1986

Preventing internal computer abuse.

Tart, Randal G.

NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

PREVENTING INTERNAL COMPUTER ABUSE

by

Randal Gerald Tart

December 1986

Thesis Advisor: Norman R. Lyons

UNCLASSIFIED
ECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b RESTRICTIVE MARKINGS
2a SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a NAME OF PERFORMING ORGANIZATION Naval Postgraduate School	6b OFFICE SYMBOL (If applicable) Code 54
7a NAME OF MONITORING ORGANIZATION Naval Postgraduate School	
6c ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000	7b ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000
8a NAME OF FUNDING/SPONSORING ORGANIZATION	8b OFFICE SYMBOL (If applicable)
9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	
8c ADDRESS (City, State, and ZIP Code)	10 SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO	PROJECT NO	TASK NO	WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification)
PREVENTING INTERNAL COMPUTER ABUSE

12 PERSONAL AUTHOR(S)
Tart, Randal G.

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Master's Thesis	FROM _____ TO _____	1986, December	106

16 SUPPLEMENTARY NOTATION

17 COSATI CODES			18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Internal Computer Abuse; Employee Computer Abuse; Top Management Control of Computer Abuse

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

American businesses lose millions of dollars every year through computer crime perpetrated by company employees. Most of these losses are the direct result of inadequate corporate security programs. They could be eliminated fairly easily if organizations would employ common sense and relatively inexpensive remedial actions that range from the mostly broad-based and non-technical efforts of top management to the very specific and technical measures inherent to lower management levels. This paper deals specifically with the steps that should be taken at the top management level. It proposes that top management must first develop a better understanding of the nature of the criminal threat and effect an ethical business environment that will detect/deter/prevent abusive inclinations. Top management must then ensure that a sound overall security program is

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT	21 ABSTRACT SECURITY CLASSIFICATION
☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	Unclassified
22a NAME OF RESPONSIBLE INDIVIDUAL Prof. Norman R. Lyons	22b TELEPHONE (Include Area Code) (408) 646-2666
	22c OFFICE SYMBOL Code 54Lb

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE
UNCLASSIFIED

19 - ABSTRACT - (CONTINUED)

in place as a framework within which specialized security controls can and must function. Finally, top management must initiate specific security controls and ensure that subordinate levels of managers follow suit.

Approved for public release; distribution is unlimited

Preventing Internal Computer Abuse

by

Randal Gerald Tart
Major, United States Army
B.S., United States Military Academy, 1972

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
December 1986

ABSTRACT

American businesses lose millions of dollars every year through computer crime perpetrated by company employees. Most of these losses are the direct result of inadequate corporate security programs. They could be eliminated fairly easily if organizations would employ common sense and relatively inexpensive remedial actions that range from the mostly broad-based and non-technical efforts of top management to the very specific and technical measures inherent to lower management levels. This paper deals specifically with the steps that should be taken at the top management level. It proposes that top management must first develop a better understanding of the nature of the criminal threat and effect an ethical business environment that will detect/deter/prevent abusive inclinations. Top management must then ensure that a sound overall security program is in place as a framework within which specialized security controls can and must function. Finally, top management must initiate specific security controls and ensure that subordinate levels of managers follow suit.

TABLE OF CONTENTS

I. INTRODUCTION

"Computer abuse" has been broadly defined as any incident associated with computer technology in which a victim suffered or could have suffered loss and a perpetrator, by intention, made or could have made gain [Ref. 1]. For purposes of this paper, it is more restrictively defined as any activity in which a computer system is used by an employee to commit fraud or theft or to deliberately misuse, alter, destroy, compromise or sabotage any organizational assets, including data and information. Nobody knows the amount of computer abuse that is occurring in the United States, because much (probably most) of it goes undetected, and there is some evidence that less than 15 percent of that which is detected is ever reported. [Ref. 2]

There is also fairly widespread disagreement among computer security "experts" about the extent to which computer abuse should be considered a problem in 1986. For example, a survey of 130 prosecutor's offices in 38 states, conducted by the National Center for Computer Crime Data, revealed that, last year, criminal charges were filed in just 75 cases of computer abuse reported in those jurisdictions. In dollar terms, those incidents totalled only $936,000 in system and data destruction. Another $551,660

were lost in program and data theft and $105,170 in cash theft. [Ref. 3]

Other surveys, however, suggest that the instances of actual computer abuse are not fairly represented by the number of cases that are reported and prosecuted. One such survey, conducted by the American Bar Association (ABA) for the same time period (1985) found estimated ". . . losses of $20 million to $45 million in the past year and said that nearly half the government agencies and businesses queried have suffered computer [abuse]." [Ref. 3] As can be seen, the ABA loss estimates are significantly higher than those suggested by the National Center for Computer Crime Data even though both surveys included as computer abuse any incident that involved computer technology and disregarded the source (internal or external) of the abuse. Still, even the ABA numbers pale in significance when considered in the context of a trillion dollar annual economy.

Dr. Jay BloomBecker, the Director of the National Computer Crime Data Center, agrees that the estimated dollar losses are relatively insignificant when compared with the annual national economy. Also, he agrees with the ABA that most instances of computer abuse are not reported, but he contends that the ABA statistics are probably too large. The findings of his organization indicate that, today, American companies have done a reasonably good job of countering computer abuse by reducing both the number of

incidents and the size of individual losses. He says that his organization refuses to get "caught up" in the numbers game that is played by so many experts in the field. [Ref. 4]

The reason that Dr. BloomBecker is unwilling to play the "numbers game" is that he feels the amount of money lost to computer abuse may be relatively unimportant. It represents only one aspect of the computer security problem. There are other, non-quantifiable, aspects that may be of even greater importance than just the dollar-size of the losses. In some cases, the quality of the losses of computer crime may be of paramount importance. For example, the potential loss to hostile intelligence agencies or through industrial espionage is incalculable in dollar terms.

In fact, the "quality" aspect of the computer losses represents such a tremendous potential risk to American information systems that it was recently addressed by the Department of Defense:

> On Nov 11, [1986], the Pentagon confirmed the worst fears of the information industry: It served notice that it intends to apply sweeping new controls over the contents of computer data bases to stem the flow of scientific, technical, and economic information to the Soviet bloc. [Ref. 5]

In this instance, the Pentagon is not really concerned about the dollar value of the information taken. It is, instead, so concerned about the quality or sensitivity of the stolen information that it has taken some rather drastic steps to stop the flow. The Business Week article, of which the

above quote is a part, went on to say that "jaws were hitting the floor all over the audience" as Diane Fontaine, head of the Pentagon's information systems directorate, startled a meeting of the Information Industry Association with a pronouncement that the Reagan Administration is studying ways to censor public data bases, even though the information contained in them may be unclassified and readily available elsewhere. [Ref. 5]

Computer data bases are the primary aim of the Administration's security efforts because they are considered ". . . gold mines for foreign agents." [Ref. 5] In the intense international competition for advanced technology, access to protected data files can often prove to be a distinct advantage to unscrupulous but sophisticated individuals or organizations capable of exploiting the benefits of information painstakingly accumulated by others. To the dismay of the American Civil Liberties Union and many business leaders, the former National Security Advisor, John Poindexter, issued a memorandum on November 5, 1986, giving federal agencies unprecedented powers to suppress information under a new sort of security classification, called "sensitive." Under this "classification," federal officials may refuse to divulge even unclassified material relating to national defense or foreign policy. [Ref. 5] Also, according to an Associated Press article, other more restrictive controls are expected to be included in a

pending 1987 Presidential executive order that will tighten information security still further by such measures as requiring better and more frequent background investigations and, possibly, stationing Defense Investigative Service agents permanently inside large defense contractor plants. [Ref. 6]

It is in this sense of the "quality" of computer abuse that Dr. BloomBecker believes that the proper focus of computer crime statistics should not be so much toward showing that computer abuse is a BIG problem, but rather that they be used as a tool to assist in eliminating the potential for abuse. For example, the Computer Crime Data Center has found that four of the top five abusers of computer systems are individuals who are "internal" to and working for the victim organization (these include full-time employees, part-time employees, consultants and contractors). [Ref. 4] So, while many organizations are currently focusing much of their attention and resources on the oft-publicized "system hacker," or external intruder, it appears that the major danger may be freely admitted into the organization every day.

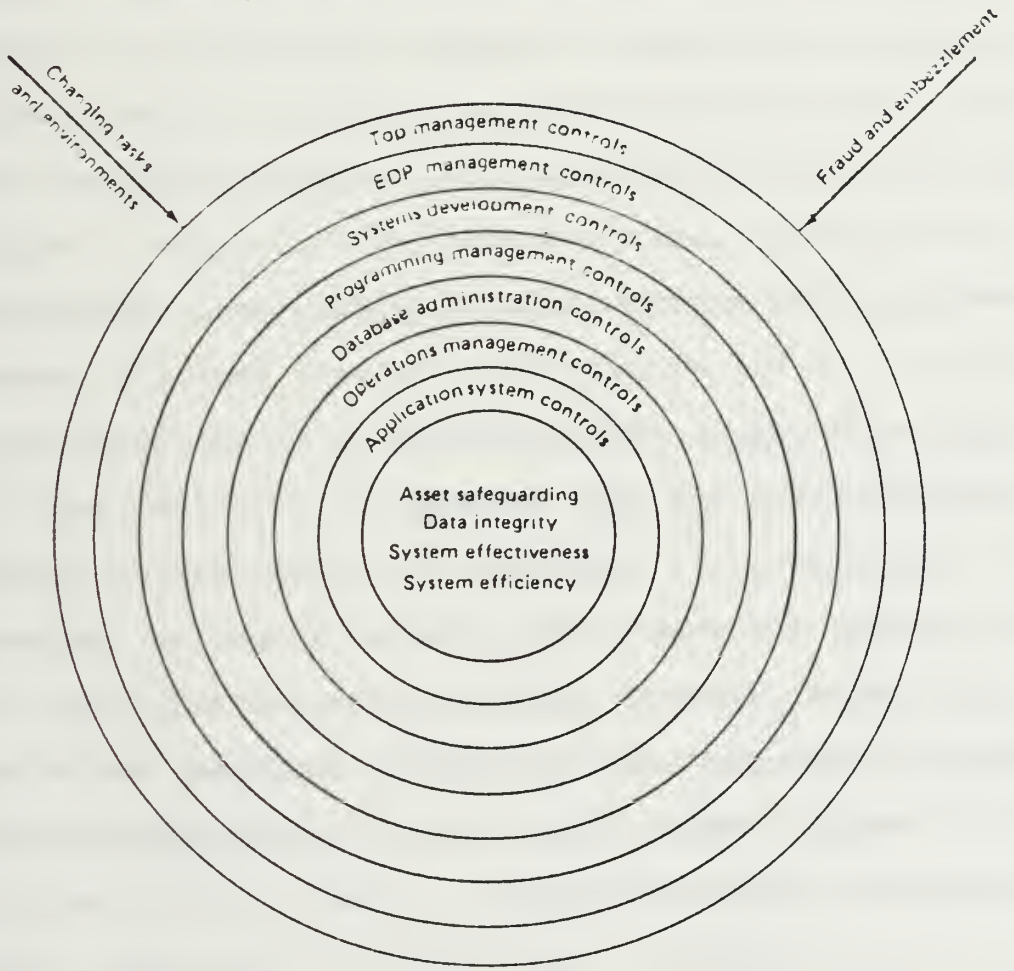
As suggested by the more restrictive definition of computer abuse, this thesis deals with the threat of information system abuse posed by organizational employees. The author agrees with Donn Parker that ". . . computer abuse and crime are [not] out of control or that they have reached

epidemic or calamitous proportions." [Ref. 2] Instead, it is believed that significant potential for computer abuse does exist in many individual organizations, mainly because of neglect of necessary security countermeasures by those organization's top management. This belief is supported by Peggy Watt, a correspondent for Computerword, who writes that only 43.3 percent of the organizations queried by the American Society of Industrial Computer Security even had a computer crime policy and still fewer (only 38.2 percent) had a model computer security program. [Ref. 3]

This thesis posits that those organizations that are not formally addressing computer security issues are leaving themselves open for abuse. It suggests that every business that employs computer assets needs a security program to help protect themselves against abuse, and especially that abuse generated by "insiders." Further, it suggests that the best countermeasures--the most cost-effective--are the practices and procedures already in place in most organizations. Proper employment of these basic managerial tools will greatly reduce the potential for computer abuse.

As a way of addressing computer security issues in the most straightforward and common sensibly correct manner possible, Ron Weber suggests that organizational leaders should view the computer security function as an "onion" whose layers of skin constitute the various levels of management and applications controls needed to adequately

protect the information system. In his book, EDP Auditing, he pictures the "onion" as shown below [Ref. 7]. Forces that erode the inner core (data integrity, asset safeguarding, system efficiency, and system effectiveness) must first penetrate the outer control layers. Weber says that to ". . . the extent that the outer layers of control are intact, it is likely the inner layers of control will be intact." [Ref. 7:p. 24]



This thesis will discuss Weber's outer layer of controls. More specifically, it will discuss the things that top management must consider and do to ensure that Weber's outer layer of security is intact so that it can be assured that the inner layers will be intact as well. The focus will be toward top managerial actions needed to secure the organizational computer assets against internal abuse.

