THE IMPACT OF ABUSES TO COMPUTER INFORMATION SYSTEMS ON MODERATE SIZED LAW ENFORCEMENT AGENCIES BY THE YEAR 2000.

By

WILLIAM C. LENTINI
ADMINISTRATIVE LIEUTENANT
BREA POLICE DEPARTMENT

ORDER NUMBER 10-0189

COMMAND COLLEGE - CLASS X

JUNE 1990

COMMISSION ON PEACE OFFICER STANDARDS AND TRAINING

SACRAMENTO, CALIFORNIA

THE IMPACT OF ABUSES TO COMPUTER INFORMATION SYSTEMS ON MODERATE SIZED LAW ENFORCEMENT AGENCIES BY THE YEAR 2000.

A study of the future impact that crimes committed with, or against law enforcement computer information systems will have on moderate sized municipal police agencies serving a population between 50,000 and 250,000. The study examines possible futures, identifies recommended policies, and defines an implementation process.

By

WIILIAM C. LENTINI

COMMAND COLLEGE CLASS X

COMMISSION ON PEACE OFFICER STANDARDS AND TRAINING

SACRAMENTO, CALIFORNIA

JUNE 1990

Order Number 10-0189

THE IMPACT OF ABUSES TO COMPUTER INFORMATION SYSTEMS ON MODERATE SIZED LAW ENFORCEMENT AGENCIES BY THE YEAR 2000.

By

WILLIAM C. LENTINI

COMMAND COLLEGE - CLASS X

PEACE OFFICER STANDARDS AND TRAINING (POST)

SACRAMENTO, CALIFORNIA

1990

The Impact of Abuses to Computer Information Systems on Moderate Sized Law Enforcement Agencies by the year 2000.

This Command College Independent Study Project is a FUTURES study of an issue of increasing importance to data contained in law enforcement computer information systems. While no predictions of the future are made, the forecasting of trends and events is used to project a number of scenarios and to develop a strategic plan.

This study examines information as it relates to the issue security to law enforcement computer information systems. Alternative plans and policies regarding security systems and training are discussed to allow planners to choose those that best fit the needs of their agencies.

The design of any futures study is to serve as a guide through an as yet uncharted territory. With a guide the planner can make those decisions necessary to successfully navigate past obstacles and to influence the outcome which will unfold in that uncertain place known as the future.

The Impact of Abuses to Computer Information Systems on Moderate Sized Law Enforcement Agencies by the Year 2000.

W.C. Lentini. Sponsoring Agency: California Commission on Peace Officer Standards and Training (POST).1990. 104 pp.
Availability: Commission on POST, Center for Leadership Development, 1601 Alhambra Blvd., Sacramento, CA 95816-7053.
Single copies free; Order number 10-0189.
National Institute of Justice/NCJRS Microfiche Program, Box 6000, Rockville, MD 20850.
Microfiche free. Microfiche number NCJ_____.

ABSTRACT

This study has three parts: a futures study of the impact of violations on a moderate sized law enforcement agency's computer information system by the year 2000; a model strategic plan for a municipal law enforcement agency serving a population of 50,000 to 250,000; and a transition management plan for a hypothetical city of moderate size. Five trends were forcaseted over the next ten years: technological advances, the availability of new security systems, security breaches of information networks will focus attention on computer security, increased reliance professional consultants, and demand for computer literate police officers will be acute. High probability events that could significantly impact law enforcement are: systems sabotaged by an employee, systems intrusion by organized crime, "virus" or rogue program infection to system, civil suit by person/s damaged by unprotected confidential information. A cross impact analysis was used to develop plan a strategic plan that includes specific policy recommendations. The transition management plan presents a feasible management structure.

THE IMPACT OF ABUSES TO COMPUTER INFORMATION SYSTEMS OF MODERATE SIZED LAW ENFORCEMENT AGENCIES BY THE YEAR 2000.

by

WILLIAM C. LENTINI

COMMAND COLLEGE CLASS X

PEACE OFFICER STANDARDS AND TRAINING (POST)

SACRAMENTO, CALIFORNIA

1990

EXECUTIVE SUMMARY

PART ONE - A FUTURES STUDY

The Age of Information: Although the ENIAC and the UNIVAC hardly resemble the modern computers of today, those warehouse sized machines were the forerunners of the personal computers which have become the cornerstone of the technological revolution society is currently experiencing.

SRI International, a consultanting firm to the U.S. government on computer security matters, cites incidents of computer abuse as early as the 1940s. Until the last few years the incidence of reported computer crime was low. An SRI study found only 669 incidents of computer abuse between 1958 and 1979. Since that time the number and scope of the intrusions into computer network systems has risen dramatically.

Impact on Law Enforcement Agencies by the Year 2000. A Modified Conventional Delphi Panel was used to identify the five key trends that strongly affected the study: (1) demand for computer literate law enforcement officers, (2) new security systems, (3) rapid technological advances, (4) reliance on outside professional consultants, and (5) attention focused on computer security. Five possible events are considered to be the most critical: (1) employee sabotage, (2) "virus" or rogue program infection to system, (3) systems intrusion by organized crime, (4) a crime committed with information gained by tapping into law enforcement computer information systems, (5) a civil suit brought by a subject on whom confidential information was kept by law enforcement but not adequately protected from unauthorized users of the information system.

PART TWO - STRATEGIC PLANNING

Organizational Analysis: A medium sized California police agency was selected as a model to examine for its strengths, weaknesses, and its capability to accept change.
Policies: A modified policy delphi panel was used to select the policies determined to be most feasible and desirable.

1. Conduct background investigations on all employees with computer access.
2. Train all personnel with computer access regarding proper computer security procedures.
3. Back-up all records on a daily basis.
4. Utilize the expertise of outside computer security consultants to recommend both hardware devices and security software programs.
5. Personal identifiers will be enhanced with retina identification, voice print, palm geometrics and other biometric devices.
6. Highly sensitive material will be encrypted.

Implementation Strategy: Key stakeholders and their positions relative to the proposed policies were analyzed. Negotiation strategies were developed according to the perceived most effective approach.

PART THREE - TRANSITION MANAGEMENT PLAN

Policy Implementation: Members of the critical mass were identified and evaluated in terms of their level of commitment, responsibility and readiness for policy change.
Transition Management: A project manager and task force were selected to ensure implementation of the strategic plan.

RECOMMENDATION

Law enforcement officials can act now to develop policies and procedures to deal with the present and future problem of computer security. In the future it will be less costly to purchase and maintain secure computer systems than to defend civil law suits from failure to implement a computer security system.

ACKNOWLEDGMENTS

I would like to thank the following people without whose help and encouragement the rigors of completing this Command College project would have been decidedly less bearable.

My children, Kelley and Kory Lentini, for all their encouragement.

Donald L. Forkus, Chief of Police, Brea, California, for his support and encouragement for me to attend Command College.

City managers Ed Wholenberg, Frank Benest and Art Simonian, for their support of my pursuit of the Command College learning experience.

Dr. Russell Hunter, my advisor for his tireless work.

TABLE OF CONTENTS

ILLUSTRATIONS

TABLES

FIGURES

CHARTS

PROJECT BACKGROUND

INTRODUCTION

Noted author and futurist, Edward Cornish, in his Global Solutions;Selections from the Futurist, makes the point that..."tomorrow's crisis may well be today's minor problem overlooked" (1). Since no major incidents of intrusions into a law enforcement computer information system have been publicized it may appear that such violations are minor. There is growing concern among computer security specialist that law enforcement computer systems will experience increasing levels of improper or illegal intrusions.

The purpose of this study is to examine the ~~the~~ current practices of computer security within the law enforcement community in order to identify weaknesses and develop strategies to alleviate these problems. By evaluating the trends and events as they will impact the issue, considering the possible scenarios which will await the future, and designing a plan of action, a course can be charted to steer agencies clear of the approaching dangers.

THE INFORMATION REVOLUTION

In 1943 Thomas J. Watson, then Chairman of I.B.M., stated "I think there is a world market for about five computers"(2). At this far removed time it seems a grossly humorous statement to make, especially given the name and identity of the speaker. One must remember, however, that in 1943, the only available computer was the "Univac" computer that required a small warehouse to contain the massive bulk of its considerable, vacuum-tube driven electronic components.

