A Preliminary Structural Approach to Insider Computer Misuse Incidents

Panda Best Student Paper Award

Tugkan Tuglular
Ege University, Turkey

About the Author

Tugkan Tuglular has received BSc degree and MSc degree in Computer Engineering, Ege University, in 1993 and 1995, respectively. He has received scholarship and worked for COAST Lab., Purdue University, under Prof. Dr. Eugene H. Spafford for 16 months between 1996 and 1998. Currently full time Ph.D. student in Dept. of Computer Engineering, Ege University. His research interests presently include insider computer misuse, security policies, auditing, and access control.

Mailing Address:
Dept. of Computer Engineering, Ege University, Bornova, Izmir 35040 TURKEY;
Phone: +(90) 232 – 388 72 21; Fax: +(90) 232 - 339 94 05;
E-mail: tuglular@staff.ege.edu.tr

Descriptors

computer security, information security, computer abuse, security attack, computer misuse, computer security incidents, response to computer security incidents, computer misuse characteristics, insider computer misuse classification, counterintelligence.

Reference to this paper should be made as follows: Tuglular, T. (2000) 'A Preliminary Structural Approach to Insider Computer Misuse Incidents', EICAR 2000 Best Paper Proceedings, pp.105 -125.

A Preliminary Structural Approach to Insider Computer Misuse Incidents

Abstract

Insider computer misuse information should be constantly and systematically collected and evaluated to track down insider perpetrators. To achieve this goal, a scheme is designed and created for insider computer misuse incidents. The development of the scheme is based on insider computer misuse classification, which groups misuse characeristics in three main dimensions; incident, response, and consequences.

Introduction

Organizations have to handle accidents, omissions, wastes, and abuses as well as attacks aiming the security of their assets. In this study, realization of all the above threats are referred to as computer misuse. When a computer misuse is performed from inside, or by an insider, that act is called insider computer misuse (ICM).

According to *Hunteman et al.* (1997, p.7), for the assurance of communications and information infrastructure the most important research and development objective is characterization of security threats and *Power* (1995, p. 5) indicates that "the greatest threat comes from inside your own organization". However, there is no known comprehensive study that addresses the characteristics of insider computer misuse to date.

There exists mainly four classifications related to ICM. The one developed by *Anderson* (1980, p.11) classifies internal penetration to computer systems in three groups: masquerade use, legitimate use, and clandestine use. *Neumann and Parker* (1989, p.396) group computer misuse techniques as external misuse, hardware misuse, masquerading, setting up subsequent misuse, bypassing intended controls, active misuse of resources, passive misuse of resources, misuse resulting from inaction, and use as an aid to other misuses. *Icove et al.* (1995, pp.68-69) used a computer crime adversarial matrix which describes a number of different types of criminals and, for each, summarizes certain characteristics in four categories:

- organizational,
- operational,
- behavioral,
- resource.

Cohen (1997, pp.30-44) describes 94 different classes of attack methods.

The classification is settled into a scheme which guides security personnel in collection and storage of ICM related information. The classification assumes that each organization has currently operative policies and controls. The user is free to add, modify, or remove some dimensions for better integration with the organizational culture. With pop-up windows and a database implementation, the scheme would be best utilized. Data analysis tools can be linked to the program so that collection and evaluation of ICM data can be performed in a single environment.

Summers (1997, page 75) emphsize that "we learn from cases of misuse. A case may be significant because its method of operation is new or widely applicable or because it reveals some weakness in safegurads". Thus, the proposed environment can be used to extract more information and to build up new dimensions for the classification and scheme.

In daily life of organizations, almost each act relates to computer systems or will do so in near future. In other words, people will work in cyberspace. Although cyberspace has some clear advantages as a work environment, it has some vulnerabilities that can be exploited by perpetrators. For instance, in cyberspace;

- information can be unrecognizably stolen,

- traces of computer misuse can be easily changed or removed,
- physical presence of the perpetrator in the computer system premises may not be necessary for ICM.

Counterintelligence has to adopt to the evolution of work environment in this cyberspace and should be able to uncover perpetrators acting within organizations. In this paper, a structural method is suggested to gather information about such insiders. The scheme developed in this study can help security personnel to foresee some repeated misuses and possibly avoid them for future. Moreover, even in cases where no information about the perpetrator can be found or suspected, with the collected misuse information some precautions can be taken or traps can be set up, assuming that the perpetrator will repeat computer misuses. If so and the perpetrator is traped for one incident then the forms filled in the past can be used as evidence in courts.

