigation process steps and investigation guidelines.

| | **Step1** | **Step 2** | **Step 3** |
|---|---|---|---|
| | **Review Policy and Procedures** | **Collect Information** | **Take Appropriate Action** |
| **Investigaion Guideline 1**<br>Apply Computer Forensic Techniques | X | X | X |
| **Investigaion Guideline 2**<br>Hypothesis the Attack | X | X | |
| **Investigaion Guideline 3**<br>Reconstruct the Intrusion | X | X | |
| **Investigaion Guideline 4**<br>Identify Source | X | X | |
| **Investigaion Guideline 5**<br>Correct and Preserve Evidence | | | X |

Figure 4.1 Intrusion Investigation Process Steps and Guidelines.

### 4.4.3 Investigation Tools

**Encase:** Forensic software application that manages and enables viewing of all evidence.

*Primary Uses;*

- Allows the examiner to perform all functions of the computer forensic investigation process, from the initial “previewing” of a target drive, the acquisition of the evidentiary images, the search and recovery of the data and the final reporting of findings, all within the same application.

*Program Features and Benefits:*

- Provides user interface that enables examiners to easily manage large volumes of computer evidence,
- Views all relevant files, including “deleted” files, file slack and unallocated data.

**Net Threat Analyzer:** A tool that identifies past Internet activitiy.

*Primary Uses:*

- It can be used to quickly and covertly determine past Internet activities on a subject computer,
- It can be used to quickly and automatically identify Internet web browsing activities.

*Program Features and Benefits:*

- Automatically identifies and process the windows swap file,
- Can be operated from a single floppy diskette,
- Options allow for automatic E-mail pattern identifications,
- Options allow for automatic identification of file downloads made from the Internet.

**CRCCMD5:** Software used to compare copies of files to ensure they are identical, it compares the contents of the files and produces a hash. If the hash is the same, the copies are identical

*Primary Uses:*

- Used in computer investigations to prove that the evidence remains unchagedafter forensic processing,
- Used to identify files that have been changed or have been altered,
- Quickly identifies altered files after a computer intrusion

*Program Features and Benefits:*

- Compact program size which easily fits on a floppy diskette with other forensic software tools,
- Output can be routed to screen or a file using standard DOS comman.

Figure 4.2 provides stages for an Investigation Policy and shows a high level stages involved in the guidelines.

| Investigation Policy | |
|---|---|
| **<u>Investigation Guidelines</u>** | **<u>Investigation Tools</u>** |
| Apply Computer Forensic Techniques | Encase |
| Hypothesis the Attack | None |
| Reconstruct the Intrusion | None |
| Identify Source | Net Threat Analyzer |
| Correlate and Preserve Evidence | CRCMD5 |

Figure 4.2 Stages for an Information Discovery for Investigation.

# Chapter 5

# INTRUSION RECOVERY

Much like any other part of intrusion response, and reactive strategy, recovery from intrusion starts before computer systems have been attacked. After investigation layer detects the intrusion, recovery layer wants to recover as quickly and efficiently as possible.

Recovery is a system's ability to restore services after an intrusion has occurred. Recovery strategies in use today include replication of critical information and services, and incorporation of backup systems for hardware and software. These backup systems include master copies of critical software in isolation from the network [CERT, 2001].

The overall goal of intrusion recovery is to answer the related questions of "why did it happen", "was it handled promptly and properly" and "could it have been handled better".

## 5.1 Goal

The goal of recovery is to return a system to its normal operational status [Northcut, 1996], or ensure that the system and the data are exactly as they were before the intrusion occurred and to restore normal operations as soon as possible [Gallagher, 1991]. Ensuring requires that the integrity of every file in the compromised system be examined and restored. Recovery also contributes to a system's ability to maintain essential services during intrusion.

After an intrusion has been detected and terminated, system administrators face two difficult tasks: determining the damage caused by the intrusion and recovery of the system to a safe state.

The recovery process allows users to assess what damage has been incurred, and what information has been lost. Once the user can be assured that the attack has been contained, it is helpful to conduct an analysis of the attack.