As late as the early 1970's, indeed, before the revolution in micro-chip processing, only "mainframe" computers existed. Such computers were maintained only in major universities and similar large organizations. These computers required banks of memory chips and tape drives larger than the average reel-to-reel audio tapes of the day. In-put was done on IBM punched cards.

By the late 1980's "desk top" models provided the memory previously available only in mainframe computers. During the past decade, the price of these models decreased sharply. By 1991 it is estimated that there will be one computer for every 50 persons in the United States, many of them in private homes rather than in businesses (3).

The invention of the modem, a device enabling computers to communicate with each other, has intensified this revolution in data processing both for individuals and organizations.

THE PROLIFERATION OF THE PERSONAL COMPUTER

As early as 1982, Future Scan, a publication of Security Pacific Bank's research division, stated that..."by 1990, companies will routinely provide terminals for employees to work at home" (4). Indeed, this prediction is nearing fruition. It is estimated that by the year 2000 about half of all service workers will be involved in collecting, synthesizing, analyzing, structuring, storing, or retrieving information. Half of these people will be working at home. With nearly one computer for every 50 people in the United States, computers are already becoming a pervasive part of American life (5).

LAW ENFORCEMENT'S RESPONSE TO THE EMERGING TECHNOLOGY

Law enforcement, as a public service industry, was at first slow to respond to the potential uses of computer technology. Many of today's criminologist believe that laws and law enforcement often lag far behind the innovative techniques of criminals in exploiting technological change. Once these technologies were harnessed for use in police work, it was predictable that law enforcement would soon succumb to the temptation to purge the system of the "old ways" of gathering, storing, and retrieving information. Herein lies a potential danger to law enforcement of monumental proportions. Some law enforcement executives have become so infatuated with this new found resource that they tend to think of it as a panacea for their

informational needs. They must be constantly reminded that computers and the attending software are tools, nothing more and nothing less. Like any tool they can be misused, broken or even stolen. Lest one become so smug as to think that such a fate could not or would not befall such a noble profession as law enforcement, one need only to look at a few recent examples of the potential havoc which awaits the law enforcement profession should it fail to take steps to protect the computer information systems it has.

PUBLIC ATTENTION FOCUSED ON COMPUTER SECURITY ISSUES

On December 3, 1988 a still unidentified hacker broke into the Pentagon's Milnet system which links hundreds of defense firms and government research centers. The perpetrator used "mail bridges" to gain access to the system and mask his/her tracks. The raid focused attention on the broad problem of computer security and the weakness of the electronic network that thousands of civilian and defense researchers use to exchange information and ideas. Less than a month earlier Robert Morris, a Cornell graduate student, launched a rogue "virus" program that jammed approximately 6,000 computers on the ARPA net, another Pentagon communications system.

WARNING TO GOVERNMENT COMPUTER INFORMATION SYSTEMS

If such intrusions into the national defense systems can so easily be made, how long will it be until the

criminal element make routine intrusions into law enforcement networks if this is not already occurring? The penetration of computer records and files could be of vast service to organized crime. A criminal past could instantly be eradicated, sensitive information about individuals could be retrieved for illicit purposes, or the names, addresses, and telephone numbers of an entire police department could be retrieved by an enterprising criminal computer hacker.

It is easy to understand why law enforcement has become so enamored with this new technology. The sheer speed with which record checks on individuals can be made is appealing enough in itself to justify police interest in computer information systems. An example of the benefits of applied computer technology is seen in figure 1. which graphically illustrates the time savings in inquiries made to Interpol from 1986 until 1989 (6). This impressive time savings is an example of why law enforcement is now rushing to embrace computer technology.

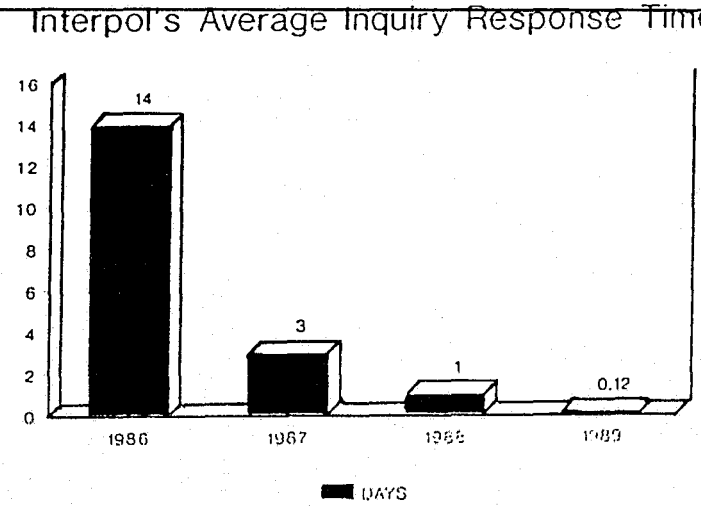


FIGURE 1

and revenge, yet industry budget figures indicate that the major expenditure for information systems protection is spent on prevention of damage due to fire, flood and earthquakes (7).

User's Perceived Security Threats

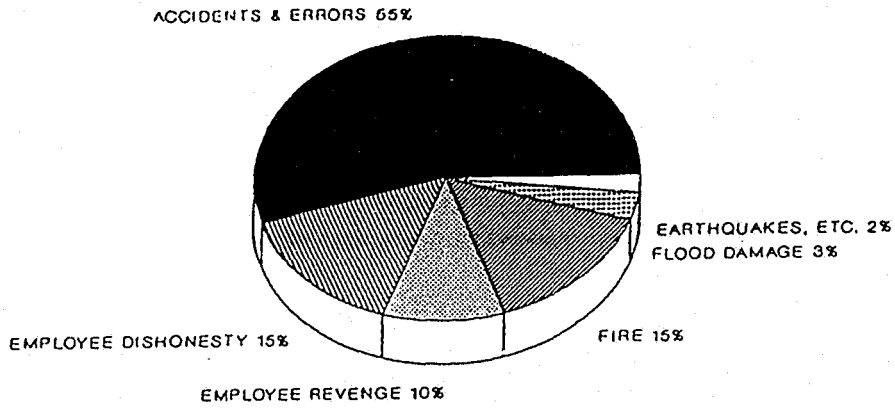


FIGURE 2

With simple back-up practices such risks can be virtually eliminated. The threat from a disgruntled employee or an outside hacker poses a potentially greater danger simply because little is being done to protect information systems from such wrongful intrusions.

Computers are commonplace in law enforcement today. What is not commonplace is a well thought-out plan to protect law enforcement from the potential abuses of such information-processing tools.

OBJECTIVE I:

DEFINING THE FUTURE

OBJECTIVE I

ISSUE STATEMENT

The first objective of this research project was to study the available data and analyze the primary issue using generally accepted methodologies. This endeavor yielded data upon which three futures scenarios were based. The information was obtained through a literature scan, personal interviews, on site visits to fourteen different law enforcement computer information centers, discussions with a broad range of professional in the field of computer technology and the use of a Modified Conventional Delphi Panel.

The primary issue of this project is: The impact of abuses to computer information systems of moderate sized law enforcement agencies by the year 2000. While much of what is discussed in this project has application to small and very large police departments alike, the scope of the study was purposely limited. Very small departments have very limited resources (for the most part), and large departments have computer problems of a grander scale, therefore the topic area was confined to moderate sized

municipal police agencies (those serving a population between 50,000 and 250,000). With this in mind an evaluation of related past, current, and future sub-issues was conducted to properly focus the study.

The related past issues were as follows:

1. What role did the increased competition for the budget dollar play in the lack of computer security devices for law enforcement information systems?

2. How has the limited computer expertise among law enforcement officials contributed to the present state of inadequate security for police computer information systems?

3. What has been the impact of the lack of planning for the new technology on law enforcement agencies?

4. Traditionally law enforcement lags behind in the application of technology, how has this impacted the issue of computer security?

The scanning process indicates that these prior issues are still relevant today which indicates that they are largely unresolved. Clearly some of the past issues are beyond the scope of law enforcements ability to have much impact on such as the availability of money from property taxes. However, these issues affect law enforcement nonetheless and therefore must be addressed to minimize their effect. The identified current sub-issues are:

1. How has the rapid proliferation of computers affected law enforcement computer information systems security?

2. What impact is the lack of current security measures beginning to have on law enforcement?

3. How will law enforcement cope with the lack of technical expertise in the field of computer security?

4. What portion of the budget dollar should be spent on computer security?

Related sub-issues which have future importance are:

1. How will law enforcement fill the need for computer literate police officers by the year 2000?

2. What role will outside professional consultants play in law enforcement agencies of the future?

3. What new technologies are on the horizon for law enforcement that may impact the area of computer information systems security?