This paper will present the development and use of ICM incident scheme. In *Insider Computer Misuse* Section, the definition of insider computer misuse is given and characteristics of insider computer misuse, which are used in the classification and in the scheme, are discussed. In *Response To Insider Computer Misuse* Section, the use of ICM incident scheme is explained. The following section is devoted to counterintelligence, where the ICM incident scheme will find extensive use. The tables that constitute the scheme are presented in Appendix.

Insider Computer Misuse

Insider computer misuse may be defined as an act, directed at or committed with a computer system, violating the insider computer use policies defined by the organization that owns the computer system. The definition of insider computer misuse has some similarities with the definitions of criminal acts, such as theft and murder. Criminal acts violate the laws of state and the accused of such acts are punishable if evidence can be presented in court.

Similar to laws, policies are references used to interpret acts and to make decisions regarding them. The organization that owns the computer system has the responsibility to protect the users and their rights. Thus, the organization has to enforce the policies and react with disciplinary actions for the insiders using the rights given by law.

Information security policy is defined as "the set of laws, rules, practices, norms, and fashions that regulate how an organization manages, protects, and distributes sensitive information and that regulates how an organization protects system services" (Longley and Shain, 1990). *Wood et al.* (1995, p.668) indicate that policies can be thought as generalized requirements regarding organizational expectations. Generally, policies include goals, objectives, definitions, strategies, responsibilities and measures of success in reaching goals.

Computer use policy aims to protect the people, who use and depend on the computer system, from computer uses that may cause disruption and loss. Guarding the confidentiality, integrity, availability, reliability, efficiency, and safety of the organization assets against the threats may be an objective of computer use policy.

The policy should define, describe and illustrate concepts such as misuse, computer system, insider, asset, threat and control. The term misuse is used to cover all the accidents, omissions, and commissions that may prevent the organization reaching its policy goals. A computer system is made up of the computer itself, its resources (i.e. I/O, operating system and power system), its connecting networks, and the owners/users of them all. An insider can be defined simply as an employee or the definition can be extended to include owners, shareholders, business partners, and consultants.

The policy should name a strategy for each <type-of-threat, asset> pair, which may be preventing, limiting, or correcting. Additionally, computer use policy should define responsibilities and accountability conditions for employees. A simple measure of success would be the correlation between the loss due to computer misuse and the investment for the enforcement of the policy to protect it.

The protection triangle starts with the policies and continues with the standards and guidelines, which are simply rules to be followed. Standards are mandatory, whereas guidelines are presented to be helpful regardless of strict compliance. Controls, which may be thought as tactics, appear at the bottom of the triangle and may be classified as administrative, logical, and physical. A strategy against a specific threat defined by the policy can be implemented by one type of control or a combination of control types.

The objects that appear in a ICM incident are insider(s), organization asset(s), and policy enforcer(s). Organization assets can be grouped in six classes:

- information,
- computer,
- operation,
- control,
- personnel,
- equipment.

The policy enforcers entitled to protect these assets are security personnel and existing controls.

Computer misuse occurs when a ready mind meets an opportunity. An insider may have a tendency to misuse the computer system due to lack of competence, psychological state, or external pressure. In any case, either the insider bumps into an opportunity causing an accident, or the insider perceives / creates an opportunity performing either omission or commission. Omission occurs when an insider fails to perform the policy requirements. Commission takes place when an insider violates of the computer use policy. Both omission and commission can be realized knowingly or unknowingly and intentionally or unintentionally.

In all computer misuse incidents, a subject acts on a target or targets using a number of methods. The subject can be either a user at terminal or a process acting on behalf of a user. The ultimate target of the subject would be people, who own, rely on, or use the computer system. The ultimate target also reflects the mission of the perpetrator. If the ultimate target were the target itself, such as the operating system, the act would be vandalism, whereas if it were what the target represents, such as information about funds, the act would be fraud. Moreover, it is important to know the types of threats realized on

target(s). The method used in a misuse may indicate that assets of the organization are compromised or exploited. In addition to these facts, information about the time and place of computer misuse incident may be necessary to distinguish any incident from others.

The policy enforcers recognize a computer misuse incident either;

- before the incident, when prevention can be accomplished,
- during the incident, when limiting the damage is possible,
- after the incident, when recovering, or correcting, is the only thing left to do.