## 5.2 Scope

Intrusion recovery refers to procedures necessary to ensure that intrusions don't compromise a system's secure operation [CERT, 2001]. The actual recovery timeline begins the moment a disruption occurs and continues until the business operation is restored.

At this point satisfactory recovery strategy must be able to accomplish restoration quickly, thereby minimize the effect on users during both backup and recovery operations which is extremely important in developing an Intrusion Recovery Plan (IRP) [Collie, 2001]. The intent of IRP is to provide a written and tested plan directing the computer system recovery process in the event of an interruption in continuous service resulting from unexpected damage [Janco Associates, Inc., 2001]. The IRP must be built to restore the applications and platforms that support these critical functions in the timeframe specified by the computer system's units. An intrusion recovery plan follows two important principle comprehensiveness and clear action:

- it covers all the details of what is to be done in the event of an intrusion
- it leads ISSO to respond in the correct way

An important component to any intrusion recovery plan is inventory associated

- software packages, with version number
- date of purchase
- name, address and telephone number
- the purpose of the software
- the acquisition date of the software
- the original cost of the software the license number
- the version number [Collie, 2001].

## 5.3 Roles & Responsibilities

This section outlines the roles and responsibilities of the individuals involved in the intrusion recovery activities in the organization. For this option, Intrusion Recovery Team must have a fundamental understanding of information systems. The comprehensive set of documented tasks are carried out during recovery operations.

**Table 5.1 Roles and Responsibilities.**

| Role | Scope | Responsibilities |
|---|---|---|
| **System Administrator (Director)** | To give answers directly to top management | • Carry out intrusion response activities<br>• Answer directly to top management<br>• Take all the responsibility of implementing the recovery plan |
| **Planning Group** | To manage the development and implementation of the intrusion recovery strategy and plan | • Responsible for all intrusion recovery activities, planning,<br>• Provide regular monthly reports to system administrator management |
| **System Users** | To work with work definitions | • Identify the list of critical H/w and software to reestablish the system<br>• Gather information about the status of the files when the intrusion occur |
| **Security/Back-up Team** | To retrieve back-up copies of operating systems, applications systems, applications data and ensuring security of the data | • Advise the System<br>• Administrator of the status of back-up data, software, of status and progress |
| **Damage Assessment Team Leader(s)** | To coordinate damage assessment and recovery activities for the system | • Develop, review and update procedures for damage reporting<br>• coordinate damage assessment operations<br>• Identify and maintain a list of critical data, service<br>• Collect and compile incoming damage reports |

## 5.4 Intrusion Recovery Process

The intrusion recovery process can recover the system that has been damaged by the intrusion or malicious attack. Method of cleaning up a compromised system is to reinstall the operating system and software allowing a faster return to normal operation. Another approach is to compare each individual file and program against a copy known to be original in order to determine if any modifications have been made. It is important to do a minimal level of analysis in order to determine the cause of the intrusion. Once a cause is determined, changes to the environment should be made to avoid future attacks by that method. This includes updating affected software access control methods that allow only certain users, systems and networks to use the services, firewalls and intrusion detection systems.

To follow those principles, it helps to have clear objectives for an intrusion recovery process:

- create and ensure reliable back-up systems in the event of an intrusion,
- make simple, clear decisions during an intrusion,
- train operational personnel,
- train employees,
- respond as quickly as possible to an intrusion,
- test and ensure the continuous reliability of the plan,
- coordinate of restoration,
- reloading of software,
- schedule migration back to original site,
- coordinate return to original site .

This process begins with the intrusion recovery team members determining the bounds of recovery in accordance with the organization’s policy [CERT, 2001]. All of the necessary tools and functions are integrated into recovery process, and allowing the examiner to multitask, manage the backup more effectively and build a case. Recovery process steps are described as follows;

*Step 1: Review investigation policy and procedures*

The first step is to assess the situation. “What is the severity level of the intrusion”, “who will be involved in the recovery”, “who is responsible for determining future actions”. The more such questions have been addressed in advance by the adoption of a written security policy, the more quickly and accurately the effects of the damage [Matuszak, 2001].