4. What impact will state and federal legislation have on the subject of computer security?

5. How much security is enough?

METHODS: IDENTIFICATION

The following techniques and methods were used to gather, develop, sort, assimilate and evaluate information pertaining to the primary issue:

1. Scanning of a large volume of literature such as books, periodicals, journals, newspapers, industry pamphlets, corporate newsletters and video presentations.

2. Personal and telephonic interviews with subject matter experts.

3. Attendance at computer security seminar.

4. Site visits to fourteen Los Angeles, Orange, and San Diego County law enforcement computer centers.

5. Use of the Modified Conventional Delphi Panel. This technique was chosen because many of the experts in the field have restrictive time schedules and are extremely difficult to get together. For this reason the Modified Conventional Delphi Panel was the desired technique. The group was composed of university instructors, police executive managers, computer programmers, computer analysts, corporate computer experts, a city administrator and a member of the U. S. Treasury Department.

6. Three separate scenarios were written using the information obtained by the aforementioned methodology.

METHODS: IMPLEMENTATION

The research on this project began with a scanning of the available literature related to the primary issue. This proved to be somewhat sparse. While there is a great deal of information on the applications of computers in the workplace, little is written about the failures of business or governmental agencies to protect their data. Within the last several months this void has begun to fill with the release of information heretofore kept out of the public. Victims of such crimes are indeed reluctant to speak of it because it points to their vulnerability.

Although written texts on the subject of computer

security issues are often difficult to find, due to the occurrence of a few spectacular computer crimes, the public's attention has been focused on the issue. This focus has caused a surge in the application of computer technology to the area of data security.

Eighteen months after he unleashed a destructive "worm program" on the Internet network, disabling thousands of computers, Robert T. Morris Jr. was sentenced to three years probation, 400 hours of community work, and a $10,000 fine. Estimates of the cost of coping with the Internet worm ran from a few thousand dollars to $90 million. By and large law enforcement still gives computer crime a low priority. This may in part be due to the fact that we are inadequately prepared to deal with such cases and furthermore we are ill trained to even protect ourselves from such intrusions.

Despite new and rewritten laws addressing specific aspects of computer crime, such cases are likely to remain difficult to prosecute. If national defense systems can be so easily breached, how can law enforcement take the position that "it can't happen to us"? The history of law enforcement has been one of preaching and practicing physical security. What we now need to concentrate on is improving our approach to systems security.

The second method used to gather information was the personal interview and or telephonic contact with industry experts. In this manner the researcher became acquainted

with a large number of incidents involving computer security breaches to law enforcement information networks, many of which are still being investigated at this writing. It appears that industry experts are willing to discuss violations that they are not eager to make public. This intentional communication is having an effect on the computer security industry as illustrated by the estimate that companies using a computer security software program will grow from one percent in 1985 to fifty-three percent in 1991 (8).

The on-site visits to law enforcement agencies throughout the southern California area provided evidence of a lack in standard security practices. While some agencies were diligent about hardware security, their software was left virtually unprotected. Other agencies locked-up disks, used materials purchased from only reputable businesses, and made regular checks of their software yet had computer terminals in locations that were left unattended for entire weekends and vulnerable to clandestine use.

The scanning technique combined with structured interviews resulted in a list of trends and events that was sent to each member of the Modified Conventional Delphi Panel (Appendix A). The panel members evaluated the impact of each trend and event and were asked to rank order these items from one to five. From the original list of thirteen trends (Appendix B) and eleven events (Appendix C), a final selection of five trends and five events was made.

TREND SELECTION PROCESS

A trend is defined as a direction of movement, a general inclination or tendency. Through scanning research, thirteen trends were identified as bearing closer examination. These trends were sent to the Delphi participants. With this information five trends considered most important by the panel as a whole were chosen for use in the second round of the process.

In the second survey, the process was repeated and the remaining five trends were again ranked using the median value. The same process was done for selection of the events. After completing these tasks the panelists did a cross-impact analysis indicating the relationships between the trends and the events.

THE FIVE MOST RELEVANT TRENDS SELECTED

1. The need for law enforcement officers with higher educations, especially those who are computer literate, will be acute.

2. New and more advanced methods of providing security to

computer systems will continue to become available.

3. Technology will continue to advance at or greater than speeds currently experienced.

4. The need to seek technological assistance and consultations with the private sector professional will accelerate.

5. Increased incidents of breaches in computer information systems will continue to focus public attention on the issue of security.

TREND EVALUATIONS

A Trend Evaluation Table (next page) was used to record each major trend and the potential increase or decrease of each trend over time was recorded. The values recorded on this form represent the "median" values as discussed earlier. Note that the columns marked "5 years from now" and "10 years from now" are divided in two. The values listed in the upper-left portion of the boxes and marked with a single asterisk are representative of what the panel opined would happen in the "real" world. The values listed in the lower-right portion of the boxes and marked with two asterisks are representative of what the panel opined could happen in an "ideal" world. All trend levels have been assigned a value of 100 for the present.

TREND EVALUATION TABLE 1

TREND STATEMENT	LEVEL OF THE TREND (Ratio: Today = 100)			
	5 Years Ago	Today	5 Years From Now	10 Years From Now
1. THE NEED FOR LAW ENFORCEMENT OFFICERS WITH HIGHER EDUCATIONS, ESPECIALLY THOSE WHO ARE COMPUTER LITERATE, WILL BE ACUTE.	60	100	125* 150**	170* 200**
2. NEW AND MORE ADVANCED METHODS OF PROVIDING SECURITY TO COMPUTER SYSTEMS WILL CONTINUE TO BECOME AVAILABLE.	75	100	120* 140**	150* 180**
3. TECHNOLOGY WILL CONTINUE TO ADVANCE AT OR GREATER THAN SPEEDS CURRENTLY EXPERIENCED.	40	100	120* 150**	150* 180**
4. THE TREND TO SEEK TECHNOLOGICAL ASSISTANCE AND CONSULTATIONS WITH THE PRIVATE SECTOR PROFESSIONAL WILL ACCELERATE.	80	100	120* 130**	140* 150**
5. INCREASED INCIDENTS OF BREACHES IN COMPUTER INFORMATION SYSTEMS WILL CONTINUE TO FOCUS PUBLIC ATTENTION ON THE ISSUE OF SECURITY.	75	100	110* 100*	130* 90**

* Real World
** Perfect World

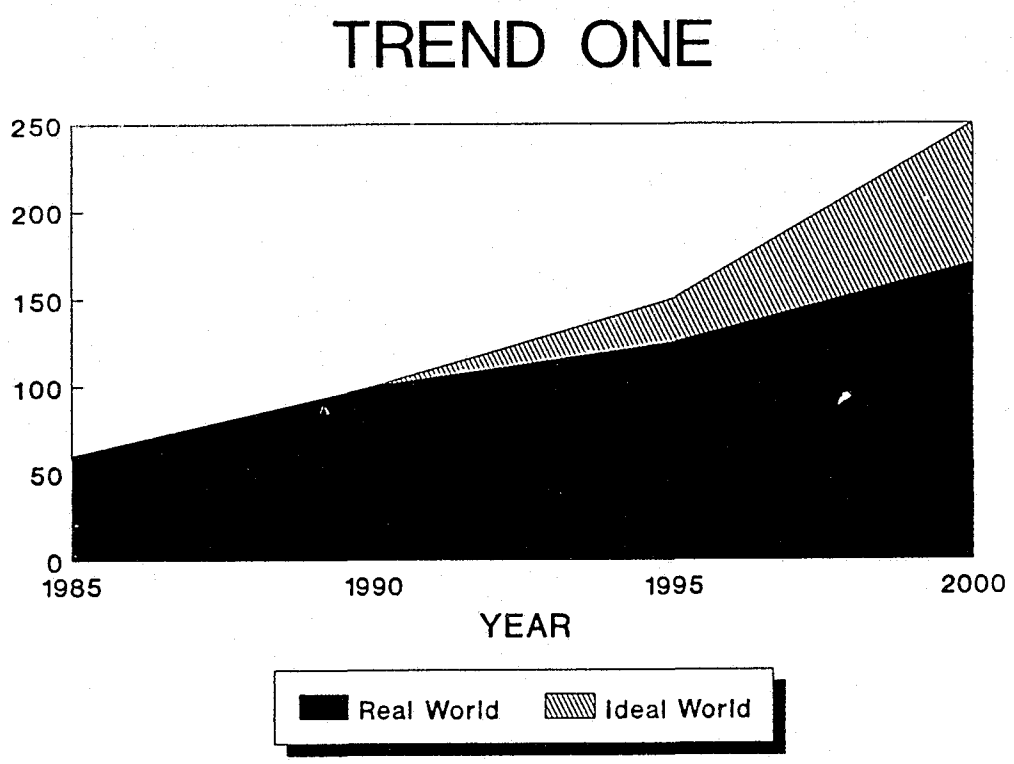


figure 3

The need for law enforcement officers with higher education, especially those who are computer literate will be acute.