After recognition of a computer misuse incident, possible traces should be checked to verify the event and admissible evidence should be collected. For any evidence to be admissible it must be produced, maintained, or used in the course of business and it must be authenticated and reliable. Moreover, there should be no suspicion about the integrity of the evidence (Barrett, 1997, p.163). With traces, suspects are expected to be identified and the perpetrator ought to be tracked down among those suspects.

The consequences of computer misuse incidents may vary depending on the performance of the policy enforcers. Consequences may be classified in two groups. The first group consists of disruptions, losses, and effects that are caused by misuse. The second group includes the type, comprising acts and the data evaluation results of the computer misuse incident.

Response to Insider Computer Misuse

Nobody would follow laws if there was not sufficient enforcement. Similarly, without enforcement, insiders would not comply with the policies. Policy enforcement within an organization is accomplished if;

- computer misuse incidents are recognized,
- perpetrators are found,
- admissible evidence are collected,
- disciplinary measures are taken.

To achieve each of the above objectives, constant and systematic information collection and evaluation is necessary. It is important to note that the success of any policy depends on the success of its enforcers.

There is a second reason behind continuous collection of information about computer misuse. In order to maintain computer use policy, information about computer misuse incidents should be gathered and evaluated in a systematic way. Policies should be modified from time to time in light of the new information if it is noted that there is insufficient addressing of threats, wrong strategies, or incomplete/inaccurate controls. To be able to collect information systematically, an information structure, a scheme, should be used. Such a scheme is to be developed using a classification of insider computer misuse.

This scheme is composed of three parts; incident, response, and consequences, where these parts can be named as dimensions or classes. The incident dimension is further divided into target, subject, method, place, and time sub-dimensions. Recognition, trace, indication, and suspect are sub-dimensions of the response dimension. The

consequences dimension has disruption, loss, effect, violation, misuse type, misuse act, and result sub-dimensions. These sub-dimensions branch into new sub-dimensions and so on. The characteristics in this classification have mutually exclusive values. Usually values are selected from either [yes / no] pairs or scales, such as [high / medium / low].

A method is developed for completing the ICM incident scheme. The main table contains three main dimensions; incident, response, and consequences. And the sub-dimensions of each dimension are presented in further tables. For instance, if incident dimension were selected, then Table 1 for the incident sub-dimensions would come into view.

Incident	
target	
subject	
method	
place	
time	

Table 1: Incident Sub-dimensions.

If there is some information available about target, then the user marks the box next to it and the sub-dimensions of target dimension would appear as shown in Table 2.

Target	
ultimate target	
target value	
threat realized	

Table 2: Target Sub-dimensions.

Similarly, if some information is obtained about the threat realized, the box next to it should be marked and then Table 3 would pop-up. In Table 3, if the box across computer and availability is marked, the sub-dimensions of computer are displayed as in the following table illustrated as Table 4. If software is checked, that would mean that the threat against the availability of software is realized. If there were sub-dimensions of software, then they would come into view as another table and so on.

Threat Realized							
	confidentiality possession	integrity authenticity	availability useability	reliability	efficiency	safety	exposure to threats
information							
computer							
operation							
control							
personnel	N/A	N/A					
equipment							

Table 3: Sub-dimensions of Threat Realized.

Once there are no further existing sub-dimensions, the main table is displayed. The tactic for the use of this scheme is to click till you reach what you want to mark. Anywhere in the scheme it is always possible to turn to the main table. If some sub-dimension is marked mistakenly, clicking once more will remove the mark. All the tables are presented in the Appendix and all the dimensions are self-explanatory. Since there are a lot of dimensions the tables are concatenated wherever possible. A user with computer security knowledge may easily understand and use the tables.

Computer	
hardware	
software	
network	

Table 4: Computer Sub-dimensions.

While proceeding with the scheme, the user may face a granularity problem. Each user would probably develop his own solution to this problem. In this study it is assumed that every user has a specific granularity level with which he/she feels comfortable. Here is an example: suppose a police officer is to fill out some forms about a theft case where things are stolen from three different offices in a building. The officer may fill just one form for the whole building, or three forms, one for each office, or six forms, two for each office -where one form will hold information about enterance to the office and the second one about stolen things. In such a case, it is advised to choose a medium granularity level and fill out three forms.

Importance of Insider Computer Misuse Scheme for Counterintelligence

Counterintelligence may be defined as information gathered and activities conducted by or on behalf of foreign governments or organizations. The operations to uncover counterintelligence activities are performed to identify inside agents.