Thus, in the chapters that follow, a process is described that will ensure the existence of a solid foundation on which a viable computer security effort may be built. The process first defines the possible sources of internally generated abuse and provides a profile of the "enemy" against whom the program must be targeted (Chapter II). Then, in Chapter III, the necessity of an ethical business environment in EDP organizations is discussed. Afterwards, a description of the makeup of an overall security program that will serve as a framework within which specialized control measures can and must function is made (Chapter IV). Finally, in Chapter V, specific top management-initiated controls needed to extend the framework and to prevent, detect, and deter internal computer abuse is detailed. It is cogently argued that top management must get intimately involved in each of these areas and lead the security effort to success or it will likely fail.

II. THE ENEMY

A. INTRODUCTION

As stated in the previous section, the present focus is on securing a sensitive computer system against internal abuse. In order for top management to properly direct the organization's security effort, it must first have a good understanding of the nature of the internal threat. This is particularly important in the computer systems arena because, normally, the threat is not easily identifiable. Generally, the computer abuser is a current and, probably, a well-regarded employee. Many managers have been shocked to discover that a highly trusted colleague, perhaps even their Saturday morning golfing partner, "doubled" as their firm's greatest criminal threat.

In this section, a profile of the "enemy" is established in order that top management will know against whom the security effort must be targeted. The discussion first looks at the types of computer criminals that have been identified and shows that each of these types represent significant internal threats to the computer system. It then concentrates on the most likely threat to most organizations, the amateur computer criminal, and provides a general description of this type of computer criminal and a discussion of why otherwise good employees might begin to

abuse the computer system. Finally, because the thrust of the security effort described is against the amateur computer criminal, other important characteristics of this type criminal are discussed in some detail.

B. PROFILE OF THE ENEMY

1. Types of Computer Criminals

Donn B. Parker, probably the most widely published authority on computer crime, writes that computer criminals may be categorized into one of seven types. These include extreme advocates, governments, system hackers, career criminals, deranged individuals, criminal organizations, and amateurs. Parker says that each type is mutually exclusive in character but, by changing his/her character, an individual may change from one type to another. [Ref. 2:p. 106]

Top management must be concerned with all these categories of computer criminals and, depending upon the purposes of the organization and the degree of sensitivity of the information processed on its EDP systems, it must take appropriate steps to combat the threats posed by them. For example, agents of foreign governments do pose significant internal risks to many computer organizations, as seen by the fact that Soviet KGB ". . . scientific collection orders have targeted dozens of American firms and over 60 universities" [Ref. 8] for high-technology information. Also, several European terrorist organizations have

specifically marked computer organizations for elimination, and there is considerable evidence that some of their most successful attacks have been linked to internal operations. [Ref. 9]

2. The Amateur Computer Criminal

However, while each of these types of computer criminals pose significant threats to information systems, the one that is considered to be the most dangerous is the amateur computer criminal. This belief is based on Parker's 1982 statement that most ". . . reported computer crime so far has been performed by amateurs" [Ref. 2:p. 107] and on his subjective opinion of the relative level of threat posed by each type of computer criminal, as shown in Table 1.

TABLE 1

RELATIVE THREAT LEVELS

Source of Threat	Past Threat: All Computer Crime
Amateur Criminals	High
Deranged Individuals	Low
Career Criminals	Low
Organized Criminal Groups	Low
Extreme Advocates	
- Economic	Low
- Religious	Low
- Political	Medium
Foreign Powers	Low

Source: [Ref. 2:p. 277]

A quick glance at a listing of the occupations of the perpetrators of all 293 cases of computer abuse reported up to (but not including) 1975 seems to verify Parker's subjective judgment:

TABLE 2

PERPETRATORS OCCUPATIONS

EDP employees	Persons	Cases
Computer maintenance engineers	99	5
EDP employees (undesignated)	87	60
Programmers	32	29
Computer operators	24	18
Keypunch operators	17	3
EDP managers	6	6
Systems analysts	3	3
Tape librarian	1	1
Non-EDP People		
Nonemployees	91	33
Students	49	31
General managers and vice presidents	17	16
Accountants	8	8
Clerks, assistants	6	5
Law enforcement officers	3	3
Political rioters--nonstudents	3	3
Auto driving school owners, employees	3	2
Claims personnel	3	1
Presidents of firms	2	2
County commissioner, supervisor	2	2
Insurance agents	2	2
Salesmen	2	2
Physicians	2	2
Army officer	1	1
Chief buyer	1	1
Controller	1	1
Auditor	1	1
Mayor	1	1
Messenger	1	1
Order entry clerk	1	1
Pharmacist	1	1
Public relations specialist	1	1
Real estate broker	1	1
Company secretary	1	1

TABLE 2 - (CONTINUED)

Non-EDP People	Persons	Cases
Head teller	1	1
Senior airline official	1	1
Senior analyst	1	1
Non-EDP employees undesignated	6	4
Undesignated		66

Source: [Ref. 1:p. 53]

As can be seen, most computer abusers are otherwise ordinary people in positions of trust. They may possess special computer-related skills, knowledge, and resources or they may not--it is significant to note that only 42.7 percent (125/293 = .4266) of the total cases were perpetrated by EDP employees. More often, the cases involved non-EDP employees and, frequently, these individuals occupied high-level, management-type positions and colluded with EDP-skilled persons [Ref. 2:p. 277], which accounts for the large number of people involved in many of the cases.

The breakdown demonstrates fairly clearly that the computer abuser who has been most identified and reported is overwhelmingly an amateur criminal. Parker suggests that about the only difference between those that are identified and reported and those that are not is that the former made mistakes in their crimes that led to their capture [Ref. 2:p. 277]. It is a fairly safe assumption that most unreported, as well as reported, cases of computer abuse are perpetrated by amateurs. Thus, the amateur is the primary

concern of this paper and his/her profile will be developed more fully in the following paragraphs.

Amateurs differ from Parker's other types of computer criminals in the following respects. They are not abnormal psychologically. Since they normally have authorized access to the system, they are not trespassers, as are system hackers. They do not depend on crime for their livelihood. They often do conspire in their crimes, but normally not to the degree that they could be classified as organized or government-sponsored criminals. Amateurs are generally not extreme advocates for any cause other than resolving their own personal problems.

Their problems include money, family, drug or alcohol addiction, gambling, or work-related difficulties perhaps created by the stressful environment in which they must function. They often consider their problems to be unshareable and find that violating their trust or using their special capabilities is a means of solving their problems. Other individuals may have a need to obtain personal goals not in consonance with the organization or to satisfy egotistical drives by means of malicious acts. Thus, amateurs may perform a wide variety of white-collar crimes or violent crimes such as sabotage. They are not necessarily extremely intelligent, but usually they are expert in the functions of their acts. [Ref. 2:pp. 107-108]

C. OTHER IMPORTANT CHARACTERISTICS OF THE AMATEUR COMPUTER CRIMINAL

As mentioned, amateurs have traditionally posed the greatest threat to an organization's computer assets. It is the amateur computer criminal that is the primary "enemy" against whom the security effort must be targeted. So, in the discussion that follows, some additional characteristics of the amateur computer criminal will be enumerated. Top level managers must consider these characteristics when formulating their security program and controls. The characteristics are mostly borrowed from Parker's Crime By Computer and are based on findings of the Stanford Research Institute. They include the following areas.

1. Age

Perpetrators are young, eighteen to thirty years old, except those in management positions who tend to be somewhat older. This is not surprising, considering that the age of all computer personnel is lower than in most other occupations. However, while not surprising, the youthfulness of the criminal relative to the high degree of trust inherent to EDP positions has often been a significant factor in computer abuse cases. The desperation frequently associated with the very stressful EDP environment combined with the courage, recklessness, and self-confidence of youth appears to be a risky mix. Also, behavioral scientists suggest that the younger the person, the greater his cynicism about managers and jobs; excessive cynicism encourages

unethical behavior on the grounds that "I'd be a fool not to if everyone else is." [Ref. 10]

2. Gender

Women generally have not been as susceptible to computer crime as men. When they are involved, they tend to be keypunch operators or clerks and are working in concert with others.

3. Rationalization of Misconduct

"Discovered" perpetrators often put more energy into rationalizing their criminality than they did into performing it. They work very hard to reduce the element of criminality in their motives. They can argue convincingly that their misconduct was reasonable under the circumstances. Their actions were designed to cause the least harm to the least number of people and, yet, still successfully solve their problems.

4. Unintentional Criminality

Amateur computer criminals generally feel very bad about violating the trust inherent in their positions, and they almost always intend to restore or make up for the loss suffered by the victim. However, they often find that committing the crime was easier than restoring the status quo in an undiscovered way. Many computer embezzlers conceived of themselves as borrowers (vice thieves) since they fully intended to return the money. Those that "borrowed" money over a period of time, later discovered that there was no

way to return it and, thus, in their minds, became criminals without intending to do so.

5. Personal Characteristics

Perpetrators are usually bright, eager, highly motivated, courageous, adventuresome, and qualified people willing to accept a technical challenge. They have exactly the qualities that make them desirable computer systems employees. Thus, designing safeguards under the assumption that potential perpetrators will not be aware of the technical intricacies is a futile exercise. The principal threat against which protection is required is the perpetrator who knows as much about the system as the designers.

6. Social Mores

Amateur computer criminals tend to differentiate between doing harm to individual people, which they feel is immoral, and doing harm to organizations, which they believe, in some circumstances, is not immoral. Often they claim that they are just getting even for the wrongs that the organization has done to themselves or to society.

7. Feelings Toward Employer

Some form of disgruntlement with their employers is almost always present among amateur computer criminals. They generally identify with their technology to a greater degree than with their employer or the business activity. Thus, high stress and discontent are quite common as EDP professionals try to do their jobs, stay abreast of a

rapidly changing technology, change practices and procedures to incorporate advancements, and deal with managers who are lacking in skills and/or understanding of new computer technology.

8. Greatest Fear

Perpetrators most strongly fear unanticipated detection and exposure. They are generally white-collar types for whom the exposure would cause great embarrassment, loss of face and prestige among their peers and families. The importance of this characteristic is that detection, as a means of protection, is at least as important as prevention.

9. Programmers

Programmers appear to be somewhat susceptible to becoming abusive toward the computer system. As indicated by Table 1, roughly 10% (29/293 = .099) of all cases reported up to 1975 were perpetrated by programmers. This is caused by several factors. Programming can be a most overwhelming, intense, and challenging activity that can obscure many other values. The development of software is an exercise that is rife with opportunities for criminal misconduct. Finally, some programmers get so immersed in their work that they lose all contact with reality. They are called computer "bums" and will sit riveted and transfixed to a CRT for 20-30 hours at a time, barely eating at all. They are compulsive and susceptible to misconduct.

When programmers are involved, they often work in collusion with others.

10. Collusion

Amateurs often collude with others in performing their criminal acts. One study of 50 incidents, involving losses in excess of $100,000 each, showed that collusion was involved in 39 percent of the cases and 32 percent of the losses [Ref. 12:p. 28]. This is because the computer crimes with the greatest potential rewards often require more skills, knowledge, and access than any one individual may possess. Collusion tends to involve a technical person who can perpetrate the act and another person who is in a position to translate the act into some form of gain. The differential association theory, which states that perpetrators' acts tend to deviate only slightly from the accepted and common practices of their associates, applies strongly in explaining collusion. A group of people working together will sometimes tend to reinforce one another in the minor unethical acts that can grow to serious acts (e.g., they'll take home pencils today, paper pads tomorrow, and pocket calculators the next day). [Ref. 1:pp. 41-51]

11. Ethical Breakdown

In Fighting Computer Crime, Parker describes another characteristic of the amateur computer criminal that has been repeatedly observed and that is noteworthy. This characteristic manifests itself in the form of those

individuals who are known to possess high ethical standards and yet who have learned to ignore them in a very technical environment that treats employees equally regardless of their ethical values and in which abusive acts can be easily concealed. Such a situation describes exactly the environment surrounding a sensitive computer system and, not surprisingly, Parker says the numbers of these individuals ". . . is growing as the percentage of assets and asset records processed by computers increase." [Ref. 2:p. 15]

12. Other Characteristics

Brian Starfire, a Washington, D.C., computer consultant, recently confirmed in his nationally syndicated column much of Parker's description of the computer criminal. Quoting the "First Annual Statistical Report," which is based on the 75 reported and tried cases that were studied by the National Center for Computer Crime Data, Starfire also writes that most non-student criminals are 22 to 30 years old and occupy programming positions (just over 14% of the survey sample), followed by data entry clerks and bank tellers. Further, theft of money was the most common type of crime (45% of the total), with theft of software or data and willful damage to software (combined at 16%) being the next largest areas abused by the amateur. The only other significant single area of abuse was theft of services which represented 10% of the total computer crimes reported. [Ref. 11]

D. SUMMARY

The amateur computer criminal is the primary "enemy" that must be targeted by the computer security effort. The amateur commits the majority of the abusive acts against computer systems even though he/she is not expert in criminal activity. Amateur computer criminals are particularly difficult with which to deal because they are not readily identifiable and because they are, for the most part, otherwise good citizens and employees. They are generally insidious and possess most of the qualities and attributes that are found in the organization's very finest workers. Stemming their abusive behavior without employing overly restrictive and counter-productive safeguards or an environment of distrust is a formidable task. In the sections that follow, the characteristics of amateur computer criminals are considered as the overall security effort is formulated.