Trend One Analysis. The security of law enforcement computer information systems will be an issue that needs to be addressed by all members of a policing agency as well as other municipal employees and vendors with access to the data base. The panel felt that the starting point of any security program should be with the ultimate users.

In most departments throughout this country, computer access is taken for granted. Many agencies have police units with on-board computer terminals that link them to a vast array of data networks.

The panel felt that the need five years ago was only

at value 60 by comparison to today's need for computer literate officers. In five years that value is expected to rise to 125 and in ten years it will continue to rise to a level of 170. The real world range (lowest and highest scores given) was 135 to 200.

In an ideal world, the panel felt that the five year hence figure would be an even greater value of 150. Ten years from now that value would rise to 250. This may, at first, seem extremely high. Remember that the panel was comprised of persons with specific expertise in the field of computer technology and law enforcement officials who are admittedly progressive. The range here was 150 to 250.

Ten years ago few agencies required a college degree for advancement through the ranks. A casual oberservation of trade journals and magazines seems to indicate that a college degree is necessary for promotions beyond entry level. It is therefore not unrealistic to suppose that computer literacy will be a prerequisite to employment as a law enforcement officer. Clearly, the competition for any suitable law enforcement candidates is an emerging issue for police executive managers today.

The issue was raised by several panel members that giving computer education to the entire department may increase the chance of unauthorized intrusions. However most agreed with the notion that the greater risk from this group was accidents or errors, and that education could help remedy that. This supports the findings of figure 2.

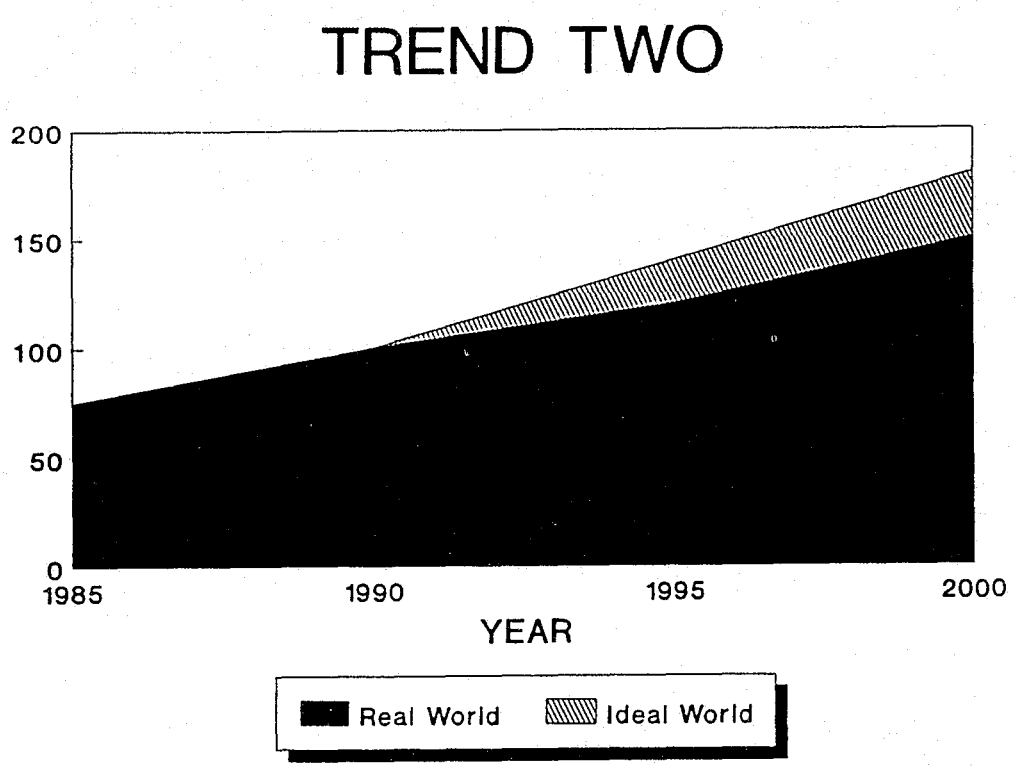


figure 4

New and more advanced methods of providing security to computer systems will continue to become available.

Trend Two Analysis. As figure 4 shows, the issue was seen as less important five years ago than it is today; the median value was 75. In the real world, the value increases to 120 five years from now and 150 ten years from now, with a range from 130 to 180. In an article in Information Week, J.J. "Buck" Bloombecker, Director of the National Center for Computer Crime Data, indicates that firms using computer security software will grow from 1 percent in 1985 to 53 percent by 1991 (9). This has, and will continue to spur technological advances.

In an ideal world, the value is set at 140 five years from now and 180 ten years hence. The range is 150 to 200.

TREND THREE

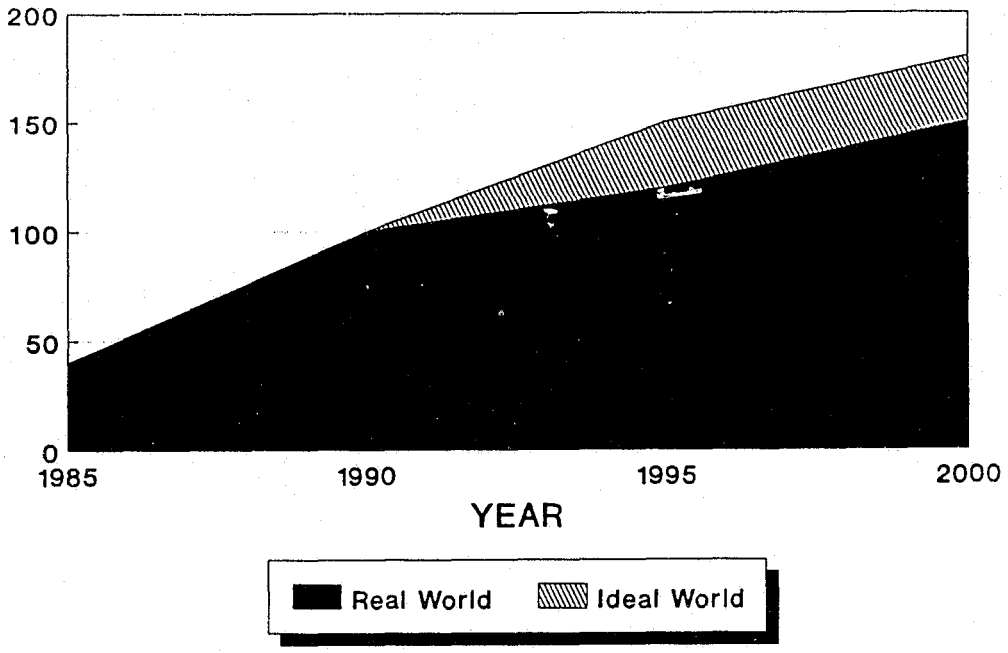


figure 5

Technology will continue to advance at or greater than speeds currently experienced.

Trend Three Analysis. As figure 5 shows, the median value placed on this trend five years ago was 40. The real world value five years from now was placed at 120, with a range of 110 to 200; ideal world five year future value was 150, with a range from 110 to 200. Ten years from now, the real world value was 150, with a range from 130 to 400, and the ideal world value was 180 with a range from 130 to 400.

The panel felt that this issue would be of increasing importance as the years pass. The spread is not extreme for most of the values save the last two. The top value of 400 was given by a panelist who consistently provided very high values. The next highest value of a panelist was 200.