A- Locate the policy that addresses Intrusion Recovery Guideline.

- It should define roles and responsibilities; System Administrator (Director), Planning Group, ISSO, System Users, Security/Back-up Team, Damage Assessment Team Leader(s)
- It should name a plan of action: Intrusion Recovery procedures

B- Locate the Intrusion Recovery Procedures

- It should state what to do, when, and by whom.

C- Evaluate the situation

- Is the intrusion urgent, what is the damage, is continued operation possible?

*Step 2: Collect Information (Damage Assessment)*

Initial assessment consists of inventory of all potentially affected systems. In the intrusion recovery process the main thing is to assess the damage. The clear assessment of damage, losses in the aftermath of an intrusion is a prerequisite for the effective planning and implementation of recovery [San Diego Supercomputer Center, 1997]. Assessments need thorough planning, design and preparation of related data about intrusion. For successful assessment;

- Data has to be timely, assessments should be carried out as soon as possible after the intrusion,
- Data has to be continuously updated, in order to re-evaluate the needs and the appropriateness of recovery actions [Planitz, 1999].

In this process the objectives of damage assessments are to determine:

- nature and extent of a intrusion,
- damage and threats,
- resource availability,
- immediate response requirements,
- estimates on value loss through damage.

*Step 3: Take appropriate action*

After the damage assessment is complete, minimize the effects of the attack. The determination to return a system to normal operation is prior to fully resolving the problem. Recovery techniques, both manual and automated, are also needed to determine what damage has been caused and to what systems, how to limit further damage, and how to bring systems back to a secure and usable state. For this reason, administrators;

A - Rollback: That is (restoring a system to its state before the attack) using the backup files created before the intrusion occurred.

B- Reconfiguration: That is appropriate when one cannot roll back to a secure state, possibly because backups have not been done recently or the system has been in an insecure state since its inception.

- reinstall the operating system,
- perform an integrity check,
- restore the services.

The steps of recovery process actions are detailed in the intrusion recovery guidelines.

### 5.4.1 Intrusion Recovery Policy

One of the initial steps by any concerned intrusion recovery process should be restartable after intrusions and formulate a security policy that has approval from the highest levels of management. Policies are later translated into standards and guidelines and also into actions, directives and consistent security behaviours. Intrusion recovery policy is explained below.

***Intrusion Recovery Policy***

*Goal :* To establish a plan for restoration of information and operations following an intrusion, to reduce the risk of disruption of operations or loss of information.

*Scope :* Intrusion.

*Roles & Responsibilities:* Security Manager is responsible for proper execution of the following guidelines.

*Description of Life-Cycle:* Create system backup, make simple decisions, coordinate of restoration.

*Guidelines:*

1 Regularly Back up

2 Develop Possible Recovery Plan

3 Perform Damage Assessment

4 Apply Computer Forensic Techniques

5 Apply Recovery Procedures

6 Validate System

7 Reporting Intrusions

### 5.4.2 Intrusion Recovery Guidelines

The purpose of this guideline is to help to understand the requirements for the ISSO to be ready Intrusion Recovery Process. The guidelines for intrusion recovery presented refers to the procedures and resources required implementing a recovery operation. The main parts of the guideline address goals, scope, roles & responsibilities and describe process issues fundamental to recovery operation. These guidelines are explained below.

***Intrusion Recovery Guidelines***

*No :* ***Intrusion Recovery Guideline - 1***

*Title :* ***Back up Regularly***

*Goal :* Minimize the effects of the loss of a data.

*Scope :* Victim Environment.

*Roles & Responsibilities:* Security Officer is responsible for proper execution of the following procedures.

*Description of Life-Cycle:* Test, Verify and Approve.