Inside agents have some capabilities creating advantages for counterintelligence activities. They have permissions to the organization premises and the computer system. They have considerably more time to operate compared to an external penetrator. They have the opportunity to observe personnel and computer system behavior and therefore are more likely to compromise such assets easily. In addition to all, they can influence management to change policies and controls. All these advantages will be enhanced if the agent is either a member of computer system or security personnel. In that case, he would be able to clear all traces and even worse create some false traces to divert attention from himself.

An intelligent insider acting covertly may not be identified by standard security measures. Systematical data collection and constant evaluation over a long period of time may be necessary to uncover an inside agent. Using the scheme presented in this paper may be helpful in systematical collection of ICM data. For evaluation, statistical, pattern matching, and anomaly detection tools should be utilized in addition to brainstorming and scenario analyses. Since all computer based counterintelligence activities are computer misuses any recognized ICM incident would reveal information about the agent.

The security personnel using a scheme like the one presented in this paper to gather information about computer misuse must be rotated and strict compartmentalization must be applied. No personnel other than the evaluation team should be allowed to see the gathered misuse information and evaluation results.

Conclusion

It is important to address the characteristics of insider computer misuse, because development of “insider computer misuse detection systems” should be based on them. The work presented in this paper constitutes the first step of developing such systems.

Before proceeding to the next step the characteristics should be checked, modified, or refined if necessary. This is possible by analyzing a large set of insider computer misuse cases. The cases that do not fit into the scheme will indicate some missing or inaccurate characteristics.

Although the tables are ready to use, they may not constitute a complete scheme because tables about specific dimensions, or classes, that change from one organization to another could be missing. For instance, if an organization owns computer controlled equipment, then the operations of such equipment should be included in the scheme. It is the user's responsibility to add those tables to the existing scheme. Moreover, the dimensions presented in this paper are not thought to be exhaustive. New (sub-)dimensions can be found and included to improve the completeness of the scheme.

Counterintelligence activities in cyberspace will grow in time as well as intelligence activities. One indication of this is the introduction of a new concept called information warfare. The conventional methods should be adopted to the new environment. This work is a step forward in that direction.

Acknowledgement

The author would like to thank Prof. Dr. Eugene H. Spafford who made helpful suggestions to improve the insider computer misuse classification.

References

Anderson J.P. (1980). Computer Security Threat Monitoring and Surveillance. Fort Washington, Pa: James P. Anderson Co.

Barrett N. (1997). Digital Crime: Policing the Cybernation. London: Kogan Page.

Cohen F. (1997). Information System Attacks: A Preliminary Classification Scheme. Computers & Security, 16: 29-46.

Hunteman W.J., Jacobsen S.E., Johnston W.E., Mansur D.L., Bailey K.C. (1997). Research & Development Priorities for Communications and Information Infrastructure Assurance. Los Alamos National Laboratory.

Icove D., Seger K., VonStorch W. (1995). Computer Crime: A Crimefighter's Handbook. Sebastopol, CA: O'Reilly & Associates, Inc.

Longley D., & Shain M. (1990). The Data and Computer Security Dictionary of Standards, Concepts, and Terms.

Neumann P.G., & Parker D.B. (1989). A Summary of Computer Misuse Techniques. Proceedings of the 12th National Computer Security Conference. Oct. 10-13. Baltimore, MD.

Power R. (1995). Current and Future Danger: A CSI Primer on Computer Crime & Information Warfare. San Francisco, CA: Computer Security Institute.

Summers R.C. (1997). Secure Computing: Threats and Safeguards. USA: Mc-Graw Hill.

Wood C.C., CISA, CISSP. (1995). Writing InfoSec Policies. Computers & Security, 14: 667-674.

Appendix

INSIDER COMPUTER MISUSE	
incident	
response	
consequences	

Incident	
target	
subject	
method	
place	
time	

Target	
ultimate target	
threat realized	
value	

Ultimate Target		
What		
	itself	
	represents	
Who		
	who own	
	who rely on	
	who use	

Threat Realized							
	confidentiality possession	integrity authenticity	availability usability	reliability	efficiency	safety	exposure to threats
information							
computer							
operation							
control							
personnel	N/A	N/A					
equipment							

Value		
	quantitative	qualitative
information		
computer		
operation		
control		
personnel	N/A	
equipment		

Information					
	processed	stored	inputted	outputted	transmitted
computer					
operation					
control					
personnel					
equipment					
business					