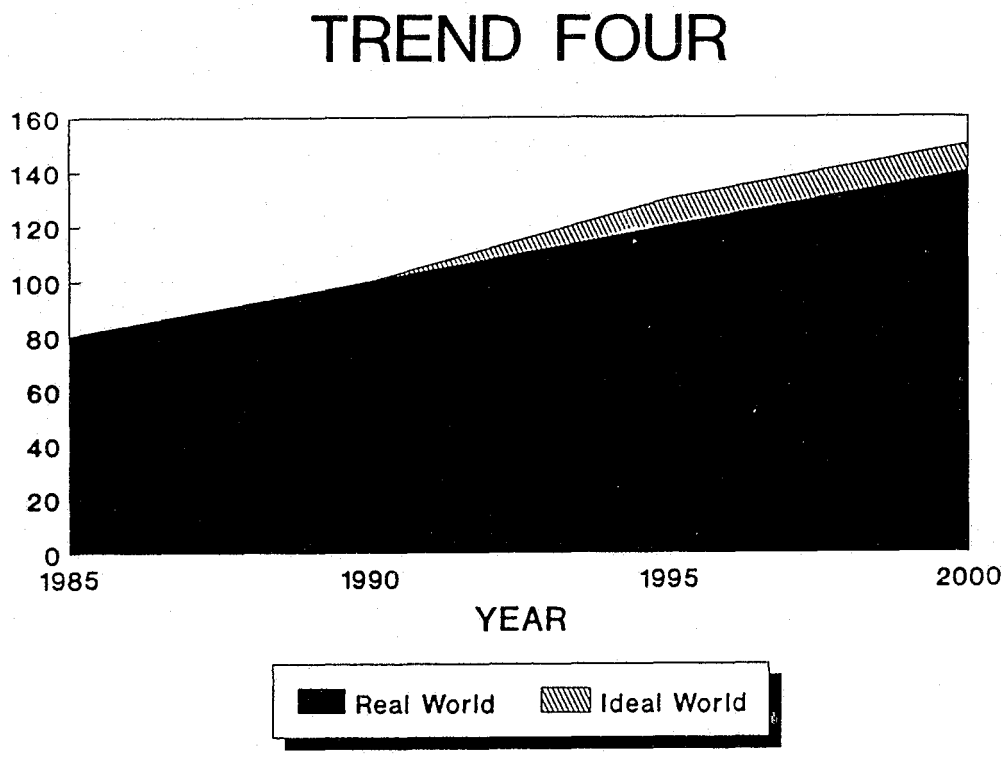


figure 6

The trend to seek technological assistance and consultations with the private sector professionals will accelerate.

Trend Four Analysis. Figure 6 shows that the median value five years ago was 80 with a range from 45 to 100. Five years from now in the real world, the value is 120, and ten years from now, 140. The range was 120 to 250.

In an ideal world, the five year value is 130 for five years hence, and 150 ten years from now with a range from 100 to 400. The high value again arises from the panelist mentioned earlier, the next lowest value was 300. It is noteworthy that the highest values were assigned to this issue by those in law enforcement. This may indicate a lack of expertise in this area and a need for outside help.

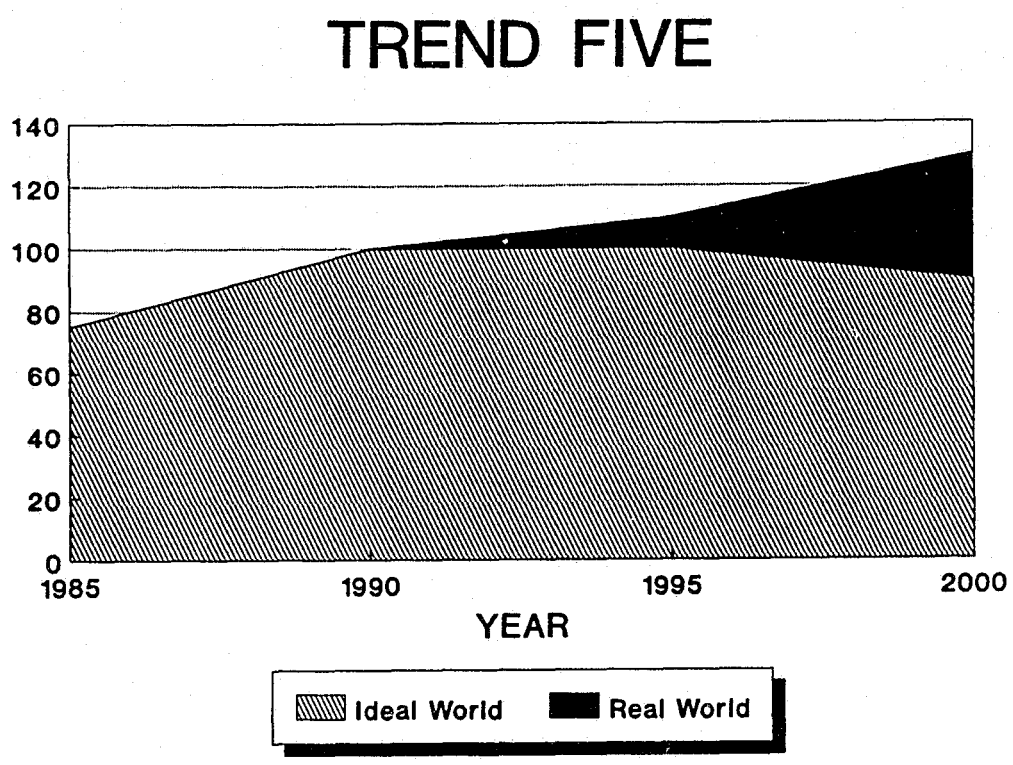


figure 7

Increased incidents of breaches in computer information systems will continue to focus public attention on the issue of security.

Trend Five Analysis. As figure 7 indicates, the median value placed on this trend by the panel was 75 five years ago with a range from 20 to 90. Five years from now in the real world, the value was placed at 110 and ten years from now 130, with a range from 40 to 200.

In the ideal world, the median value was set at 100 five years from now, and ten years from now at 90 with a range from 50 to 400. Once again, the extreme range was a function of the same panelist noted earlier; the next highest value was 150, which reduces the range considerably. This reflects the hope that future information users will contain the security problem.

In light of the literature of the day this seems highly unlikely to occur. All the signs point to the fact that the public's attention continues to be drawn to the issue of computer information systems security.

Society has grown-up reading novels such as George Orwell's 1984 and there is an inherent suspicion of "Big Brother". Most feel that it is difficult enough coping with the fact that the government has so much information readily available about its citizens, yet alone to have to worry about that "so called confidential information" slipping into the hands of others.

The panelist were unanimous in their conviction that the ideal world is not in sight or not realistic and that things will very likely get worse in the area of computer security before improvement is made.

The well publicized case of Robert Morris is not the only instance of unauthorized intrusion into a supposedly secured system nor was it the first. The 414 Group (named after the telephone area code for their home base of Milwaukee, Wisonsin) tapped into businesses, hospitals and government agencies before Morris was active (10). There are recent cases which are even more disturbing to law enforcement officials. In Arizona a group called "The Legion of Doom" brought down the 911 emergency codes by hacking into their systems. It would be naive to think that this problem will go away on its own.

EVENTS SELECTION PROCESS

An event, for the purposes of this study, is defined as an act which, when it occurs, will have an effect on the issues under consideration in this futures research. In the first round of the Delphi process the panelists were given eleven possible events previously identified in the scanning and interview process. These events were evaluated and returned to the researcher.

Utilizing the median scores, these events were narrowed to the five most important events as selected by the Delphi panel. After a second round of evaluation, the five remaining events were then ranked and a cross-impact analysis was done to determine the effect of these five events on the trends and vice versa. Those events are listed below:

THE FIVE MOST IMPORTANT EVENTS
AS SELECTED BY THE DELPHI PANEL

1. A displaced or disgruntled employee sabotages a law enforcement information system.
2. A system is designed which is masked by an innocuous looking program and when it is used in any computer it captures the passwords and identifiers which grant access to the user's computer. This information is then sent by mailbridge or modem to the program designers for their own clandestine use. (Note: for purposes of this study, the above described program shall be referred to as a "mole"

program because it acts much the same way a "deep cover" spy would in the world of espionage.

3. Organized crime puts a priority on obtaining information in law enforcement computer records systems.

4. Sensitive or confidential information is obtained by tapping into a police agency's computer system and this information is used to perpetrate a crime.