III. ETHICAL BUSINESS ENVIRONMENT

A. INTRODUCTION

Before top management can effectively introduce a computer security program or any specific control measures into the corporate workplace, it is first necessary that the executives ensure that a healthy ethical business climate predominates all other facets of the work environment. This is so because of the natural tendency to circumvent controls, especially those that may be viewed as obstacles to progress in other important areas. Since top management cannot be omnipresent to ensure that its prescribed security measures are being employed, it must rely upon the goodness and professionalism of subordinate personnel in this regard. Thus a strongly internalized sense of ethical conduct, ubiquitous at all levels of the organizations is of paramount importance if information systems are to be secure.

In this section, the concept of ethical business behavior is explored in some detail. First, the requirement for sound business ethics in a computer organization is discussed. Then, four rationalizations, whose widespread acceptance in organizations cause unethical behavior, are presented. Finally, the significance of these

rationalizations, especially for top management of an organization that employs computer systems, is considered.

B. REQUIREMENT FOR ETHICAL BUSINESS ENVIRONMENT

The requirement for a strong, ethical environment in any business seems obvious. It appears especially obvious when one considers the security needs of a computer organization because ethical conduct serves as the foundation on which the overall security program must be built. It is not only at the core of individual control mechanisms, in essence making them viable safeguards, but it properly recognizes the fact that most employees want to (and, under normal circumstances, will) act ethically. Thus, an ethical business environment is most facilitative of relatively unencumbered productive effort and would have to be considered as the most cost-efficient security control mechanism.

The fact that ethics is discussed here separately, and not later with the other control mechanisms, only attests to its overwhelming importance to a computer organization. By fostering a strong sense of ethical propriety, management can be quite effective in stymieing abusive inclinations. Also, by establishing and relying upon a code of ethics, management is allowed to take a precautionary posture that minimizes the opportunities or perceived need for abuse on the one hand while motivating honest activities on the other (see the discussion on "Standards of Conduct" in Chapter V

for precautions). To function differently would be unwise because, as Leonard Krauss and Aileen MacGahan write, ". . . it makes little sense, and is quite counterproductive, for management to harbor a distrustful attitude." [Ref. 12]

C. FOUR RATIONALIZATIONS THAT CAUSE UNETHICAL BEHAVIOR

In view of the above, one would think that ethical business conduct would be strongly internalized into the cultures of most business organizations. However, this apparently is not the case. As Dr. Saul Gellerman, Dean of the University of Dallas Graduate School of Management, wrote in the Harvard Business Review, roughly two-thirds of America's 500 largest corporations have been involved, in the last ten years, in some form of criminal behavior [Ref. 13] Also, consider the recent disclosures of insider trading on Wall Street. Financial malfeasance at the very heart of corporate America appears to be no insignificant threat.

Dr. Gellerman postulates that this dangerous situation is the result of the pervasiveness within organizations of four "rationalizations" that can cause managers to fall prey to ill-advised, criminal conduct:

> A belief that the activity is within reasonable ethical and legal limits--that is, that it is not "really" illegal or immoral.
>
> A belief that the activity is in the individual's or the corporation's best interests--that the individual would somehow be expected to undertake the activity.

A belief that the activity is "safe" because it will never be found out or publicized; the classic crime-and-punishment issue of discovery.

A belief that because the activity helps the company the company will condone it and even protect the person who engages in it. [Ref. 13:p. 88]

Since at least one of these rationalizations is, to some extent, virtually always used as justification by managers when they engage in illegitimate activities, they pose significant threats to the high ethical standards and, hence, the internal security posture, of any organization and especially to those that electronically store and process sensitive information (recall that one of the characteristics of the amateur computer criminal is his/her strong tendency to rationalize the misconduct). So, in the paragraphs that follow, these rationalizations are described and discussed more fully, and then their significance for EDP organizations will be explained.

The first rationalization, that an action is not "really" immoral or illegal, is a very old issue. How far is too far? Exactly where is the line between smart and too smart; between sharp and shady; and between profit maximization and illegal conduct? The issue is complex and involves significant interplay between top management's goals and middle managers' efforts to interpret those goals. [Ref. 13:p. 87]

Top executives rarely overtly ask a subordinate to commit an act that both know is against the law or is

imprudent. However, their actions sometimes speak loudly enough. They can leave things unsaid or give the impression that there are things they do not want to know about. They can seem, deliberately or otherwise, to distance themselves from their subordinates' tactical decisions, so they will not be involved if things go awry. They can promise rich rewards for achieving lofty goals and imply that the means to achievement of these goals will not be too closely scrutinized. [Ref. 13:p. 88]

The second reason that managers take unhealthy risks, believing that the unethical conduct is in the individual's or the corporation's best interests, nearly always results from a parochial view of the interests involved. Ambitious managers search for ways to make themselves and their organizations look good. They attempt to distinguish themselves by outperforming their peers. Many, in their selfish efforts to succeed, will sacrifice potentially outstanding long-term gain for potentially smaller, but more immediately recognized, short-term rewards. The sad truth is that many managers have been promoted because of "great" results obtained in these ways, leaving unfortunate successors to inherit the inevitable whirlwind. [Ref. 13:p. 88]

Believing that one can get away with abusive (even criminal) behavior, the third rationalization for taking risks, is perhaps the most difficult with which to deal, because it is so often true. A great amount of misconduct

escapes detection. [Ref. 10:p. 89] This rationalization is particularly relevant to a computer system's environment because of the fleeting nature of the evidence of abusive acts and the fact that, relatively speaking, ignorance of computer technology reigns supreme among the general populace which often can be easily duped (including honest managers and officials attempting to investigate the abuse).

Also very relevant to a computer system's environment is the final rationalization that allows/encourages managers to commit criminal acts, the belief that the company will condone actions taken in its interests and will even protect the responsible managers. The primary question here is, "How does top management foster a healthy sense of company loyalty without allowing it to go berserk?" [Ref. 13:p. 90] The issues behind this question are many and appear to apply especially to computer organizations. As Starfire wrote, many (perhaps most) computer crimes go unreported, even after they are discovered. Also, since only 20 percent of the relatively few people that are tried and convicted ever serve any prison time, it ". . . is one of the safest crimes anyone could commit." [Ref. 11]

These four rationalizations were posited by Gellerman after an in-depth review of three incidents in which unethical behavior by top management proved calamitous (and, in two of the cases, nearly fatal) for three of America's financial and industrial giants. The three companies

involved were Manville Corporation, Continental Illinois Bank, and E.F. Hutton. Although the details of the three cases differ greatly, there are some similarities in them that are worthy of consideration.

First, the executives whose unethical conduct cost their organizations so dearly, were not extraordinary people. As Gellerman said, the ". . . people involved were probably ordinary men and women for the most part, not very different from you and me." [Ref. 13:p. 86] They found themselves in a dilemma, and they solved it in a way that seemed the least troublesome and most advantageous for their respective companies (one might call them high-level amateur criminals!).

The cases also illustrate the fine line that exists between acceptable and unacceptable managerial behavior: managers are expected to pursue their companies' best interests but not overstep the bounds that outsiders will tolerate [Ref. 13:p. 86]. When the "heat is on," managers may neglect standard controls and, if pushed by very lofty goals, may not see clearly their real interests. Instead, they may focus on the ends, overlook the ethical questions associated with their choice of means, and ultimately hurt themselves and their organizations. [Ref. 13:p. 87]

D. SIGNIFICANCE OF RATIONALIZATIONS FOR EDP ORGANIZATIONS

The significance of Gellerman's findings for the top management of an organization employing computerized information systems is enormous. Consider the likely outcome of

a situation in which widespread rationalization is allowed to persist in a business alongside other predispositions toward abuse. For instance, it has been discovered that the motives most frequently driving employees to criminally abuse their computers are:

1. Avarice.
2. Desire for the "good life" and material possessions.
3. Financial problems (arising from pressures to spend beyond one's means, drug abuse, illnesses, college costs, gambling debts, and much more).
4. Ego gratification (the challenge of it).
5. Charitable (take from the rich and give to the needy).
6. Revenge (due to a perceived grievance against the employer). [Ref. 12:p. 36]

If these motives are strongly felt and if Gellerman's rationalization process has been widely assimilated into the norms of the organization, otherwise honest employees will very likely abuse the computer system and will have very little difficulty justifying their actions in their own minds. This explains the increased frequency with which Parker has observed the amateur computer criminal who has high ethical standards and, yet, begins to act dishonestly because others' unethical acts are seen as being rewarded, while ethical behavior is not only overlooked but, in fact, sometimes hampers progress in a sterile, technical environment.

Another significant aspect of the rationalizations for top management is that the rationalizations suggest that the

mores of the company must be set by top management. This means that top managers must first ensure that their own behavior is beyond reproach and then mandate a company-wide ethics policy that is intertwined with corporate culture [Ref. 14]. It is not enough for them to simply dictate the policies; they must also practice them in their daily work routines. As has been written:

> Every young manager will experience the pressure of others' behavior as determinant of his own. [Most]. . . maintain that their superior's behavior is the major reason they behave unethically. It is the top that sets the ethical tone in most organizations and this is one of the gravest obligations of high-level executives. Their behavior will be emulated and converted into institutionalized custom by lower managers. [Ref. 10:p. 105]

In a computer organization there is also much risk that unethical behavior by managers will be emulated and institutionalized by nonmanagerial personnel. This is another significant aspect of the four rationalizations that must be considered by top management. While the discussion so far has dealt entirely with managerial ethical issues, it is important to note that practically everything mentioned applies equally well at all levels of many organizations and especially to those that electronically manipulate data.

In fact, the great extent to which illegal conduct has been found to occur at all levels of a computer organization prompted Robert Courtney, an experienced computer security consultant, to dub the phenomenon as the "democratization of white-collar crime." He says that white-collar crime used to be the domain of managers and other traditional

occupations of high trust. However, the use of computers has resulted in new and larger numbers of occupations in positions of trust and changed patterns of trust in old occupations. [Ref. 2:p. 103] It is vitally important that top management recognize this fact and take steps to ensure that the expanded nonmanagerial segment of the computer organization acts ethically, as well as the organization's managerial personnel.

E. SUMMARY

Thus, top management must institute ethical business practices at all levels of the organization. It necessarily must begin the process by acting ethically itself (lead the effort from the front) and, then, it must ensure that subordinate personnel understand the need for acting ethically and that unethical behavior will not be tolerated. Top management can greatly facilitate this effort by realizing the dangers inherent to the existence of Gellerman's four rationalizations and by proscribing their employment from the organization. Once the appropriate ethical business environment has been established, top management can then turn its attention to setting up the overall security program.

IV. OVERALL SECURITY PROGRAM

A. INTRODUCTION

After top management has ensured the existence of an appropriate ethical business environment, it must then use that environment as a foundation on which to establish an overall security program. This is important because an ethical business environment, alone, will not succeed and because no amount of individual controls, discussed in the next section, will be sufficient without an overall computer security program within which the safeguards can function. [Ref. 15] This chapter discusses some of the important aspects of the overall security program. It describes some of the important issues that must be considered by top management in setting up an overall security program and demonstrates the importance of top management's active involvement in formulating and supporting the security effort. It then discusses the elements that should be included in any overall security program if it is to viably serve as a framework within which specific control mechanisms can function.

B. IMPORTANCE OF TOP MANAGERIAL INVOLVEMENT

Just as top management's active involvement in and support of the appropriate ethical environment is of paramount importance, the same can be said of the

functioning of the overall security program. Indeed, the two issues are so closely related and the management of their processes so closely interconnected that it is difficult to separate them, even as topics of discussion. Surely both are worthy of top managerial consideration.

In the case of organizations that employ computerized information systems, top management's involvement in prescribing and overseeing the security program is especially important. This is not only true because computerized information is very vulnerable (e.g., it may be easily accessed, stolen, altered, or destroyed without anyone knowing for long periods of time), but also because the controls, themselves, are frequently unwieldy, burdensome overheads that act antithetically to the very purposes of the computer's original "being." Controls stifle creativity and innovation; workers feel encumbered by them (a feeling, often with much merit!); and they will be circumvented unless they are carefully planned and implemented and are seen as being fully supported by top-level management.

Also, since every business is different and has different perceived needs, the specific makeup of the overall security program may naturally be somewhat debatable and will require active high-level participation to be accepted as appropriate for the particular situation. It would be most advantageous if some organization, such as the National Bureau of Standards (NBS), could simply specify a

functional security program for any and all companies. Such a specification, however, is not possible because of the many variables involved.