Business	
private	
proprietary	
trade secret	

Computer			
hardware			
	main hardware		
		server	
		workstation	
		miniframe	
		mainframe	
	external hardware		
		monitor	
		printer	
software			
	operating system		
	compiler / interpreter / shell		
	application		
		office	
	information management system		
		database	
		docubase	
	network software		
		webbrowser	
		telnet	
		ftp	
		finger	
		gopher	
network			
	network architecture		
		client/server	
		dedicated server	
	network connection		
		modem	
		hub	
		router	
	firewall		

Operation		
Information		
	add	
	archive	
	delete	
	disseminate	
	evaluate	
	receive	
	retrieve	
	search	
	update	
	verify	

Control			
	administrative control	logical control	physical control
security control			
I/O control			
operational control			
environmental control			

Security Control		
authorization		
identification & authentication		
access control		
	discretionary	
	mandatory	
event monitor		
	anomaly	
	error	
	intrusion	
audit		

I/O Control	
input validation	
output validation	

Operational Control	
installation	
process	
administration	
maintenance	

Subject	
subject type	
decision	
reason	
mission	
effort	

Subject Type	
process acting in behalf	
user at workstation	

Decision		
rational choice		
knowingly		
intentionally		
idea		
	told	
	read	
	self thought	

Reason		
incompetence		
	lack of incentive	
	lack of motivation	
	lack of knowledge	
	lack of skill	
	lack of training	
	lack of understanding	
	carelessness	
internal condition		
	economic	
	ideological	
	psychological	
external pressure		
	financial pressure	
	peer pressure	
	family pressure	
	group pressure	
	blackmailed	
warning		

Psychological	
disaffected	
job unsatisfaction	
available opportunity	
challenge	
criminality	
fun	
grudge	
recognition	
revenge	
self-expression	
being disgruntled	

Mission	
action	
consequences	

Effort	
research	
trial & error	
surveillance	
devise hardware	
devise software	

Method	
compromise / exploit	
access	
computer's role	
complexity	

Compromise / Exploit				
	observe	modify	destroy	create
information				
computer				
operation				
control				

Access			
	physical access	logical access	
	local	local	remote
with authorization			
with exceeding authorization			
without authorization			

Computer's Role	
mean	
goal	

Complexity	
ordinary	
complex	

Place	
virtual place	
organization	

Virtual Place	
workstation	
domain	

Organization			
	government	private sector	public
academic			
commercial			
educational			
industry			
law enforcement			
military			
professional society			
research			

Time	
Date	_ _ / _ _ / _ _ _ _
Wall Clock	_ _ : _ _

Response	
recognition	
trace	
evidence	
suspect	

Recognition	
before incident	
during incident	
after incident	

Trace		
security control information		
	authorization list	
	identification & authentication log	
	access information	
	event information	
	audit records	
I/O control information		
operational control information		
environmental control information		
damage on asset		
	information	
	computer	
	operation	
	control	
	personnel	
	equipment	

Evidence	
	admissable
physical evidence	
logical evidence	
testimonial	

Suspect		
attribute		
	sex	
	age	
profile		
	economic profile	
	social profile	
	psychological profile	
	ideological profile	
	legal profile	
	professional profile	
	computer use profile	
qualification		
	intelligence	[high / medium / low]
	professional knowledge	[high / medium / low]
	professional skill	[high / medium / low]
	education	[highschool / university / Ms / PhD]
role		
	employee	
	owner	
	shareholder	
	business partner	
	consultant	

Suspect (continued)		
access authorization		
	computer system	
	system administration	
	system security management	
	premises	
ownership		
	information	
	program	
responsibility		
	correctness of input	
	accuracy of work	
	efficiency of work	
	quality of use of product/service	
	reliability of product/service	
	security of product/service	
	timeliness of product/service	
	volume of product/service	
accountability		
	totally accountable	
	relieved if caused by others	
	relieved if not due to negligence	
	relieved of all	

Economic Profile	
income sufficient for living	
inherited valuables	

Social Profile	
married	
children	
memberships	
hobbies	

Psychological Profile	
addiction	
egocentricism	
epileptic	
high living	
instability	
malice	
passionate	
social adjustment	

Ideological Profile	
politically involved	
religiously involved	

Legal Profile	
previous offense	
offense(s)	

Offense	
type of offense	
seriousness of offense	
target of offense	
punishment	

Professional Profile	
committed	
foresighted	
honest	
loyal	
risk taking	
security conscious	
self control	
strength of character	