5. Confidential information is revealed when an unauthorized intrusion into police records is made on an unsecured (or poorly secured) system and this results in the subject named in that information bringing a successful negligence action against the agency.

EVENTS EVALUATION

The Delphi Panel members completed four tasks in relation to the critical events. The results are recorded on an "Events Evaluation Form" (next page). The evaluators were asked to select the first year that the probability of the event occurring exceeds zero and to give a "percent of probability" that the event would occur in the next five years (1995). The evaluators were then asked to repeat this estimate using a ten year time frame (2000). Finally the evaluators were ask "what impact on the issue the occurrence of this event would have". The ranges were listed as positive ten to negative ten. After this, a cross-impact analysis was completed.

EVENT EVALUATION TABLE 2

EVENT STATEMENT	(Ratio: Today = 100)			IMPACT ON THE ISSUE AREA IF THE EVENT OCCURED	
	Year that Probability First Exceeds Zero	5 Years From Now (0-100)	10 Years From Now (0-100)	Positive (0-10)	Negative (0-10)
1. DISPLACED OR DISGRUNTLED EMPLOYEE SABOTAGES A LAW ENFORCEMENT INFORMATION SYSTEM.	1990	70	100		8
2. A "MOLE" PROGRAM IS DESIGNED THAT SENDS CONFIDENTIAL INFORMATION FROM AN INFECTED INFORMATION SYSTEM TO THE "MOLE" PROGRAM DESIGNERS.	1992	25	65		8
3. ORGANIZED CRIME PUTS A PRIORITY ON OBTAINING INFORMATION CONTAINED IN LAW ENFORCEMENT COMPUTER RECORDS SYSTEMS.	1991	35	55		5
4. SENSITIVE OR CONFIDENTIAL INFORMATION IS OBTAINED BY TAPPING INTO A POLICE AGENCY'S COMPUTER SYSTEM AND THIS INFORMATION IS USED TO PERPETRATE A CRIME.	1991	40	55		5
5. CONFIDENTIAL INFORMATION IS REVEALED WHEN AN AUTHORIZED INTRUSION INTO POLICE RECORDS IS MADE RESULTING IN A LAW SUIT BY THE PERSON FOR NEGLIGENCE AGAINST THE POLICE DEPARTMENT.	1990	50	85		7

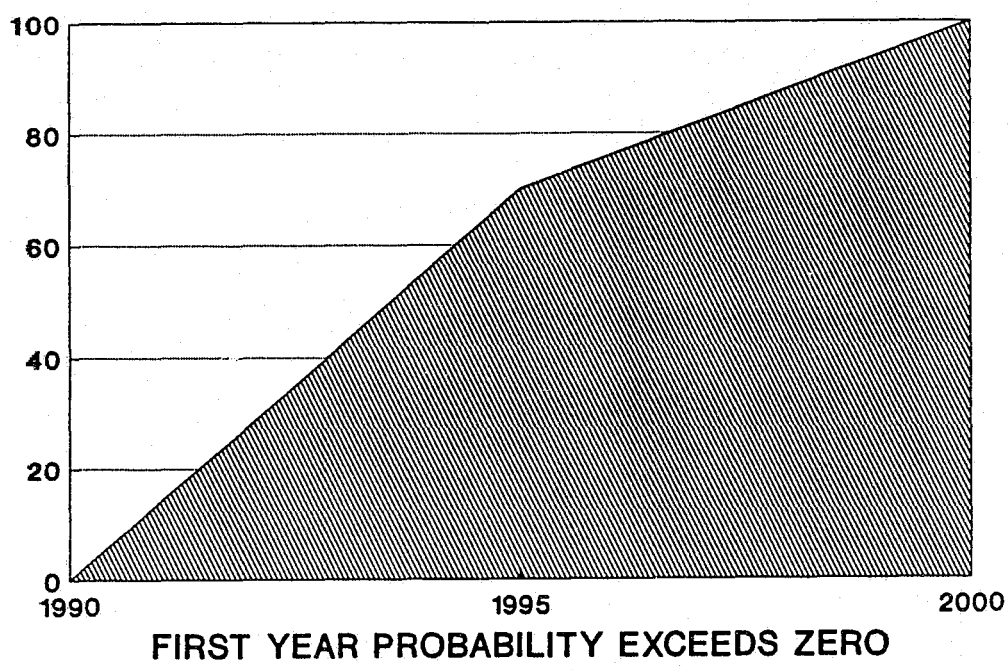


figure 8

A displaced or disgruntled employee sabotages a law enforcement information processing system.

Event One Analysis. The panel estimated that the year the probability of this event occurring first exceeds zero is 1990, with a range from 1990 to 1992. The probability of this occurring within five years was set at 70%, with a range from 60% to 90%. The panel felt that there was a 100% probability that this event would occur within the next ten years, with a range of 50% to 100%. One panel member set the impact at positive three, probably because it would force implementation of security systems. The rest of the panel set the impact at negative 8 with a range from -7 to -10.

EVENT TWO

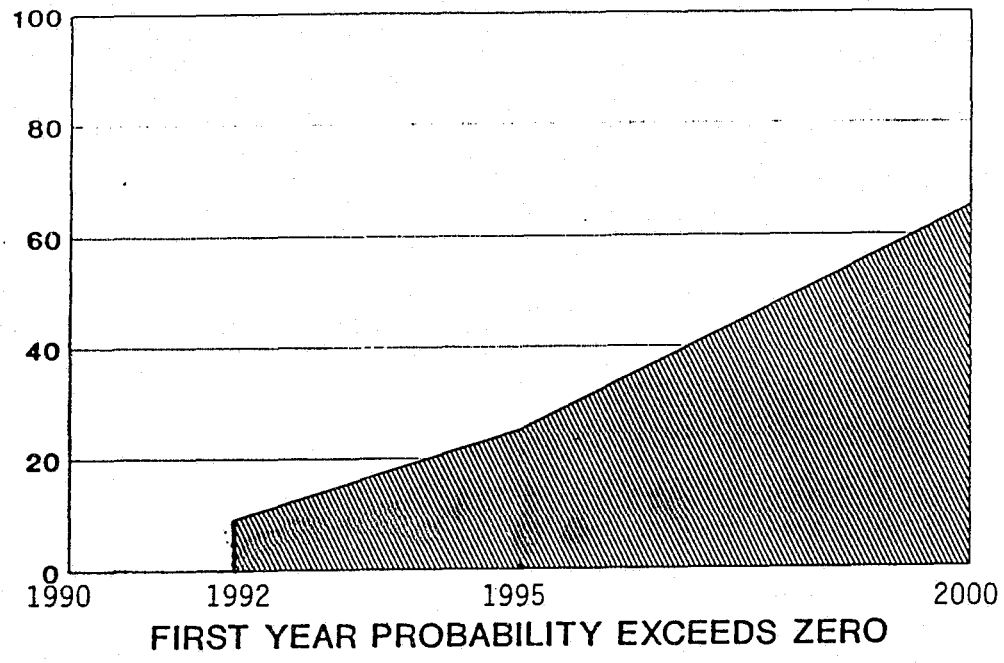


figure 9

A system is designed which is masked by an innocuous looking program, and when it is used in any computer, it captures the passwords and indentifiers of the user and sends this information to the system designer for clandestine use. (referred to as a "mole" program)

Event Two Analysis. This is called a "mask" or mole program since it acts like a deep cover spy and waits to send information to an unauthorized source. The year 1992 was the first year the probability of this event happening exceeded zero, with a range from 1990 to 1995. The probability five years hence was set at 25%, with a range from 25% to 100%. Ten years from now, the probability was set at 65%, with a range from 30% to 100%. The negative impact of is event was set at -8 with a range of -5 to -10.