*Procedures:*

1.1 Operating System, Applications, Database management system components

1.2 Database backup - User Data

1.3 Program backup - Program modules

1.4 Log file backup - Transaction Logs

1.5.Individual files backup - files in which Critical Tables are stored in

***Intrusion Recovery Guidelines***

*No :* ***Intrusion Recovery Guideline - 2***

*Title :* ***Develop Possible Recovery Plan***

*Goal :* Determine the important and less-important data, processes, and services.

*Scope :* Victim Environment.

*Roles & Responsibilities:* Security Officer is responsible for proper execution of the following procedures.

*Description of Life-Cycle:* Analyze system, Determine the priorities of the system.

*Procedures:*

2.1 Establish planning group

2.2 Perform risk assessment and audits

2.3 Establish priority organization’s network and applications

2.4 Develop recovery strategy

2.5 Prepare an up to date inventory and documentation of the plan

2.6 Develop verification criteria and procedures

2.7 Implement the plan

***Intrusion Recovery Guidelines***

*No :* ***Intrusion Recovery Guideline - 3***

*Title :* ***Perform Damage Assessment***

*Goal :* Analyze the system.

*Scope :* Victim Environment.

*Roles & Responsibilities:* Security Officer is responsible for proper execution of the following procedures.

*Description of Life-Cycle*: Analyze system, Determine impact of damage.

*Procedures:*

3.1 Identify extent of damage to the computer system

3.2 Determine condition of equipment

3.3 Identify software problems

3.4 Define data problems

3.5 Identify data communications problems

3.6 Define restoration requirements

3.7 Schedule and restoration

3.8 Monitor salvage and restoration operation

***Intrusion Recovery Guidelines***

*No :* ***Intrusion Recovery Guideline - 4***

*Title :* ***Apply computer forensic techniques*** (Stephenson 1999)

*Goal :* Determine if a security intrusion actually occurred.

*Scope :* Victim Environment.

*Roles & Responsibilities:* Security Officer is responsible for proper execution of the following procedures.

*Description of Life-Cycle:* Collect background information, Collect evidence, Assess damage.

*Procedures:*

4.1 Discover all files on the subject system (normal files, deleted yet remaining files, hidden files, password-protected files, and encrypted files)

4.2 Print out an overall analysis of the subject computer system

***Intrusion Recovery Guidelines***

*No :* ***Intrusion Recovery Guideline - 5***

*Title :* ***Apply Recovery Procedures***

*Goal :* Return the systems to normal.

*Scope :* Victim Environment.

*Roles & Responsibilities:* Security Officer is responsible for proper execution of the following procedures.

*Description of Life-Cycle:* Watch the logs, Find the hole , Repair them.

*Procedures:*

5.1 Disconnect the local area network that an intruder is using

5.2 Disconnect the compromised system from the local network

5.3 Ensure all backup/recovery types are addressed in the Backup and Recovery Plan

5.4 Test out all backup and recovery procedures to ensure they meet desired objectives

5.5 Determine the requirements and timeframe for returning the system to normal operations

***Intrusion Recovery Guidelines***

*No* ***: Intrusion Recovery Guideline - 6***

*Title* ***: Validate the system***

*Goal :* Where the system has been restored monitor the systems.

*Scope :* Victim Environment.

*Roles & Responsibilities:* Security Officer is responsible for proper execution of the following procedures.

*Description of Life-Cycle:* Watch the logs, Maintain the integrity.

*Procedures:*

6.1 Verify that the operation is successful

6.2 Check the system is back to its normal condition

6.3 Update your security policy

6.4 Continue to monitor for back doors may be escaped detection

***Intrusion Recovery Guidelines***

*No* ***: Intrusion Recovery Guideline - 7***

*Title* ***: Reporting Intrusions***

*Goal :* Document security violations.

*Scope :* Victim Environment.

*Roles & Responsibilities:* Security Officer is responsible for proper execution of the following procedures.

*Description of Life-Cycle:* Write a report.