Computer Use Profile		
login		
	frequency	
	last login time	
	last login location	
	password fail pattern	
	location fail pattern	
session		
	elapsed time pattern	
	resource usage pattern	
	command & program execution pattern	
	excaption pattern	
	file access pattern	

Employee		
manager		
	chief executive	
	information system chief	
	information system security chief	
computer personnel		
	system administrator	
	system analyst/designer	
	system tester	
	backup personnel	
	maintenance personnel	
	supervisor	
	programmer	
	operator	
	data custodian	
security personnel		
	building security personnel	
	computer security officer	
	internal auditor	
end user		

CONSEQUENCES	
disruption	
loss	
effect	
violation	
misuse act (type I)	
misuse act (type II)	
misuse type	
result	

Disruption							
	confidentiality possession	integrity authenticity	availability usability	reliability	efficiency	safety	exposure to threats
information							
computer							
operation							
control							
personnel	N/A	N/A					
equipment							

Loss			
tangible			
	lost income		
		cancelled contracts	
		downtime	
	extra expenses		
		damage on assets	
		labour for investigation	
		labour for restoration	
		fines	
intangible			
	affect staff morale		
	legal prosecution		
	lose clients & prospects		
	negative publicity		
	personal suffering		
	reduced efficiency		
	reduced productivity		
	weakened position in market		

Effect		
	short term	long term
single point		
multi point		
massive		

Violation					
laws					
policies			preventing	limiting	correcting
	asset policies				
		information policy			
		computer policy			
		operation policy			
		personnel policy			
		equipment policy			
	threat policies				
		confidentiality policy			
		integrity policy			
		availability policy			
		reliability policy			
		efficiency policy			
		safety policy			
	control policies				
		security policy			
		I/O policy			
		operation policy			
		environment policy			

Misuse Act (Type I)					
allow access		espionage		mismanage	
analyze system response		exploit vulnerability		mispresentation	
arson		extortion		misrepresentation	
assult		fabricate		misroute	
blackmail		fake communication		observe system behavior	
break		fake call forwarding		obtain data/info/file	
bug		falsify		obtain privileges	
bypass control		forge		overflow	
cause error		fraud		penetration	
cause shortage		gain access		piggyback	
change logs		guess password		piracy	
cheat		hack		plant	
circumvent		hangup hook		random snooping	
compromise		insert illegal value		relocation	
consume/waste resources		insert logic bomb		reluctance to exercise	
contaminate		insert time bomb		replay	
corrupt		insert trapdoor		reveal	
counterfeit		insert trojan horse		sabotage	
covert channel		insert virus		seek access	
crack		insert worm		seize	
damage		intercept		shoulder surf	
deception		interfere		spoof	
degrade		interrupt		sniff	
delay		jam		steal	
deny service		larcen		subvert	
destroy		malfunction		suppress information	
destruct		malpractice		surveillance	
disable		manipulate		take possesion of	
disclose		masquerade		tamper with	
disrupt		mischief		terror	
dumpster diving		misconfiguration		theft	
eavesdrop		misevaluation		trespass	
embezzlement		misinformation		wiretap	

Misuse Act (Type II - if performed unauthorized)					
access		enable		remove	
accreditate		encrypt		repeat	
allow		enforce		review	
announce		enter		revise	
assist		evaluate		run	
audit		examine		scan	
backup		execute		search	
browse		grant		set	
classify		identify		share	
consult		initiate		state	
control		instruct		store	
coordinate		investigate		submit	
copy		load		supervise	
create		login		supply	
decrypt		maintain		support	
delegate		modify/alter/change		suspend	
detect		monitor		transfer	
devise		move		transmit	
diagnose		notify		update	
dial-in		possess		upgrade	
disseminate		publish		validate	
distribute		read		warn	
eliminate		reduce		write	

Misuse Type			
accident			
omission			
	failure to act after an actual notice		
	failure to use necessary control		
comission			
	waste		
		inefficient use	
		inadequate supervision	
		poor quality control	
	mistake		
		inaccurate operation	
		unreliable operation	
	unethical practice		
		conflict of interest	
		disloyalty	
		fraud	
		embezzlement	
		privacy violation	
	attack		

Result		
response successful		
	preventing	
	limiting	
	correcting	
misuser found		
conviction		
	clandestine	
	legitimate	
	masquerade	
	external penetration	