Consider, for example, that:

> Each individual computer [organization] is a unique case. The threats it faces are a function of its location, its workforce, its parent organization, its workload, its equipment and software, and its physical facilities. Furthermore, the threats faced by an installation change over time due to changes in employee morale, the workload, the competitive situation, the financial health of the parent organization, and even changes in the environment and physical situation. For instance, the fire hazard may change drastically when a new tenant moves into the floor overhead; competitors' interest in product design information or sales figures may suddenly flourish when the parent company successfully launches a new product. Any event which changes the computer environment or the attitudes of people working in that environment can cause a change in the threat posture and should prompt reanalysis to determine if additional countermeasures are warranted. [Ref. 16]

Deriving an effective security program for such a diverse and dynamic environment is difficult. It is often nearly impossible without the active involvement of top executives. This simple realization by top management is a most important ingredient to any effective security program.

It is also important that top management realize that its involvement can be dysfunctional, however, in some cases. As top managers consider the requirements for a computer security program, they will gather environmental information in either a preceptive or receptive manner. Those that "preceive" will judge the situation based on their preconceived notions about computers and computer security. Receptive individuals, on the other hand, are not

unduly swayed by preconceptions and reach their conclusions in a more objective manner. [Ref. 17]

High-level managerial recognition of this fact is an extremely important issue to the management of computer systems' security. The personal preferences of top management will often dictate the final nature of the overall security program. Depending upon how top management views the importance of the information system within the organization (as either a strategic or merely a supportive activity), it will take a more or less active role in managing and supporting the system. [Ref. 18] Today, because many high-level managers have reached their positions with little exposure to computer systems in their early careers, or perhaps because their exposure was to radically different types of computer issues, they suffer an extremely acute discomfort in addressing information systems' matters [Ref. 18:p. 36].

Such "discomfortable" individuals are likely to approach a computer security program in a preceptive manner and, figuratively, transfer their suffering to the security effort. Under these circumstances, there is no way that a viable security program can exist. This situation possibly underlies a study finding of the Institute of Internal Auditors that general (top) management support for audit and control programs needs to be improved if the integrity of

the computer-based information systems is to be ensured. [Ref. 15:p. 11]

Ensuring the integrity of the information system comes at great cost, and this represents another reason why top management must be involved in the implementation of the overall security program. Not only are security controls often expensive to purchase and install, but they can be even more costly in terms of their negative impact on organizational productivity. Security generally means controls and controls generally mean that laissez-faire will be replaced with encumbrances on the production floor. Such a situation can quickly become destructive as the best interests of production personnel are placed directly at odds with the security needs of the organization. Conflicts ranging from a disregard of the controls (if allowed to occur) to outright abuse of the system (if the controls are strenuously enforced and are viewed as too debilitating) are likely to arise, depending upon how the situation is managed.

Top-level management is clearly needed under such circumstances. Its task in this environment is to ensure the appropriate structure and management processes are in place to referee the balance between the information system user and safeguards imposed by the computer security program. A solid ethical business environment can greatly facilitate the balancing act (by allowing looser controls

and, hence, more unfettered work processes), but dozens of security controls will still be necessary. Deciding the extent to which these controls can be allowed to interfere with an organization's raison d'etre falls clearly within the province of top management.

In making this decision, it is important for top management to realize that the inherent risks of an information system mean that it cannot be made 100 percent risk-free and still remain functional. Management must decide not only the character of the overall security program and the types of controls employed, but it must also decide the level of risk that is acceptable and the amount of time, energy, money, creativity, and/or innovation that can be expended in attaining that level. A tradeoff must be made between the direct and indirect costs of the security program and the probable loss that could be incurred if the security effort were not made. [Ref. 19]

In light of the above, it is incumbent upon top management to effect an overall security program that is appropriate for its individual organization at that particular time. It must provide leadership, resources, and support for the effort. It must actively participate in the formulation of the overall security program because it is that program that will serve as the framework in which specific safeguards will be implemented. A small investment of high-level time and energy during the inception of the security program will

later pay significant dividends in terms of enhanced effectiveness of the security effort, minimized damage to the efficiency (productivity)of the organization's mainstay operations, less duplication and fewer requirements for change, and better acceptance and support at all hierarchical levels.

C. NECESSARY ELEMENTS OF THE OVERALL SECURITY PROGRAM

The remaining important issue, with which top management must deal, is the makeup of the overall security program. As has previously been stated, it is impossible to specify the exact composition of a security program that can be universally employed in any organization. However, there are certain elements of a security program that should be considered and stated by top managers of any organization as they implement a security strategy. These include the objectives of the program, issues that should be written into the program's charter, comprehensive and wide-ranging security guidance, and other key ingredients that will be discussed below.

1. Objectives

R.C. Summers, in "An Overview of Computer Security," says that a computer security program should ". . . include concepts, techniques, and measures that are used to protect computing systems and the information they maintain against deliberate or accidental threats." [Ref. 20] He states that the objectives of a good security program should be to:

a. Protect The System

The security program must ensure the protection of information against unauthorized modification, destruction, or disclosure. This is especially important when one considers that the computer has become many organization's main repository of records representing all types of information ranging from personnel files to cash and inventory records to trade secrets.

b. Maintain Integrity/Availability

The security program must ensure the maintenance of the integrity and availability of the computing system and its applications. This area includes the use of computers in such applications as manufacturing process control and airline reservation systems in which the data must be protected and readily available for use.

c. Secure Computer Records

The program must ensure that computer records are secured in compliance with the legally mandated requirements of the countries and states in which the system is operated. Examples of such legal mandates include provisions of the Foreign Corrupt Practices Act and the 1974 Privacy Act. [Ref. 20:p. 309]

2. Security Charter

In order for these objectives to be met, the computer security program must be based on top management policy and support that clearly define a security charter and its

scope [Ref. 15]. While these are also situation-dependent and cannot be described specifically, there are certain items that should be included in the security charter of most organizations. For example, the specific goals and objectives of the security program should be included, along with the degree to which top management intends to support the program and the authority that is possessed by security personnel. These things should be clearly specified in writing because of the likelihood of conflict between security implementors and system users. The written document can serve as a contract between top management and security personnel and eliminate much misunderstanding, frustration, and organizational infighting. Also, the mere act of formalizing and reducing to writing the scope of the security program, the bounds of the authority of security personnel, and the degree of managerial support forces high-level managers to address these important issues head-on and in an open-eyed fashion.

3. Security Guidance

Another issue that should be addressed in a similar fashion is top management's security guidance to the organization. This guidance should be fairly specific in intent but should be comprehensive and wide-ranging so as to cover all areas that are deemed important by top management. For example, the Department of the Army's guidance begins with a general statement:

> Sensitive defense information processed by Army automated operations and associated telecommunication systems must be safeguarded against unauthorized access, modification, use, destruction, or denial of use. [Ref. 21]

The Army then proceeds to list 14 specific guidelines, along with their associated subparagraphs. Many organizations will not require the type of in-depth guidance from the top that has been provided by the Department of the Army (DA), but much of the Army's guidance is relevant to any organization that has a need to secure its computer assets.

A good case in point is DA's policy that resolution ". . . of the complex problems inherent in automation security requires an approach which cuts across functional lines . . . [and] the greatest degree of coordination and cooperation between all levels of management." [Ref. 21] The "top brass" of the Army has seen the need to concern itself with such mundane matters, and its counterparts in any organization employing computer systems should do likewise. Other DA-directed guidance that top management of civilian businesses should include in their security programs includes the features listed in Table 3. These items are briefly described in the following paragraphs.

a. Risk Management Programs

Top management should mandate the establishment of a formal risk management program for each system handling sensitive information. Security measures should be applied in response to identified risks. [Ref. 21] Ron Weber says that a formal risk management program should consist of the

TABLE 3

ITEMS TO BE INCLUDED IN THE OVERALL SECURITY PROGRAM

- Risk Management Programs
- Control and Compliance Audits
- Protection of Remote Devices
- Priority Employment of Countermeasures
- Design Security Measures into New Systems
- Balance Security with Security Needs
- Background Investigation
- Performance Appraisals

following three major activities: risk identification, risk measurement, and risk control. [Ref. 7:p. 76] Each will be briefly discussed below.

(1) Risk Identification. The first step in risk management is to make an inventory of potential disasters that face the organization. This inventory should include consideration of natural disasters (e.g., hurricanes); man-made disasters (e.g., accidents, riots, sabotage); external threats and financial disasters (e.g., legal/social responsibilities, management changes, competition changes); instability and unreliability of man and high-tech machinery; and, hostile action (e.g., espionage, fraud, theft, mischief). Each list of potential disasters must be complete so that contingency plans will not be inadvertently omitted.

(2) Risk Measurement. Assessing the loss that may occur from different disasters is difficult, but it must be accomplished as a basis for establishing the amount of money that should be spent on security. One way of measuring risk is to estimate the possible losses that can occur from a disaster, and the probability of the disaster, itself, occurring. These estimates form the basis of calculating the expected loss from possible disasters facing the organization. The expected loss in turn forms the basis for deciding how much to spend on risk control.

(3) Risk Control. Risks can be controlled through system design, installation of security measures, and regular security audits. However, some residual risk will always exist. This type risk may be handled by the individual organization's treating any losses as normal operating expenses; by sharing the risk with other firms through trade associations (e.g., members agree to provide each other with backup facilities); or, the risk may be transferred contractually through insurance (discussed later). [Ref. 7:pp. 76-77]

b. Control and Compliance Audits

Requiring strict control and compliance audits of operations and software development and maintenance activities should be a top management priority. [Ref. 21] Weber suggests that, in control audits, both management and application controls be reviewed. He says that management

controls should be checked first because pervasive weaknesses in these controls may cause the auditor to deem further review to be unnecessary. When auditing controls, the auditor should assume that necessary controls are in place and functioning as alleged by the organization. He/she then identifies causes of possible loss and evaluates the effectiveness of the controls at prohibiting the expected loss or at reducing the losses to acceptable levels.

The purpose of compliance auditing is to determine whether or not the system of internal controls operates as it is purported to operate. The auditor seeks to determine whether or not alleged controls in fact exist and if they work reliably. In compliance auditing, computer-assisted testing is especially valuable. [Ref. 7:pp. 30-31]

c. Protection of Remote Devices

Top management must recognize the peculiar vulnerabilities inherent in remote terminal devices and ensure that EDP management adequately protects these systems. [Ref. 21] Remote devices may be teletypewriters, keyboard/displays, minicomputers, microcomputers with modems, remote job entry stations, and automated teller machines. Because they are machines through which data are entered and output received, and can be used to perpetrate computer fraud, their security deserves special attention.

Generally, security measures for these devices should be the same as for the central computing facility. Access to the terminals should be restricted when possible. It is particularly important to restrict access to terminals that are used to access or update sensitive data files, data bases, and programs. It may be desirable to isolate such terminals in locked rooms to which only authorized users have keys. [Ref. 12:pp. 170-171]

d. Priority Employment of Countermeasures

A key top management responsibility is to ensure that costly or elaborate security countermeasures are applied only after administrative, personnel, physical, and communication security controls have been shown to be inadequate. [Ref. 21] Inherent in this element are the system efficiency and effectiveness issues discussed by Weber. The countermeasures are considered to be effective if they accomplish their objective of ensuring a reasonable level of protection for the information system. They are considered efficient if they consume the minimum resources in achieving the expected level of effectiveness. [Ref. 7:p. 9]

As was suggested in the introduction to this thesis, many experts believe that most computer security needs can be met by common-sense measures, such as the administrative and personnel procedures currently employed in most organizations. It would be unwise to expend

resources on more elaborate measures until the benefits of the already-in-place controls have been maximized.

e. Design Security Measures into New Systems

Top management should mandate that protective measures be made a part of the original design of all new automated systems because of increased effectiveness and decreased cost. [Ref. 22] This guideline pertains particularly to the high-technology controls that are implemented at the lower levels of Weber's security onion. Specifically, it refers to security-related algorithms and auditing processes that are incorporated directly into a software system. It is important that these type controls be planned and incorporated at the earliest possible stages of development because of the exponential rate of increase in the costs of changing the software to add the features at a later stage. For example, as taught in Naval Postgraduate School software engineering classes, it is 100 times more expensive to change a large software system after the system is in operation than it is to simply incorporate the change during the initial requirements specification stage. While all security needs cannot be known in advance and, therefore, some countermeasures must be incorporated in later stages of development or after the applications program is in operation, it is very important that top management ensure that security is a prime design consideration and

that its needs, to the greatest extent possible, are included in the design specifications.

f. Balance Security With Security Needs

Top managers must require that measures taken to attain security objectives be commensurate with the importance of the operation to mission attainment, the sensitivity and criticality of the material being processed and the relative risks of the system. This guideline also deals with system efficiency and effectiveness issues and was previously discussed in Section IV.B.

g. Background Investigations

The personnel department must be required to conduct background investigations on all persons filling positions designated as sensitive [Ref. 21]. After an applicant has successfully completed all the initial hiring steps (e.g., employment application, job interview), the information must be reviewed and verified for accuracy. The purpose of the review and verification is twofold: to determine the suitability of the individual for the job; and to determine if there are any problems in the applicant's background that may indicate potential risks.