*Procedures:*

7.1 Review and analyze intrusion-tracking database

7.2 Share information on security violations with other system managers.

Figure 5.1 shows common parts of intrusion recovery process steps and recovery guidelines.

| | **Step1** | **Step 2** | **Step 3** |
|---|---|---|---|
| | **Review Policy and Procedures** | **Damage Assessment (Collect Information)** | **Take Appropriate Action** |
| **Recovery Guideline 1**<br>Back up Regularly | X | | |
| **Recovery Guideline 2**<br>Develop Possible Recovery Plan | X | X | |
| **Recovery Guideline 3**<br>Perform Damage Assessment | X | X | X |
| **Recovery Guideline 4**<br>Apply Computer Forensic Techniques | X | X | X |
| **Recovery Guideline 5**<br>Apply Recovery Procedures | X | | |
| **Recovery Guideline 6**<br>Validate System | X | | |
| **Recovery Guideline 7**<br>Reporting Intrusion | X | | |

Figure 5.1 Intrusion Recovery Process Steps and Guidelines.

### 5.4.3 Recovery Tools

Many software tools have been developed to assist the ISSO during recovery process. Below are just a few of the tools on the market today and their main functions are shown;

**SafeBack** used to covertly to duplicate all storage areas on a computer hard disk drive

*Primary Uses:*

- The program is used to archive the image hard disk drives on Intel based computer systems.
- The program is also used to restore archived images on another computer hard disk drive of equal or larger storage capacity.

*Program Features and Benefits:*

- Provides a detailed audit trail of the backup process for evidence documentation purposes.
- Copies all areas of the hard disk drive
- Allows for the backup process to be made via the printer port.
- Fast and efficient. Depending on the hardware configurations involved, the data transfer rate exceeds 50 million bytes per minute during the backup process.
- Copies and restores multiple partitions containing one or more operating systems.
- Can be used to accurately copy and restore Windows NT and Windows 2000 drives in a raid configuration [New Technologies Inc.].
- **CRCCMD5** this tool is described on page 34.
- **Encase** this tool is described on page 35.

| **Recovery Policy** | |
|---|---|
| **Recovery Guidelines** | **Recovery Tools** |
| Back up Regularly | SafeBack |
| Develop Possible Recovery Plan | None |
| Perform Damage Assessment | CRCCMD5 |
| Apply Computer Recovery Procedures | EnCase |
| Validate System | None |
| Reporting Intrusions | None |

Figure 5.2: Stages for an Information Discovery for Recovery.

# Chapter 6

# COMPARISON

This chapter provides a comparison of the guidelines which are used in the investigation and recovery processes. The aim is to show similarities and differences in guidelines between these two processes. These guidelines are used by ISSO for managing their systems after intrusion occurred. ISSO needs to analysis and eliminate an intruder's access to system as soon as possible and recover the data and the system, recognize that the system is vulnerable to another occurrence of the same type of intrusion.

Guideline No-1 for Investigation Process and Guideline No-4 for Recovery Process has the similarity which is computer forensic analysis. Before attempting to collect evidence from a computer, it is important to have an understanding of how forensic science is applied to computers. Computer forensic is a digital detective work. Electronic data can include any record, file, source code, program, computer manufacturer specifications, and other information on a computer storage device. Forensic analysis comprised mainly digital evidence recovery, forensic data analysis and document management services.

The "Identify - Preserve - Analyze - Report" model serves to describe the overall forensic process. Once a forensic technician identifies the systems containing data of an evidentiary nature, then the team member must properly preserve their digital contents in a forensically sound manner. After preserving the evidence, an investigator conducts some series of examinations by analysing the data on the system to extract relevant information from it. After identifying relevant information, the results of these efforts are reported in predetermined format.

Data requirements and the level of detail of information vary at different times for investigation and recovery processes. Therefore, different types of guidelines are conducted for investigation and recovery processes. Data for investigation process has to be thoroughly analysed and interpreted in order to become meaningful and useful information for investigation team members.

It is observed that Intrusion Investigation Guidelines other than No-1 possess no similarities with the guidelines of intrusion recovery except No:4 Due to different objectives of these processes, the remaining guidelines are different.