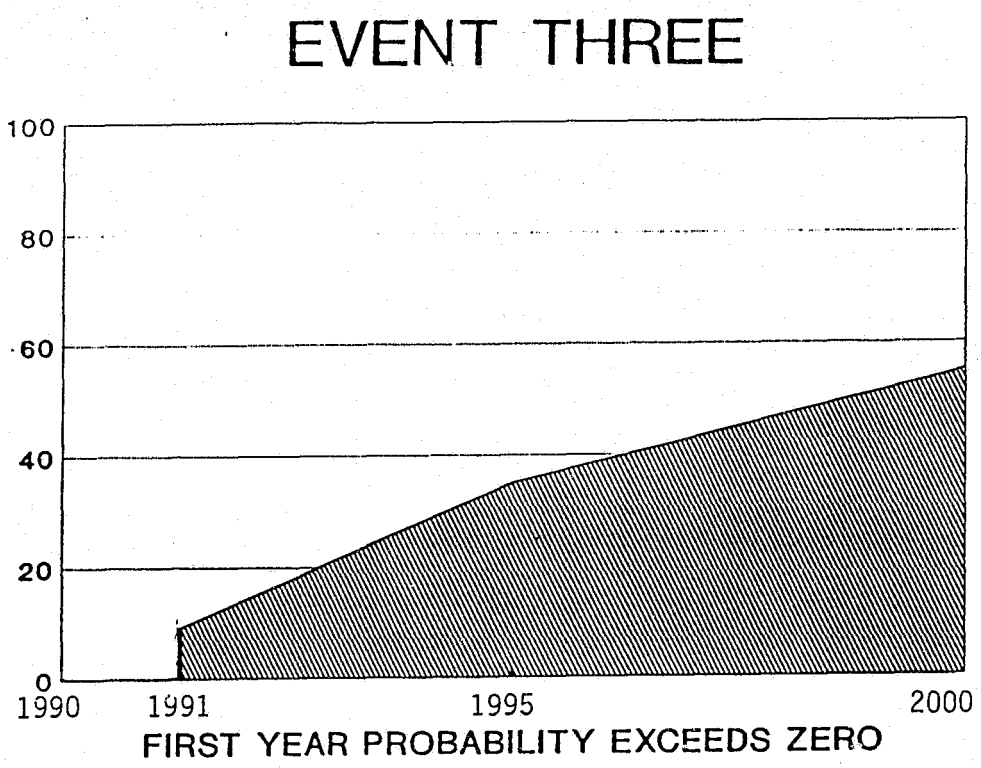


figure 10

Organized crime puts a priority on obtaining information contained in law enforcement computer record systems.

Event Three Analysis The year that the probability first exceeds zero was set as 1991, with a very narrow range, 1990-1992. The probability of occurring within five years was 35% with a range from 10% to 50%, and 55% within ten years, with a range from 50% to 100%. One panel member set a positive value at 9 for this event, probably because such an event would force the development of effective security systems. The balance set the negative impact at 5 with a range from -5 to -10. A few panelists expressed concern that there is a good probability that this type of intrusion is already occurring undetected. A number of cases were discussed which potentially fit this scenario.

EVENT FOUR

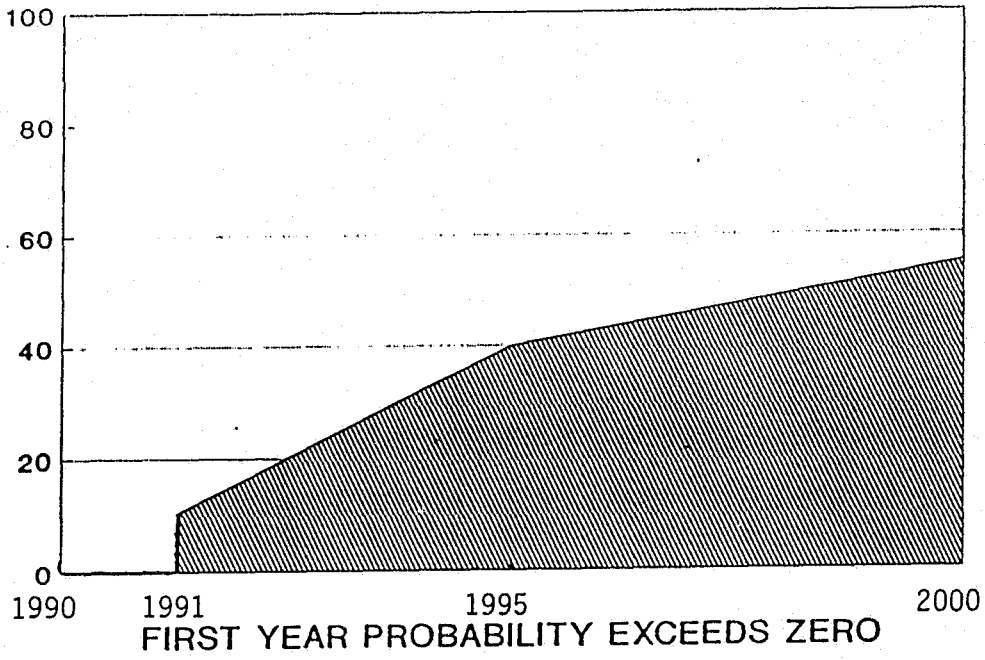


figure 11

Sensitive or confidential information is obtained by tapping into a police agency's computer system, and this information is used to perpetrate a crime.

Event Four Analysis. The panel set the year at 1991 when the probability of this event first exceeds zero with a range from 1990 to 2000. The probability was set at 40% within the next five years, with a range from 10% to 60%. By the end of ten years, it was set at 55%, with a range from 30% to 60%. One panel member set the positive impact of this event at 8, the balance of the panel set the impact at negative 5, with a range from -2 to -9. It should be pointed out here that all unauthorized uses of a law enforcement computer information system are violations, this particular event was defined to mean outside users.

EVENT FIVE

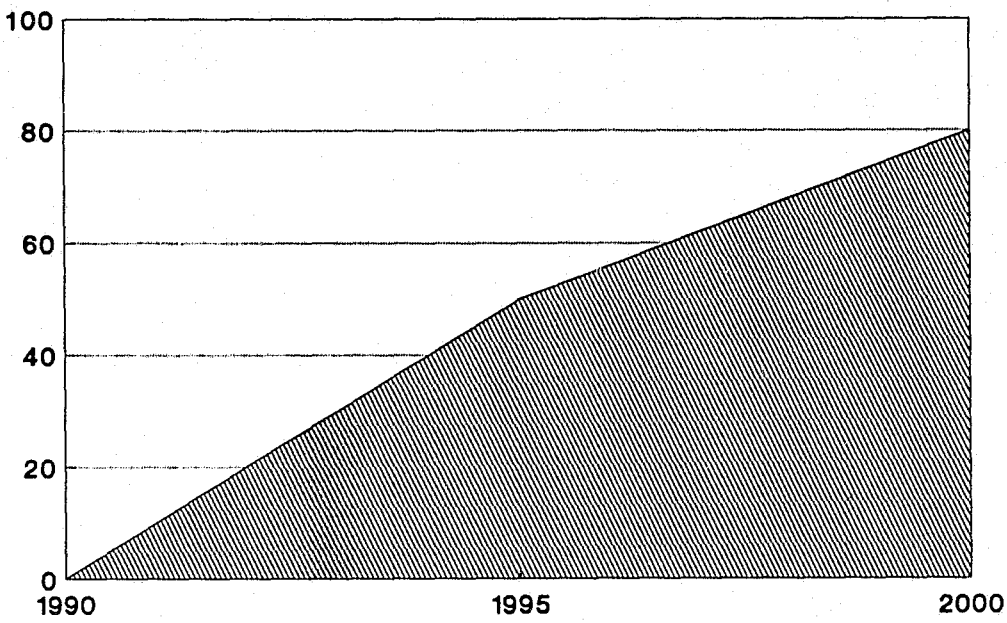


figure 12

Confidential information is revealed when an unauthorized intrusion into police records is made, resulting in a law suit by the subject of the information against the police department for negligence in not sufficiently securing the informations system.

Event Five Analysis. The median value set by the panel for the first year the probability exceeds zero was 1990, with a range of 1990-1995. The five year probability was set at 50%, with a range from 15% to 70%. Within the next ten years, it was set at 85%, with a range from 30% to 100%. Three panelists set the impact at an average of +9, with a range from 8 to 10, probably because it would force the introduction of better security systems. The balance set the impact at negative 7, with a range from -6 to -10.

THE CROSS-IMPACT ANALYSIS

The top-ranked five events and trends were subjected to a Cross-Impact Analysis to determine the relationship that existed between the events, and between the events and the trends. The results are shown on the Cross-Impact Evaluation Form (table 3).