The verification, or background investigation, may be conducted by the company's own personnel or by an outside agency. Regardless of who performs it, the cost of verifying the information is dependent on the extent of the investigation (which is driven by security needs) and on the

time in which it must be completed. The goal of the background investigation is to prepare an impartial profile of the applicant from which an objective evaluation regarding the applicant's suitability can be made. The methods employed in conducting the investigation include personal, face-to-face contact, telephone interviews, and letters requesting desired information. The most effective way is face-to-face discussion; the least effective way is by written correspondence. [Ref. 12:p. 61]

In light of the recent spate of espionage incidents involving high-level government officials (e.g., a retired Naval intelligence officer, and agents of the FBI and CIA), all of whom presumably withstood extensive background investigations, it seems obvious that background checks cannot be considered the sole panacea. They should not be viewed as such, especially since good people can always go bad. Rather, background investigations should be viewed as an effective tool to "weed out" undesirable employee candidates and make the hiring procedures as effective as possible. This is not a terrible end, in and of itself, since, as Dick Brandon has been quoted as saying, better than 80 percent of the incidents of employee theft, fraud, misuse of information, or sabotage could have been prevented by more effective hiring procedures (based upon an examination of the records of the victimized organizations). [Ref. 12:p. 56]

h. Performance Appraisals

A final guideline that top management should specify is the requirement that EDP management must include in individual job descriptions the fact that maintenance or enhancement of EDP security has high priority and will be heavily weighed in performance appraisals. Stoner and Wankel define performance appraisal as ". . . the continuous process of feeding back to subordinates information about how well they are doing their work for the organization." [Ref. 17:p. 342] They also make a distinction between informal appraisals (i.e., those conducted spontaneously and on a day-to-day basis) and systematic appraisals that are more formal, occur semiannually or annually, and are directly related to merit raises and promotions. [Ref. 17:p. 342]

In order for performance appraisals to be effective at enhancing computer security, it is important that both types of appraisals be employed and that they include matters related to security. Spontaneous, day-to-day recognition of security-conscious performance of duty, coupled with appropriate pay raises based, in part, on security-enhancing work practices, will demonstrate clearly to all employees that the organization is paying more than "lip-service" to security. The old adage, "The squeaky wheel gets the grease," applies very well.

4. Other Key Elements

In addition to the objectives, security charter and guidance set forth by top management, the National Bureau of Standards says there are five other elements that should be included in an overall security program if individual controls are to be effectively implemented and used (see Table 4). [Ref. 12].

TABLE 4

NATIONAL BUREAU OF STANDARDS PRESCRIBED ELEMENTS FOR A SECURITY PROGRAM

- Computer Security Policy and Control
- System Design Standards
- Insurance
- Contracting Management
- Control Implementation Strategy

A brief discussion of these elements follows.

a. Computer Security Policy and Control

General management must ensure that the organization has a computer security policy coordination function. This function may be the responsibility of one or more persons who act as a focus for computer security policy and coordination. The function should be separate from, but closely coordinated with, EDP activities. Its primary responsibility is to develop workable computer security standards and to coordinate the acquisition or

implementation of security controls. In addition, this function works closely with auditing to verify compliance with standards and adequacy of the controls in place. [Ref. 15]

The policy and control function is important not only because computer security standards must be set commensurate with the needs of the organization (i.e., they must adequately control without becoming dysfunctional), but they must also be maintained in a state that is ready and prepared to meet the current threat. Managing this process is a real challenge because of the "natural enemies" of any program to prevent computer abuse. Krauss and MacGahan have identified three such natural enemies as being:

(1) Inertia. This is a two-headed monster that represents the organizational forces that make compliance with newly implemented security measures difficult to achieve and also those that create tendencies to affect business or system changes without considering computer security needs. [Ref. 12:p. 424]

(2) Changing Business Requirements. Business requirements can change as a result of competitive pressures, because new products and services are offered to the public, or because new technologies provide more desirable computer processing alternatives. These changing business requirements will be translated into changes in the company's computer applications. Unless there is a function

to supervise the changes and to ensure that computer security considerations are integrated into the new system, the company will be in trouble. [Ref. 12:p. 425]

(3) Changes to Organizational Structure. Any organization's structure can be expected to change over time, e.g., two departments may be combined under the direction of one manager. Such changes can be extremely hazardous unless security is a prime consideration at the time the change is made. For example, combining two departments may reduce the effect of dual controls over assets and the amount of separation of duties present in specific job applications. [Ref. 12:p. 425]

The computer security policy and control function should be designed to be especially on guard against these "natural enemies." Security policies and controls should be carefully selected so that it is easier for individuals to comply with them than it is to circumvent the security effort. Also, the policies and controls must be flexible and carefully managed to ensure that they remain appropriate for the dynamic environment in which they must function. Close coordination is a "must" under such circumstances, and therein lies the need of the security policy and control element.

b. System Design Standards

As suggested by the DA-directed guidelines, top management must ensure that internal controls and other

security mechanisms are included among the system design considerations. Standards or guidelines should be established to ensure that they are included. [Ref. 15:p. 10] This, in essence, means that standards should exist requiring that,

> . . . the [EDP] auditor participates in the system development process . . . to ensure, for a specific application system, that controls are built into the system to safeguard assets, ensure data integrity, and achieve system effectiveness and efficiency. [Ref. 7:p. 99]

The guidelines in the following table (Table 5) should be employed in the design of any computer system.

TABLE 5

SYSTEM DESIGN GUIDELINES

- Require user department and internal audit department approval of system development projects
- Require user department and internal audit department involvement in the system's specification and design phase of the project
- Require user department and internal audit department approval od detailed user specifications
- Require the preparation of detailed technical specifications and of a detailed plan for the development of the system.

Source: [Ref. 12:p. 125]

A brief description of these guidelines follows.

(1) Require User Department and Internal Audit Department Approval of System Development Projects. Before

a system development project is undertaken, the project should be reviewed, authorized, and approved in writing by the appropriate user department and internal audit department. These departments will have to be intimately involved in the system development process. They must, therefore, be aware of and approve all system development projects at their inception. [Ref. 12:p. 124]

(2) Require User Department and Internal Audit Department Involvement in the System Specification and Design Phase of the Project. The two departments should be involved in this phase of the project to ensure that the designed system complies with acceptable accounting policies, accounting and applications controls, and with other recordkeeping procedures required by regulatory agencies, such as the IRS. They should also ensure that the system is designed with management's objectives and user's needs in mind. [Ref. 12:p. 127]

(3) Require User Department and Internal Audit Department Approval of Detailed User Specification. System analysts must, in the course of designing the new system, prepare a detailed user specification manual fully describing the new system. This manual must be carefully reviewed by the user and internal audit departments to ensure that the specifications are accurate and complete and meet their needs. After these departments are satisfied, they must indicate their approval in writing. Then, and only then,

can the system development process proceed. [Ref. 12:p. 127]

(4) Require the Preparation of Detailed Technical Specifications and of a Detailed Plan for the Development of the System. These documents will guide the programming, file conversion, user training, and testing of the system being developed. They will also be used to guide, control, and check the programmers' work. [Ref. 12:p. 128]

c. Insurance

Top management must ensure that the insurance program is maintained in an up-to-date manner. [Ref. 15:p. 10] It can accomplish this by considering the types of insurance necessary for covering EDP equipment and facilities, EDP media, business interruptions, valuable papers and records, accounts receivable, and malpractice, errors, and omissions. [Ref. 16:pp. 86-87] It must then employ the eight steps in Table 6 (next page) to determine the amounts of insurance to purchase for each of these types (if any--many large corporations and most governments are self-insuring). On a periodic basis or when major changes or purchases of equipment are made, the steps in Table 6 must be repeated to ensure that the organization is not under or over covered.

TABLE 6

STEPS REQUIRED TO DETERMINE AMOUNTS
OF INSURANCE COVERAGES

1. Make a formal threat analysis.

2. Eliminate from further consideration those threats adequately countered by the environment, the facility, and the security procedures.

3. Prepare a worst-case disaster scenario covering the remaining risks.

4. For each scenario, prepare a contingency plan which would keep the facility in operation.

5. For each step in the contingency plan, make sure elapsed time and dollar expense have been estimated.

6. Summarize the costs for all contingency plans and post the totals, as appropriate, to the types of insurance mentioned above (e.g., to equipment and facilities, media, business interruptions, etc.).

7. Review the coverage and the exclusions prior to going into final negotiations with the insurance agent.

8. If the quoted premium seems excessive, arrange for an on-site field inspection with technical representatives of the insurance company to determine what can be done to change the system, procedures, or facilities to reduce the risk and bring the premium in line.

Source: [Ref. 16:p. 87]

d. Contracting Management

Top management must ensure that contracting personnel are well-trained in computer technology and terminology. They must have a thorough understanding of security safeguards, the need to have them designed into new systems, and other particular security-related problems associated

with software development and purchases of hardware, supplies and services.

e. Control Implementation Strategy

An important issue for top management to consider in developing a security program is the manner in which the controls should be implemented. To ensure that controls are not installed haphazardly, that they are not overly restrictive, and that they are the most cost-effective for the risk at hand, a strategy for implementation of controls should be employed. [Ref. 15:pp. 9-11] Robert H. Courtney, in a document prepared for the Federal Information Processing Standards Task Group 15, detailed the steps that should be included in such a strategy. These steps include:

1. Perform a security risk analysis.
2. Consider all security measures (controls) available.
3. Select the control that minimizes the risk at minimum cost.
4. Implement the control measure that is deemed most feasible.
5. Evaluate its effectiveness and actual cost.
6. Restart the process. [Ref. 22]

It is important to mention that, generally, top management will not be the actual implementor of this strategy. Its task is to ensure that a strategy is derived and employed. Security personnel, working with EDP management, will follow the strategy in implementing most of the computer security controls within the framework of the

overall security program. A further discussion of this process follows in the next section.

D. SUMMARY

It is extremely important that top management gets directly involved in the formulation of the overall security programs. This is true for several reasons. First, the overall program serves as the framework in which the whole security effort must function. Also security controls will not be popularly accepted without high-level support. Finally, because they are expensive in direct and indirect costs and must be tailored to each specific organizational setting, top management will, of necessity, be required to provide input and resources. Regardless of the circumstances, there are certain elements that must be made part of all security programs. These include clearly stated objectives and guidance, a carefully written security charter, and several other key elements normally found in good overall security programs.

V. TOP MANAGEMENT CONTROLS

A. INTRODUCTION

After top management has ensured that an overall security program has been implemented as a framework within which specific security controls may function, it then must take steps to ensure that appropriate control mechanisms are selected and employed. It does this by selecting and implementing its own measures and by ensuring that lower level managers follow suit. The controls implemented within the organization will, therefore, range from the relatively broad-based and non-technical measures of top management to the very specific and technical controls initiated by the managers of the lower-level control layers described by Ron Weber's model.

This section covers the security controls needed to protect an organization's computer assets. It describes how the Department of Justice and the National Bureau of Standards approached the task of identifying security controls that are needed at each organizational level. Then, it describes the specific controls that should be initiated at the top management level. First, however, the discussion briefly focuses on how security controls at various organizational levels function interdependently to

provide an adequate security "blanket" against computer abuse.

B. INTERDEPENDENCE OF SECURITY CONTROLS

As mentioned, top management's controls are general, broad-based, and non-technical. Their purpose is mostly to tackle major problems that affect the whole organization and to provide direction and guidance to managers at subordinate levels. In this latter sense, top management controls are nothing more than a very closely related extension of the overall security program: they extend the framework within which the subordinate level controls must operate.

The part that top management's controls play in extending the security framework is crucial to the appropriate functioning of the security effort. They assist subordinate managers in determining the appropriate security emphasis and controls needed at their levels and ensure that all the controls are coordinated and integrated in a manner that will eliminate "holes" from the layers of Weber's security "onion" (otherwise his "onion" would be more analogous to a layered ball of swiss cheese!). By ensuring that each successive layer of controls is properly interleaved, top management can, in effect, form a relatively impervious, protective seal around the organization's sensitive information systems. Also, by carefully selecting their control mechanisms, top managers can allow subordinates the greatest possible latitude in selecting and installing their more

specific controls and, thus, lessen the perceived impact of all controls on subordinate operations. The key to success seems to be in identifying the appropriate top managerial controls and in implementing them in the least restrictive manner possible consistent with the security needs of the organization.

C. PROCESS OF IDENTIFYING THE APPROPRIATE CONTROLS

There has been much research into which controls are most effective at securing a computer system while leaving it, operationally, the most unfettered. Much of the research has been conducted by two agencies of the federal government, the U.S. Department of Justice (DOJ) and the U.S. National Bureau of Standards (NBS). As seen below, although the agencies took quite different approaches to identify the needed controls, their findings were remarkably similar.