# CHAPTER 7

# CONCLUSION and FURTHER WORK

Intrusion investigation and recovery from an intrusion are two goals of intrusion management systems. Both processes usually consist of checking logs for unusual activity, unusual connections, and alterations in the system files.

When an intrusion has been detected, the investigation team members need to first regain the control of the compromised system. The system must then be investigated thoroughly by reviewing audit files. System data should also be checked to make sure the intruder has not changed them. This is a primary source of information on how, when and where the intrusion occurred.

Once an intrusion has been investigated and reported, then follows the task of recovery from the intrusion. First, the system should be backed up to allow the intrusion to be analyzed later, and then the recovery team members should restore compromised system. It must be secured to prevent other intrusions.

System administrators should report all intrusions to an authority, which may be the manager of the company or CERT. Intrusion investigation and recovery team members need to know who specifically will perform which procedures, what reports will be generated, and who will review the findings in these reports. Investigation process and recovery process team members require,

- *a* search tool that can use both character sets in its searches. Preferably, a single pass through the media will search using both character sets simultaneously.
- an ability to generate a listing of all the date/time stamps an operating system may store in relation to each file in the file system. This means that; some operating systems store various dates and times in relation to the files in the file system. Those dates/times may include Date/Time Last Modified, Date/Time Last Accessed, or Date/Time Created. Not all operating systems record all those date/time combinations. But if an operating system records any date/time stamp data in relation to files in a file system, the tool must list all date/time data available.

- an ability to identify and generate a listing of all deleted files in the file system. This means that; various operating systems handle deleting files in various ways, so the specific capability of a tool will be dependant on the file system the tool is examining, but to some degree, all file systems have a way of at least identifying that a file once existed in a certain space.
- an ability to search the contents of the regular files in a file system without changing either the data in the file or any date/time data recorded by the operating system about the file.
- an ability to identify and process special files. This means that; special files are in a format where their contents are either not written to disk or not maintained internally in a readily readable, searchable format. These files include compressed or password protected files; graphics files, video files and audio files; .PDF format files; files housing email archives and/or active email content.
- the capability to make forensically sound images of a wide variety of media. This means that; once the preview process has identified that certain systems or media contain information relevant to the issues at hand, an investigator must have tools capable of making forensically sound images of those systems or media. The criteria for "forensically sound" media images is fairly straightforward: the image must include a true, validated copy of every bit of every byte contained on the media, without regard to media contents, from the absolute beginning of the media to the end of the physical device.
- the capability to recover pertinent deleted files or portions. This means that; logically include a capability to identify and search
    - all file slack,
    - all free (unallocated) space,
    - relevant file headers in free space,
    - deleted directories in free space.
- the capability to thoroughly document their activities and succinctly document the data recovered from a piece of media that are relevant to the under investigation. This means that; preferably be an automated part of the forensic analysis software. If the software is self-documenting and certain reports are automatically generated for the user, based on the results of exercising the capabilities of the software, this could help make reporting results much simpler.

- an ability to identify physical space, hardware, software, communications, personnel support, supplies, and the prioritization of the applications to specify the order of restoration. Based upon these requirements, appropriate backup procedures and guidelines must be used.
- an ability to use backup/recovery procedures. This means that; when an object has been modified and to copy the new object to an alternate location The new location may be a file system or a database.

In this thesis the requirements of investigation and recovery processes are represented as a policies, guidelines, procedures and tools in Chapter 4 and Chapter 5. In order to express the similarities and differences between guidelines comparison have been made.

Still a lot of work exist to be done in order to define the requirements for investigation and recovery processes. For these processes' data requirements, detail level of information are different. Future work could therefore concentrate on providing an estimation of data requirement level for each process. According to these new data types, new guidelines and procedures could be developed. It is suggested that investigation and recovery procedures should be performed through standard operating procedures (SOP). Another future work could include development of additional guidelines accomplishing complex SOP's. But, it is difficult to develop and difficult to apply. that cover every aspect of investigation and recoveries because intrusions vary in a wide spectrum due to their nature. And finally, a software which shows the guidelines and procedures applicable to intrusions can be developed and this software should be used by ISSO.