The approach taken by DOJ was to exhaustively search through dozens of organizations that employ computer systems to identify the security control measures, based on common usage and prudent management, that are so widely employed that they could be considered absolutely essential to the security of any computer system under normal circumstances. The Department's idea is that, if such a set of controls could be developed, it could serve as a baseline of control measures which could assist all computer organizations in

effecting and maintaining at least a minimally acceptable information system's security posture. [Ref. 23]

The DOJ does not purport its baseline concept as an alternative to quantitative and qualitative risk assessment methods, but it does believe that there are many benefits of a baseline of controls. For example, accepting industry standard and time-tested controls would save organizations much time, money, and effort that they would otherwise expend on researching already resolved problems. Also, management could be relatively content knowing that the firm's computer assets were safeguarded at least up to the baseline level by generally used controls. [Ref. 23:pp. 36-38]

However, as DOJ attempted to identify baseline security measures, it found that no such commonly employed set of controls exists. Instead, the Department found dozens of controls, each usually recommended by one or two users but:

> . . . not necessarily supported by widespread use. The Systems Auditability and Control Reports from the Institute of Internal Auditors identifies 300 controls and a set of control objectives based on a survey of 1,500 computer-using enterprises. However, one conclusion of these 1977 reports was a significant lack of common usage. Only a few organizations were found to be using any particular control. [Ref. 23:p. 37]

Every computer organization has traditionally viewed its situation as unique and has derived its security-related controls completely independently of other organizations, even those with similar functions. The result is that a plethora of controls and security postures, of varying forms

and degrees of effectiveness, exists throughout the industry. Because of the dearth of industry-wide commonality, DOJ narrowed the scope of its search to only a few organizations that dealt with highly sensitive personal data and managed to identify 82 separate controls for different organizational levels and functions, including eight baseline controls that should be "management initiated."

The National Bureau of Standards' approach to identifying essential security controls was different, even though its objectives and expected benefits were basically the same. The NBS attempted to identify a set of security controls by having independent research organizations, expert in computer crime, study actual criminal cases to identify the control measures that would have been necessary to prevent or detect the illegal activity. The NBS study identified 88 total controls, with only three listed as falling under the purview of "general management." [Ref. 15:pp. 11, 12, 20]

D. SPECIFIC TOP MANAGERIAL CONTROLS

In the subsections that follow, specific top management controls needed to ensure the protection of sensitive computer assets are discussed, starting with those of DOJ and NBS. Then, other top managerial controls, as gleaned from pertinent literature, are considered. In essence, this section describes the DOJ and NBS skeletal frame-work of top management-initiated controls. It then "fleshes out" that

framework by providing additional controls needed to manage the inherent dishonesty, negative motivational forces, and available opportunities that might cause/allow an otherwise good employee to become an amateur computer criminal. The controls that are discussed are listed in the following table (Table 7).

TABLE 7

TOP MANAGEMENT CONTROLS

DOJ:
- Computer Security Officer
- Computer Security Management Committee
- Cooperation of Computer Security Officers
- Keeping Security Reports Confidential
- Data Classification
- Financial Loss Contingency and Recovery Funding
- Separation and Accountability of EDP Functions/ Duties

NBS:
- Adjustment/Correction Reporting
- Job Rotation
- Disaster Avoidance

Other:
- Guidelines for Ethical Decisionmaking
- Standards of Conduct
  * Gratuities
  * Moonlighting
  * Organizational Property
  * Nonuse/nondisclosure
  * Substance Abuse
  * Gambling
- Employee Assistance Program
- "Whistle Blower" Policy
- EDP Auditor

1. Top Management Initiated Controls (DOJ)

The Department of Justice suggests the following controls be initiated.

a. Computer Security Officer

The first of DOJ's eight top management-initiated controls is the "Computer Security Officer." It is described in DOJ's pamphlet, Computer Security Techniques, as follows:

> An organization with sufficient computer security resources should have an individual identified as a computer security officer. In small organizations, the individual appointed may share this responsibility with other duties. In large organizations, one or more full-time employees should be assigned computer security administration responsibilities. The computer security officer should ideally report to the protection or security department covering the entire organization. This provides proper scope of responsibility for information and its movement throughout the organization. For practical purposes the computer security officer often functions within the computer department. Job descriptions are highly variable; examples may be obtained from many organizations with established computer security officers. [Ref. 23:p. 4-9]

The objective of this control is to prevent inadequacy of system controls. Its main strength is that the security officer provides a focus for the formal development of a computer security program. Also, depending upon his or her hierarchical placement within the organization, top management's degree of support for the security effort may be conveyed to the entire firm. Working through the security officer, top management can ensure an effective security program without having to "micro manage" the effort. The two main weaknesses of the control are its relatively high cost and the fact that line managers may attempt to transfer their responsibility for security to the computer security officer. [Ref. 23:p. 4-9]

A job description for the computer security officer should include, but not be limited to, the following duties:

(1) Represent the EDP Organization. The security officer will function on behalf of the EDP manager as the point of contact for all aspects of EDP security. His or her position must be separated from the primary EDP operations so that it can remain totally objective.

(2) Suspend EDP Operations. The security officer must cause total or partial suspension of operations (depending on the situation) upon detection of any activity which will affect the security of the operations. The suspension will remain in effect until removed by the EDP manager. The security officer must be given written authorization to suspend access to any system subscriber.

(3) Provide Written Directives. The security officer will prepare, distribute, and maintain plans, instructions, guidance, and/or standard operating procedures concerning the security of automated operations. He or she must also conduct periodic surveys to determine compliance with written standards.

(4) Conduct Risk Assessment. The security officer must review threats and formally assess risks of vulnerabilities so that effective countermeasures may be employed.

(5) Provide for Physical Security. The security officer should periodically conduct physical security surveys to ensure that computer assets are safe and secure in their physical setting.

(6) Conduct Reviews and Evaluations. The security officer should review and evaluate the security impact of system changes, including interfaces with other automated systems.

(7) Provide for Training. The security officer should coordinate and monitor periodic security indoctrination and training sessions for all employees.

(8) Advise Higher-Level Managers. The security officer should stay abreast of state-of-the-art security practices and technology and advise higher-level management of cost-effective improvements in the security posture.

(9) Review Reports. The security officer should conduct, from a security viewpoint, a daily review of audit trail and system management or user access reports.

(10) Control System Access. The security officer will issue and control physical access authorization of personnel with a demonstrated requirement to enter the activity or site (including users, contractors, and maintenance personnel). This also includes the management and issuance of system passwords.

(11) Retain Review Authority. The security officer should retain the capability to audit or review

every file within the system without obtaining prior permission from the file owner. [Ref. 21:p. 4]

b. Computer Security Management Committee

The second DOJ control, "Computer Security Management Committee," is described as follows:

> A high-level management committee is organized to develop security policy and oversee all security of information handling activities. The committee is made up of management representatives from each of the parts of the organization concerned with information processing. The committee is responsible for coordinating computer security, reviewing the state of security, ensuring the visibility of management's support of computer security throughout the organization, approving computer security reviews, receiving and accepting computer security review reports, and ensuring proper control interfaces among organization functions. It should act in some respects similar to a Board of Director's Audit Committee. Computer security reviews and recommendations for major controls should be made to, and approved by, this committee. The committee ensures that privacy and security are part of the overall information handling plan. The Steering Committee may be part of a larger activity within an organization to carry out the function of information resource management. For example, in one research and development organization an oversight council made up of representatives from organizations that send and receive data bases from the R&D organization was established. They are charged with oversight responsibilities for the conduct and control of the R&D organization relative to the exchange of data bases. Especially important are questions of individual privacy concerning the content of the data bases. [Ref. 23:p. 4-9]

The objective of this support is also to prevent loss of support for the security effort. In fact, the steering committee's major strength is that it visibly shows the dedication and support of top management for maintaining an acceptable security posture. By mandating that membership must cross all organizational lines, the security activity will be more consistent across interfaces; better

attention will be paid to all information-processing-related functions; security can be considered within the context of other issues confronting the organization; and, policies and procedures can be more effectively enforced. Also, a committee approach can avoid the control of security by technologists who tend to be limited to technical solutions that may be more stimulating to them but more expensive and less effective to the organization. [Ref. 23:p. 4-3] Finally, this control can meet the requirements of the computer security policy and control function of the overall security program, discussed in the previous chapter.

c. Cooperation of Computer Security Officers

The third top management control of DOJ is "Cooperation of Computer Security Officers." It is described as follows:

> Maintaining an effective computer security function can be enhanced by exchange of information with computer security functions in other outside organizations. Local computer security organizations can be developed within a city, a part of a city, or regionally. Monthly or other periodic meetings of computer security officers can be held to exchange useful information and experience. A hotline communication capability can be established for exchange of information on an emergency basis to provide warning of possible mishaps or losses. It is important to limit the details of information exchanged to ensure that confidential controls information is not disseminated to unauthorized parties. [Ref. 23:p. 4-11]

This control is also an extension of the computer security officer control and has the objective of proactively strengthening the adequacy of system controls. By exchanging information with computer security officers of

other organizations, important knowledge and techniques may be gained in the most time- and cost-efficient basis possible. Also, security officers can strengthen their sense of professionalism by relating directly with others in their chosen career field. A weakness of this control is the danger inherent in too much information regarding an organization's security posture/problems becoming known to unauthorized persons. [Ref. 23:p. 4-11] However, that danger must be weighed against the positive aspects of sharing information.

d. Keeping Security Reports Confidential

The Justice Department's fourth management-initiated control, "Keeping Security Reports Confidential," is described as:

> Computer security requires the use and filing of numerous reports, including results of security reviews, audits, exception reports, documentation of loss incidence, documentation of controls, control installation and maintenance, and personnel information. These reports are extremely sensitive and should be protected to the same degree as the highest level of information classification within the organization. A clean desk policy should be maintained in the security and audit offices. All security documents should be physically locked in sturdy cabinets. Computer-readable files should be secured separately from other physically stored files and should have high-level access protection when stored in a computer. [Ref. 23:p. 4-10]

Although keeping security information under a high degree of protection makes the information difficult and time-consuming to use, it is nonetheless important to prevent taking, disclosure, or unauthorized use. It is also important because the security function must set the example

for the remainder of the organization by appropriately caring for confidential information. [Ref. 23:p. 4-10]

e. Data Classification

The fifth control, "Data Classification," is described as follows:

> Data may be classified at different security levels to produce cost savings and effectiveness of applying controls consistent with various levels of sensitivity of data. Some organizations maintain the same level of security for all data, believing that making exceptions is too costly. Other organizations may have only small amounts of data of a highly sensitive nature and find that applying special controls to the small amount of data is cost-effective. When data are classified, they may be identified in two or more levels, often referred to as general information, confidential information, secret information and other higher levels of classification named according to the functional use of the data, such as trade secret data, unreported financial performance, etc. [Ref. 23:p. 4-6]

The objective of this control is, obviously, to prevent compromise of sensitive data. By treating data security requirements differently, according to the data's sensitivity level, and allowing access only on a need-to-know basis, an organization can most easily ensure that data is provided adequate protection but also that needed data is most readily accessible for legitimate purposes. Thus, this control allows the most cost-efficient balance between security and productivity requirements. A special consideration should be the danger of over or under classifying data and the fact that classification can easily result in excessive data handling/processing complexity. [Ref. 23:p. 4-6] It is also important to point out that classification of

data in a hierarchical scheme and access to it on a need-to-know basis is extremely hard to implement in practice. The only organization that has been able to do this is the federal government, which achieves it only by a process of segregated computer systems.

f. Financial Loss Contingency and Recovery Funding

The sixth control that should be implemented by top management is "Financial Loss Contingency and Recovery Funding" and is described by DOJ as follows:

> Self-insured organizations, such as government agencies, should be assured of readily available emergency funds for contingencies and recovery. Specialized EDP insurance is available and should be considered when insurance covering other types of losses in a business may not apply. Financial risk protection should cover asset losses, business interruption, and extra expenses resulting from contingency recovery. Organizations not self-insured should bond all employees against fraud in high-risk areas of data processing activities. Blanket bonds will normally cover this activity. [Ref. 23:p. 4-5]

This top management control was also discussed by the National Bureau of Standards, but as an element that should be included in the overall security program. Regardless of its placement, the objective is to ensure that the organization can recover from a business interruption. The most cost-effective method of accomplishing this objective (for non-self-insuring organizations) is by gaining protection and sharing economic risks with other companies, i.e., through purchased insurance programs. However, insurance must not be allowed to become an alternative to good security discipline. [Ref. 23:p. 4-5]

g. Separation and Accountability of EDP Functions/Duties

"Separation and Accountability of EDP Functions/Duties," the seventh DOJ control, is described in this manner:

> Holding managers accountable for the security in the areas they manage requires that these areas be clearly and explicitly defied so that there is no overlap or gaps in managerial control of EDP functions. EDP functions should be broken down into as many discrete self-contained activities as is practical and cost-effective under the circumstances. Besides being a good general management principle to maintain high performance, it also provides the necessary explicit structure for assignment of controls, responsibility for them, accountability and a means of measuring the completeness and consistency of meeting all vulnerabilities adequately. Separate, well-defined EDP functions also facilitate the separation of duties among managers, as is required in separation of duties of employees. This reduces the level of trust needed for each manager. The functions of authorization, custody of assets, and accountability should be separated to the extent possible. [Ref. 23:p. 4-1]

This control is designed to prevent loss of support for the security effort and reduce the possibility of accidental or intentional acts resulting in losses. It forces the need for collusion among individuals who may attempt unauthorized activities. It enhances efficiency in EDP functions and inhibits the loss of control from migrating from one function to another. However, increased complexity of EDP functions could result from excessive separation of functions, making the application of individual controls more difficult. Also, small shops may not have adequate numbers of employees to support extensive separation of duties. [Ref. 23:p. 4-1]

Krauss and MacGahan expound upon the importance of this control, saying that it cannot be overemphasized. They believe that no single individual should have responsibility for the complete processing of any single or group of transactions. Further, there should be no way that a person could make an error or abusive act without being detected by some other person during the routine execution of that other person's responsibilities. Forcing dishonest employees to collude serves as a deterrence and prevention measure and increases the likelihood of detection, since the greater number of people involved means that mistakes are more probable and the presence of a particular person needed to perform a required manipulation is less likely as the conspirators' numbers increase. [Ref. 12:pp. 80-81]

h. EDP Auditor

The eighth and final control measure that DOJ suggests top management of any organization should employ as a security measure to protect its computer assets is the "EDP Auditor." Since the EDP auditing function is one of the most important controls and because it is used as a feedback mechanism to top management on the effectiveness of the other measures, discussion of it will be held until all other top management controls have been considered.

2. Top Management Initiated Controls (NBS)

The discussion will now turn to the three control measures that the National Bureau of Standards identified as

worthy of top management initiation. These include the following factors.

a. Adjustment/Correction Reporting

The first, "Adjustment/Correction Reporting," is described by NBS as:

> Policy, procedures, and software to provide reports of adjustment/correction transactions covering the sphere of influence for each manager. For example, any modification, updates, deletions, or other changes to the payroll master file should be reported regularly to the manager of payroll systems for his information and action. [Ref. 15:p. 82]

This control is actually an extension of the "Separation and Accountability of EDP Functions/Duties" control described by DOJ. It is important because error corrections and adjustment transactions are initiated in reaction to existing problems and are often not subjected to appropriate and adequate control procedures. Such situations provide an opportunity for the dishonest employee to perpetrate fraud by preparing and submitting improper or fictitious transactions. If not controlled, such fraudulent transactions may never be detected. [Ref. 12:p. 106]

b. Job Rotation

The second of NBS's top management controls, "Job Rotation," is described as:

> Policy and procedures to periodically rotate those positions that have a great deal of authority among individuals in the data handling process. For example, the position responsible for address changes should be assumed by new persons periodically and without notice. The new person's first responsibility would be to verify the integrity of the file. [Ref. 15:p. 82]

The reason that unannounced duty rotations should be standard procedure is that the practice serves as a deterrence to abuse and to collusion. If a person is aware that he or she, without notice, is likely to be asked to switch jobs, he or she will be less inclined to begin to fraudulently manipulate the system, because the fruits of the manipulation will often remain for long periods and be discovered by the replacement. Also, other individuals will be less likely to collude, because they know that job rotations mean that still other people must be brought into the scheme and, hence, the collusion becomes expanded and more risky. [Ref. 12:p. 123] Anytime that an individual resists rotating from a sensitive computer position, foul play should be suspected until the person's reason for resistance can be checked out.

c. Disaster Avoidance

The third of NBS's three management-initiated security controls, "Disaster Avoidance," deals mostly with ensuring that the physical plant is protected. It is described as:

> Policy that facilities, both central and remote, are to be designed and constructed (or modified) so as to provide maximum protection against natural disasters and against persons intent on destroying physical or intellectual property. [Ref. 15:p. 83]

Physical security measures are generally beyond the scope of this paper. However, some aspects of this control do pertain to protecting a computer system against

internal abuse. These include designating certain areas, such as the computer room, data library, and software development areas, as "off limits" to unauthorized personnel; eliminating non-essential doors and controlling access to those considered essential; utilization of identification badges; and enforcing visitor controls. While much of these measures clearly falls within the controlling province of EDP management and below, general policies and guidelines that classify and/or specify expectations of top management are not out of order.

3. Other Top Management Initiated Controls

In addition to the eleven controls discussed above, there are others that are important for top management to initiate in order to complete the computer security framework. Several of these are discussed in the following paragraphs. Because different organizations will require the implementation of different top managerial controls and because there are literally dozens of such controls from which to choose, the following discussion does not attempt to cover all the possibilities. Rather, it covers the additional top management controls that appear most widely addressed in the literature, that are appropriate to safeguard the assets of most computer organizations, and/or that seem especially pertinent to a computer system's environment. These controls include the following features.

a. Guidelines for Ethical Decisionmaking

The first of these controls is called "Guidelines for Ethical Decisionmaking." This control is necessary to counter the four rationalizations that may persist in all organizations and cause employees to act unethically. It must be designed to address the following situation, as stated by Gellerman:

> How can managers avoid crossing a line that is seldom precise? Unfortunately, most know that they have overstepped it only when they have gone too far. They have no reliable guidelines about what will be overlooked or tolerated or what will be condemned or attacked. [Ref. 13:pp. 88-89]

The solution to this situation is for top management to establish specific and unquestionable guidelines for ethical behavior. The line between proper and improper conduct must be made exactingly precise by stating clearly the bounds within which decisions must be made. When employees must operate in murky borderlands, top management is obligated to force them to trust in and employ the most reliable guideline of all: when in doubt, don't--especially until the legality of the situation can be clarified. [Ref. 13:p. 89]

Also, senior executives are responsible to draw the line between loyalty to the company and action against the laws and values of society in which the company must operate. Further, because the line may become obscured in the "heat of the moment," it must be drawn well short of where reasonable men and women could begin to suspect that

their rights have been violated (and especially well short of the point at which a prosecutor might consider an indictment is warranted). Finally, and most importantly, top managers must stress that excuses of company loyalty will not be accepted for criminal or unethical behavior. They must make it clear that employees who harm other people, even allegedly for the company's benefit, will be fired. [Ref. 13:p. 90]

b. Standards of Conduct

The next top management control to be discussed is "Standards of Conduct." Because this control mechanism is very important to the security effort, it is considered in some detail. In Chapter III, the discussion on ethics mentioned that establishing a code of ethics can greatly assist top executives in managing the security effort. It can, too, and a strong ethical environment, as stated, is absolutely essential if the computer assets are to be secure. However, top managers would not only be naive but also big losers if they believed that a code of ethics or strong sense of ethics would be sufficient to protect their computer system:

> One of the most troubling aspects of the . . . case is the company's admission that those involved were thoroughly familiar with the company's ethical standards before the incident took place. This suggests that the practice of declaring codes of ethics and teaching them to managers is not enough to deter unethical conduct. Something stronger is needed. [Ref. 13:p. 90]

That "something stronger" is a Standards of Conduct, which is significantly different from a Code of Ethics. The code deals more with normative issues. It explains that which "should be" versus that which "is." Ethical codes are based on trust and derive their strength by appealing to one's sense of professionalism and moral obligations to do that which is right.

Standards of Conduct, on the other hand, deal more straightforwardly with the reality of the workplace. As seen in the description of the "enemy," employees (even normally honest ones) do sometimes face situations that may cause them to look beyond ethical means for solutions. Properly designed Standards of Conduct will not only specifically proscribe certain behaviors but will also cause tempted workers to think long and hard before committing themselves to abusive acts, i.e., the standards serve as a strong deterrent as well as a preventive control.

In order for Standards of Conduct to serve these dual purposes, they must possess something that Codes of Ethics normally lack: "teeth." This means that Standards of Conduct must have built-in enforcement mechanisms. If an employee violates a standard, he or she should be disciplined commensurate with the seriousness of the violation. The measures taken may range from simple "wrist slapping" to dismissal and should always include criminal prosecution if warranted. Further, the discipline should be administered

according to the "hot stove" rule, as described by Stephen Robbins: it should be immediate, consistent, and impersonal. [Ref. 24] Also, especially important for a computer systems environment, news of the situation and the disciplinary action taken should be widely disseminated as a deterrence to others and to counter the notion, mentioned by William Starfire, that computer crime is safe crime.

Inherent in the discussion of enforcement of Standards of Conduct are two other issues that are worthy of note. First, the standards will only be as effective as they are made to be. Often companies will specify formalized, written standards, but then they do little to review for compliance. However, unless the standards are closely monitored to ensure compliance, they will be useless. This policy compliance feedback mechanism must be designed into the system and checked closely by internal and external auditors.

Second, employees must be well versed in the specific details of the standards. This is crucial if the standards are to be enforceable. Many organizations require that all newly assigned or newly hired personnel be trained in the Standards of Conduct soon after arrival. Thereafter, they must review the standards on a periodic basis (frequently annually). After training or reviewing, employees are required to sign a statement acknowledging that they understand and will comply with the provisions of the

standards. The signed acknowledgement has a strong deterrence value and clearly eliminates ignorance as an excuse for standards violations.

The "Standards of Conduct" control is actually an "umbrella" control under which top management can specify other more specialized or ad hoc controls that it sees are needed to manage high-potential problem areas or situations that may arise unexpectedly. There are many such controls that are at management's disposal. Some of these apply especially to a computer environment and should be included by top management in any published Standards of Conduct for an organization that employs electronic information systems. These include the following measures.

(1) Gratuities. The giving and receiving of gifts between customers and vendors, regardless of the stated reasons, are bribery if either party or both parties stand to benefit as a result of the "gift." Receiving or giving gifts as part of business operating procedures must be strictly prohibited. This control should also specifically address the receipt of gifts from business associates by family members of company employees.

(2) Moonlighting. "Moonlighting on the job," or engaging in secondary income activity while employed in a full-time position, costs American businesses a significant and growing portion of the estimated $160 billion spent each year on employees' deliberate waste of on-the-job time.

There are four compelling reasons why moonlighting should be curtailed from an EDP environment: it causes reduced performance; encourages unauthorized use of resources; represents potential conflicts of interest; and affects employee morale. [Ref. 26]

Even if circumstances do not allow moonlighting to be totally prohibited, it should be publicly discouraged and strictly controlled. If the second job appears to interfere with the employee's on-the-job performance, or if it is such that conflicts of interest are likely, then permission to moonlight should be denied. It is especially important in a computer systems environment that workers who deal with sensitive assets or functions not be allowed to perform similar functions in other organizations. This is because of the natural tendency to illegally transfer proprietary information/assets away from the parent organization (in effect, to pirate them for use on the second job).

While moonlighting on the job is insidious to an organization, moonlighting per se may not be. It is thus important that every organization derive a moonlighting policy and guidelines that are appropriate for its particular circumstances. According to Jeffrey Davidson, however, all firms must include in their guidelines statements that:

1. Spell out the conditions under which top management will approve, disapprove or be neutral toward moonlighting (e.g., it may applaud teaching at local

colleges or lending skills to government service but "frown upon" working for a competitor).

2. Classify whether in-house telephones, secretaries, copy machines, or computers can be used for outside purposes.

3. Leave no doubt in anyone's mind concerning expected job performance and steps that will be taken if moonlighting causes performance to decline. [Ref. 25]

(3) Organizational Property. Organizational property should only be used in the direct pursuit of legitimate, organizational business. Guidelines to clarify this fact are especially important to a firm operating a computer system because ownership of property is frequently not clear. The individual developer of a piece of software, for example, may feel that the final product is really personal property, vice organizational, because he/she perhaps spent many off-duty hours in completing it. The laws governing such cases are not always clear, and many cases are decided in court. To prohibit any misunderstandings, top management must specify, in terms that cannot be misconstrued, that property which comprises organizational assets. As much as possible, such assets should be marked as organizational property. Also, it is wise that top management issue a policy that all fruits of all employees' work-related efforts will be considered company-owned property. This will put the obligation to prove individual ownership on the shoulders of those who claim otherwise and will cause questionable cases to be decided individually.

(4) Nonuse/Nondisclosure. All computer personnel and all employees who possess and use confidential information and trade secrets or those who may find themselves in a position in which conflicts of interest may arise should be required to read a policy explaining legitimate use and disclosure of the company's valuable informational assets. The statement should explain specifically that confidential information can be used only in the context of one's immediate, legitimate job-related activities. As a condition of employment, employees should be required to sign a statement acknowledging their understanding of the policy and their agreement to comply with it. [Ref. 12:p. 65]

(5) Substance Abuse. The use of illegal drugs or the abuse of prescribed drugs and/or alcohol must be proscribed from the workplace. Also, substance abuse away from the job that affects on-the-job performance/behavior must be strictly controlled. While managerial controls should only focus on those activities that are job-related, it is important to note that substance abuse has frequently been found to be a root cause of identified computer systems abuse. Thus, those individuals who are suspected of abusing drugs should be considered unreliable and denied access to sensitive information and processes until their reliability can be reestablished. In this regard, the employment of

urinalysis testing is becoming much more widespread and should be considered as a control and verification tool.