## References:

Braid, M. (2001). “Collecting and Preserving Evidence after a System Compromise”, SANS Institute.

CERT, (2001). “An Emerging Discipline Defining Requirements for Survivable Systems”, CERT Survivable Network Systems, Retrived May 15, 2001, from www.cert.org/research/97tr013.pdf.

Collie, B. S. (2001). “Intrusion Investigation and Post Intrusion Computer Forensic Analysis”, Technical Operations Australian Federal Police, Retrived November 20, 2001, from http://www.usyd.edu.au/su/is/comms/security/intrusion_investigation.html

Gallagher, J. .P. (1991). “A Guide to Understanding Trusted Recovery in Trusted Systems”, National Computer Security Center.

Janco Associates, Inc. (2001). “Disaster Recovery Plan”, Retrived March 14, from http://www.e-janco.com/SamplePages/DisasterRecoveryPlanSample.pdf

Joel, W. (2001), “Developing a Security Policy SunPS Java™Centers.

Kangasluoma, M. (2001).“Expressing Security”, Helsinki University of Technology. Department of Computer Science.

Kernek, A. (2001).“ Solutions for Mission-Critical Applications Requiring High-Availability or Disaster Recovery Capabilities”, Land-5 The Network Storage Company.

Lunn, D. (2001). ” Computer Forensics – An Overview”, SANS Institute.

Matuszak, A. (2001). “An Introduction to Computer Crime Prevention and Response”, Network Security Corp., Retrived January 5, 2002, from http://www.lawsight.com/risk/cybercrm/ccrime.htm

National Institute of Standards, (2001). “An Introduction to Computer Security: The NIST Handbook”, National Institute of Standards and Technology Technology Administration U.S. Department of Commerce. Special Publication 800-12.

New Technologies, (2001). “Computer Forensics & Security Software Tools”, Retrived April 2, 2002, from http://www.forensics-intl.com/thetools.html

Nikhil, J. A. (2000). “Resource/Attack Modeling and Optimal Intrusion Recovery”, Department of Computer Science, University of California at Davis.

Northcutt, S. (1996). “Computer Security Incident Handling Procedure”, Retrived October 8, 2001, from http://www.all.net/books/ir/nswc/incident.handle.html.

Oxford University Press, (1996). Retrived February 5, 2001, from http://www.albion.com/security/intro-4.html

Planitz, A. (1999). “A Guide To Successful Damage And Needs Assessment”, South Pacific Disaster Reduction Programme.

Rfc 1244, Retrived 2001 May 11,
from http://www.net.ohio-state.edu/rfc1244/

Rfc 2196, “Site Security Handbook”, Retrived 2001 April 11, from http://www.ietf.org/rfc/rfc2196.txt

San Diego Supercomputer Center, (1997). “Distributed Object Computation Testbed (DOCT)” ,*Technical Report,* San Diego Supercomputer Center, Retrived February 5, 2001, from http://www.sdsc.edu/DOCT/Publications/f1-1/f1-1.html.

Shah, B. (2001). “How to Choose Intrusion Detection Solution”, SANS Institute.

Stephenson, P. (1999). “Investigating Computer-Related Crime”, CRC Press.

Stephenson, P. (2000). “Intrusion Management: A Top Level Model for Securing Information Assets in an Enterprise Environment”, 9th EICAR Annual Conference Best Paper Proceedings, Brussel.

Strydom, L. (2001). “Computer Evidence”, Forensics Services, Price Waterhouse Coopers.

The Computer Security Handbook of CIT, (2002). Retrived April 14, from http://www.cit.nih.gov/security/handbook.html

Toigo J. (1996). “Excerpted from Disaster Recovery Planning For Computers and Communication”, Systems Recovery Planning Chapter 8.

Tuğlular, T. (2001). “Nüfuz Yönetim Politikaları”, Bilişim Zirvesi '01, Lütfi Kırdar Uluslararası Kongre ve Sergi Sarayı, İstanbul, Eylül 2001.