(6) Gambling. Any form of gambling should be strictly prohibited from occurring on organizational property. Also, individuals who are known to be heavily involved in gambling should be monitored closely and, in some cases, offered counselling services. If knowledge of indebtedness also surfaces, they should be removed from having access to sensitive, valuable assets until the matter is resolved.

c. Employee Assistance Program

The "Employee Assistance Program" is another top management control that should be employed to help safeguard sensitive computer systems. Of all the controls discussed so far, the Employee Assistance Program (EAP) is potentially one of the most rewarding, because it will be viewed most favorably by employees and offers the opportunity to deter computer abuse and provide more stability, productivity and higher morale in the workplace, all at the same time. It is a proactive, pro-worker measure that has been gaining in popularity in businesses across the country as they attempt to combat theft and high rates of absenteeism and turnover. Today, 60% of the Fortune 500 companies employ some form of internal or external EAP. They are finding it less expensive and more beneficial to get their employees help them to "lose" them. [Ref. 26]

Employee Assistance Programs help workers by providing them with counselling for everything from domestic problems to drug abuse [Ref. 27] They are especially effective in EDP organizations, because they offer a place for troubled workers to seek help for that "unshareable problem" that often causes them to turn to illegal means for solutions. The EAP can also counter the extremely high levels of stress that are inherent in EDP positions, as well as "burnout," disgruntlement, and substance abuse that can lead employees into amateur crime.

d. "Whistle Blower" Policy

Another top management control for ensuring the security of a computer system against internal threats is the "Whistle Blower Policy." Whistle blowing can be an outstanding weapon for top management to use in battling computer abuse, but it must be employed properly. As Stoner says, the practice is often discouraged because it ". . . usually embarrasses management and can be done with impunity only when the whistle blower is leaving the organization voluntarily." [Ref. 17:p. 69]

However, this does not have to be the case. If top management is proactively employing the security program and controls already discussed in this paper, instances of whistle blowing should be rare and can be viewed not as an embarrassment but as a sign that the security effort is working properly. As part of their management of the

ethical environment, if top management were to encourage whistle blowing and guarantee in words and deed that the whistle blower would be protected against reprisal, then the practice would gain in popular acceptance and would be a viable deterrence against abuse (this assumes, of course, that top management is viewed as trustworthy in its own right).

Deterring abuse in government by changing the "flavor" of whistle blowing is the motive behind a bill that is currently pending before the Senate (it has already been passed by the House of Representatives). The bill is designed to remove the stigma that may be associated with whistle blowing and to promote the practice by assuring a "firm and swift investigation" into allegations and by providing protection for the whistle blower against possible reprisal. According to the sponsor of the bill, whistle blowers are patriots, not troublemakers, and they should be treated as such. [Ref. 28] By viewing and treating whistle blowing in the same positive manner prescribed by the pending legislation, any organization would undoubtedly reap large benefits not only in the form of detecting crimes but also in deterring abusive behavior.

e. EDP Auditor

The final top management control that will be discussed as a tool for securing a sensitive computer system is the "EDP Auditor." As mentioned earlier, this control

was identified by the Department of Justice as one that should be initiated by top management. It ". . . can be one of the most effective countermeasures a company has in its total system of safeguards to prevent, detect, and deter computer [abuse]." [Ref. 12:p. 222] It is also one of the singular most important top management controls because it is implemented with the specific intent of overseeing all the other security countermeasures. A detailed discussion of this control would require a book and is beyond the scope of this paper. However, there are two important aspects of EDP auditing that are particularly worthy of top managerial consideration.

First, it is very important for top management to realize that for EDP auditing to be effective it will require large doses of the highest level support. This is true for at least two reasons. These include the fact that EDP auditing has received a tremendous amount of criticism in the past and that EDP auditing is extremely time and resource consuming and will be seen as an especially vibrant albatross to organizational progress.

According to Krause and MacGahan, EDP auditing has been heavily criticized by more than a few experts in the EDP security field. These experts contend that EDP auditors lack the necessary training and tools to do an adequate job, especially in the area of identifying on-going computer fraud. This criticism appears not to be without

merit. [Ref. 12:p. 222] The significance for top management is that it must take steps to ensure that the organization's internal auditing section receives the training and tools necessary to make it proficient in auditing computer systems.

Making the EDP auditing function more palatable to an organization's processes is extremely important to the auditor's success and represents the second reason that top level support for the control is mandatory. Computer systems auditing basically serves two roles in an organization: a reactive role in which it checks or verifies the efficiency/effectiveness of other controls, the overall security program, and in fact of the computer system, itself; and, a proactive role in which it plays an active part in the design and implementation of individual EDP processes. This latter role is one that will not be favorably viewed by other elements of the business. Everything mentioned previously about the fettering of productive effort by security mechanisms seems magnified when one considers EDP auditing.

There is a vast difference between EDP auditing and traditional auditing--EDP auditing is newer and is generally considered a much more difficult process. While traditional auditing has physical records that establish traceable audit trails, the same is not true of EDP auditing. In many cases, the audit trails of EDP functions

disappear, literally, at the speed of light as the electronic pulses change or, perhaps, as the computer is turned off. In other words, there is inherently no physical, tangible record, in many cases, that can later be inspected or audited.

Thus, auditing process functions must be built right into other operational aspects of the system. This entails a lot of work and resources and generally compounds an already complex problem. For example, consider that adding functions to establish audit trails in an applications program may require hundreds of lines of code in addition to the hundreds that the software application itself may require. Plus, to be most effective at ensuring that the audit needs are met, the internal auditors should be actively involved in the design (especially early design) and should have authority to approve or disapprove many aspects of the system as it is developed. In such a situation, it is not hard to imagine the organizational problems that may exist as the system developers fight with the auditors over control of the developers' project. Without active support of top management, the required auditing features are likely to be dropped or amended, especially as time constraints begin to take their toll (as they generally do).

The second aspect of EDP auditing that is especially worthy of top managerial consideration is the

frequency with which the system should be audited. As Gellerman commented, "Simply increasing the frequency of audits and spot checks is a deterrent . . ." [Ref. 13:p. 90] However, increasing the frequency of audits is no simple matter, because audits are very expensive. Top management must, therefore, determine the most cost-effective approach to dealing with systems security problems. It may employ the reactive (yet cheaper) "big stick" method of resolving problems that are discovered, or it may employ the more expensive and more proactive technique of making frequent audits designed to deter crime from occurring in the first place. [Ref. 13:p. 90]

The final approach taken will likely consist of some balance between the two methods. Regardless, there are two ways in which top management can make its auditing control more effective. First it should not only increase the frequency of audits to the greatest extent that is economically feasible, but it should also schedule the audits irregularly, making at least half of them unannounced and setting up some checkups soon after others. Second, if the audits do detect a trespass, top management should announce the misconduct and the punitive actions taken. [Ref. 13:p. 90] Recall that the amateur computer criminal fears most unanticipated detection and public disclosure of his or her acts. By designing the auditing process so as to most

effectively exploit this fear, the control will realize its fullest deterrence potential.

VI. CONCLUSION

The enormous losses suffered by American organizations through computer abuse can be greatly reduced if a well-planned and coordinated security effort is employed. Ron Weber suggests that a common sense approach which breaks the security process down into seven separate levels of controls can greatly facilitate the effort. The controls range from the broad-based and nontechnical measures of the outer layers of Weber's security "onion" to the very technical and expensive controls employed at the inner layers. The inner layers of controls and, hence, the security effort itself, will only be as effective as the outer layers of controls.

This paper agrees with Weber's thinking and discusses his outermost layer of controls, those prescribed by top management of an organization. In essence, it describes those things that top management must consider and the things it must do in order to ensure the security of its sensitive information systems against internal abuse. It, first, provides a profile of the "enemy" against whom the computer system must be protected. Although there has been identified six different types of computer criminals, and each type, to some extent, poses a threat to organizations' computer assets, it was found that organizational employees constitute the greatest danger to computer systems. These

individuals, called amateur computer criminals, may be some of the business' best performers but, because they have some "unshareable" problem, they may turn to illegal acts for what appears to be the most expedient resolution.

The focus then turns to a discussion of how an ethical business environment is especially important to the security of computerized assets. Four rationalizations that cause managers to act unethically were presented. It was shown how allowing widespread employment of these rationalizations may be particularly detrimental in computer organizations because of the expanded size of the workforce in positions of trust. It was shown how and why top management must lead the way in overcoming the tendency to rationalize and to act unethically.

After top management has a firm grasp of the "enemy" and has instilled the appropriate ethical environment, it must then take an active role in the formulation of the overall security program for the organization. Top management's active participation in this process is vital for several reasons. Without its support, security control measures will not be accepted since they inherently stifle productive effort. Also, since security controls are expensive in both direct and indirect costs, top management must take an active role in determining the appropriate level of security necessary for the individual organization. Finally, the overall security program serves as the framework within

which all the other control mechanisms can and will function. Thus, the computer security effort will only be as good as the overall security program.

After top management has ensured the establishment of the appropriate overall security program, it then must prescribe its own more specific security controls and ensure that lower management levels of Weber's security "onion" do likewise. The controls necessary for top management initiation have, to a great extent, been provided by the Department of Justice and the National Bureau of Standards. They and others presented in Chapter V basically serve as an extension of the framework of the overall security program and may cover any situation that top management sees as needing special attention in the effort to secure the organization's information systems against internal abuse.

LIST OF REFERENCES

1. Parker, Donn B., Crime By Computer, p. 12, Charles Scribner's Sons, 1976.

2. Parker, Donn B., Fighting Computer Crime, p. 25, Charles Scribner's Sons, 1983.

3. Watt, Peggy, "Protecting Your Company's Data Base," San Jose Mercury News, p. 12F, 6 July 1986.

4. Telephone conversation between Dr. Jay BloomBecker, Director of the National Center for Computer Crime Data, Los Angeles, California and the author, 1 December 1986.

5. Starr, Barbara, "Are Data Bases a Threat to National Security?" Business Week, p. 29, 1 December 1986.

6. Sniffen, Michael J., "Reagan Orders Overhaul of Defenses Against Spies," Monterey Peninsula Herald, 1 December 1986.

7. Weber, Ron, EDP Auditing: Conceptual Foundations and Practice, p. 25, McGraw-Hill Book Company, 1982.

8. Range, Peter Ross, "The KGB's New Muscle," U.S. News & World Report, p. 27, 15 September 1986.

9. Lamb, John and Etheridge, James, "The Terror Target," Datamation, pp. 44-46, 1 February 1986.

10. Hampton, David, Summer, Charles and Webber, Ross, Organizational Behavior and the Practice of Management, 4th Edition, p. 106, Scott, Foresman and Company, 1982.

11. Starfire, Brian, "Computer Criminals Are Growing Older," San Jose Mercury News, p. 1F, 13 April 1986.

12. Krauss, Leonard and MacGahan, Aileen, Computer Fraud and Countermeasures, p. 27, Prentice-Hall, Inc., 1979.

13. Gellerman, Saul W., "Why 'Good' Managers Make Bad Ethical Choices," Harvard Business Review, p. 85, July-August 1976.

14. Weber, Austin, "Ethics, Conduct Standards Brand Real Professionals," Data Management, p. 12, May 1985.

15. Ruder, Brian, An Analysis of Computer Security Safeguards For Detecting and Preventing Intentional Computer Misuse, p. 9, National Bureau of Standards, 1978.

16. Browne, Peter, Security: Checklist For Computer Center Self-Audits, p. 3, American Federation of Information Processing Societies, 1979.

17. Stoner, J.A.F. and Wankel, Charles, Management, 3rd Edition, p. 179, Prentice-Hall, Inc., 1986.

18. Cash, James I., McFarlen, F. Warren and McKenney, James L., Corporate Information Systems Management: Text and Cases, p. 26, Richard D. Irwin, Inc., 1983.

19. Brown, William F., Greenlee, M. Blake and Jacobson, Robert, Computer and Software Security, p. 14, Advanced Management Research International, Inc., 1971.

20. Summers, R.C., "An Overview of Computer Security," IBM Systems Journal, pp. 309-310, 4 November 1984.

21. Army Regulation 380-380, Automation Security, p. 6, Department of the Army, 1985.

22. Orceyre, Michel J. and Courtney, Robert H. Considerations in the Selection of Security Measures For Automatic Data Processing Systems, p. iii, National Bureau of Standards, 1978.

23. Stanford Research Institute, Computer Security Techniques, p. 35, U.S. Department of Justice, 1982.

24. Robbins, Stephen P., Personnel: The Management of Human Resources, 2nd Edition, p. 398, Prentice-hall, Inc., 1982.

25. Davidson, Jeffrey P., "Curtail Moonlighting With Solid Guidelines, Performance Evaluations," Data Management, p. 26, January 1986.

26. Nolan, Maria, "Mutual Respect, Understanding Combat Substance Abuse," Data Management, p. 19, December 1985.

27. Nolan, Maria, "Employee Assistance Programs Ease Tension, Stress," Data Management, p. 18, November 1985.

28. Maze, Rick, "House OK's Protection for Military 'Whistle Blowers'," Army Times, p. 8, 18 August 1986.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Major Randal G. Tart USA Information Systems Software Development Center Fort Lee, Virginia 23801	4
4.	Dr. Carson K. Eoyang, Code 54Eg Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943-5000	5
5.	Dr. Norman R. Lyons, Code 54Lb Department of Administrative Sciences Naval Postgraduate School Monterey, California 93943-5000	1

Thesis
T162
c.1 Tart
Preventing internal
computer abuse.

Preventing internal computer abuse.