Among events, all can be considered actors since each of them received either 7 or 8 "hits" out of a possible 9 on the combination of events and trends. With respect to events only, all received two, three, or four "hits" out of a possible five. Among trends, only trend no.3 failed to receive more than one "hit". All the others received 5, the maximum possible. Trend three was left in, because the delphi panel felt that the advance of technology has significant impact on the issue at hand. The following is a description of the effect that each of the events had on other events and on trends:

Event No. 1

This event involves revenge by a disgruntled employee and received seven "hits". There was no perceived effect on event no.2. It increased the probability of event no.3 by 75% since it provided the possibility of the introduction of a "mole" program. The probability of event no. 4 occurring was increased 100% because of the likelihood of dissemination of sensitive information. The

probability of event no. 5 was also increased 100% because a breach of confidence might well lead to a major law suit. Among trends, this event increased the probability of trend no. 1 by 40% because it highlights the need for more law enforcement officers with computer experience. It increased trend no.2's probability by 90% because of the need of more computer security. It had no effect on trend no. 3 because the advance of technology would not be effected. Event no.1 would increase the probability of trend no. 4 by 20% because this event would make it necessary for police departments to seek outside assistance for greater security. It would increase trend no. 5's probability because public attention would inevitably be focused more on the issue.

Event No. 2

This event involves a "mole" program, a program embedded in an innocuous program that has some other purpose. The "mole" program orders the system to provide information to an outside source. This event had 8 "hits". It had no effect on event no. 1, being more likely to be affected by that event. With respect to event no. 3, the probability is increased by 50% because it would provide organized crime with access to police computer systems. It would increase event no. 4's probability by 75% because it would lead to the dissemination of confidential information. It would increase the probability of event no. 5 by only 20% because not all releases of confidential

information might lead to a suit against a police department.

With respect to trends, it increased the probability of trend no. 1 by 50% because it would highlight the need for better knowledge of computer systems among police officers. It would increase trend no. 2 by about 90% because it would create the need for more technology. This is the only event that would affect this trend. Trend no. 4's probability would go up by 90% also, because of the need for greater technological assistance. This event increases trend no. 5's potential by a little less, 70%, since it would focus public attention on the matter.

Event No. 3

This involves organized crime's putting a priority on obtaining information contained in law enforcement computer systems. It produced 8 "hits". On event no. 1, it produced a 100% increase in the probability of occurrence since this could operate through the use of a disgruntled employee. It increased the probability of event no. 2 by 80% since it is likely that they (organized crime) would employ a rouge program. With respect to event no. 4, it would mean an increase of 70% because their incursion would likely result in one or more crimes being committed. Last, on event no. 5, the increase would be only 10% since their activities would not be likely to result in law suits since generally there is no public culpability for a criminal act committed by another.

With regards to trends, trend no.1 would be increased by 60% since, again, the need for computer expertise among police officers is highlighted. It would increase trend no. 2 by 90% since more security would be required to combat it. Trend no. 3 would not be affected. Trend no. 4 would increase by 75% because outside technology would be required to combat this event. It would increase trend no. 5 by only 20% since the public would not be likely to learn about it.

Event No. 4

This event involves the perpetration of a crime arising from the use of sensitive or confidential information. Event no. 4 received 8 "hits". It would increase the potential of event no.1 by only 10% since it is a step beyond that event. Event no. 2 would increase by 70% because it could involve a "mole" program. Event no. 3 would be increased by 80% because of no. 3's effect on organized crime's interest in the enterprise. Event no. 5 would go up 100% because the crime victims might well bring suit against the police department for its failure protect its own information.

The effect on trends indicate that trend no. 1 would be increased by 40% since it focuses on the need for computer literacy among police officers to prevent that kind of event. With respect to trend no. 2 the effect would be an increase by 50% because the crime would likely arouse public interest and outcry. It would have no affect

on trend no.3 since it would not have an impact on technology. The panel felt that this type of event would force law enforcement to give serious consideration to outside consultants therefore, trend no.4 was impacted by 50%. Trend no.5 was seen to be heavily impacted by event no.4. A rating of 80% was given by the panel.

Event No. 5

This event involves a suit against a police department because confidential or sensitive information was revealed. It received a total of 7 "hits". It would have no effect on event no. 1 because that event would likely have already occurred, and might well have produced event no. 5. It would decrease event no. 2 by 30% because it would shock the police department into providing greater security. Event no. 3 would also be decreased, this time by 50% because of the increase in security noted above. This logic produces a decrease of 70% for event no. 4 for the same reason.

Regarding trends, event no. 5 would effect trend no.1 by increasing it by 40% because of the need for computer literacy in police departments. Trend no.2 would increase by 75% because of the recognized need for increased security. Trend no. 3 would not be affected. Trend no. 4 would be increased by 60 % since outside assistance would be required to render the system more safe. Trend no. 5 would increase by 50% because of public outrage arising from the law suit.

CROSS-IMPACT EVALUATION TABLE

	SUPPOSE THAT THIS EVENT ACTUALLY HAPPENED					TRENDS				
	E1	E2	E3	E4	E5	T1	T2	T3	T4	T5
E1		0	+75	+100	+100	+40	+90	0	+20	+90
E2	0		+50	+75	+20	+50	+90	+20	+90	+70
E3	+100	+80		+70	+10	+60	+100	0	+75	+20
E4	+10	+70	+80		+100	+40	+65	0	+50	+80
E5	0	-30	-50	-70		+40	+75	0	+60	+50

TABLE 3

TRENDS

T 1. The need for Law Enforcement officers with higher educations, especially those who are computer literate, will be acute.

T 2. New and more advanced methods of providing security to computer systems will continue to become available.

T 3. Technology will continue to advance at or greater than speeds currently experienced.

T 4. The trend to seek technological assistance and consultations with private sector professionals will accelerate.

T 5. Increased incidents of breaches in computer information systems will continue to focus public attention on the issue of security.

EVENTS

E 1. Displaced or disgruntled employee sabotages a Law Enforcement information system.

E 2. A "mole" program is designed that sends confidential information from an infected information system to the "mole" program designers.

E 3. Organized crime puts a priority on obtaining information contained in Law Enforcement computer records systems.

E 4. Sensitive or confidential information is obtained by tapping into a police agency's computer system and this information is used to perpetrate a crime.

E 5. Confidential information is revealed when an unauthorized intrusion into police records is made resulting in a law suit by the subject named in the information for negligence against the police department.

SCENARIOS

The following narratives are used to describe possible projections suggested by the assimilated data. By reviewing the information contained in the evaluations of the trends, events and cross-impact analysis, suggestions of future occurrences can be assessed for planning purposes. Those who fail to prepare for the future are often doomed to live in the past and be woefully unprepared for situations which occur and impact their lives.

These scenarios are cast against a backdrop of a medium sized municipal police department serving a community comprised of mainly residential land users with a smaller commercial and industrial area. On the whole the community is relatively well balanced with regard to composition and is neither more nor less susceptible to trends and events than most other California communities. The first scenario is a hypothetical, "worst case" scenario. That is, based on the information collected, it is "feared, but possible". This scenario is based on the failure of an executive police manager to research, assimilate the data, and put a viable policy into effect.

The second scenario, again is normative but presumes some proper planning on the part of the same executive police manager. This scenario is "desired and attainable". As was the case with the first scenario, information

collected in the evaluation of trends and events were used to formulate this scenario. Information from this scenario will be the basis for the Strategic Plan and Transition Management Plan sections of this study.

The third and final scenario for this section is done in the hypothetical mode and contains speculations as to what might occur in the future if the executive police manager acted on all available information and took a pro-active approach to futures planning. This potential future, also known as the "what if?" scenario, will examine the "best case" scenario.

SCENARIO No. 1

(Feared but Possible)

Chief Williams punched in his personal identification number and logged on to his computer. He looked at the date on the screen and mused to himself that just a year ago, June 1st, 1997, he would never have used a computer for sending messages to his subordinates, that's what he paid his secretary to do. At first he felt a little intimidated by the new technology at his disposal but he soon learned to treat this device just like any other piece

of equipment. He even reveled in the fact that he had become so adept at utilizing the new technology that he actively searched for new ways to employ it. He boasted that his department was the most computer literate and technologically advanced police department on the west coast. Only a few months earlier he had convinced the City Manager, Wayne Stuart, to put all city records on the computer system. The advantages in updating documents and personnel files were quickly realized. The efficiency gained by the use of computers was nothing short of phenomenal! Chief Williams had previously converted the police department's records to the computer system. He had even been careful enough to have the system backed-up by duplicate disks.

The uses of his computer were limitless. Since he had personally joined several "bulletin boards" and user groups he was able to get new programs and information almost at will. Sure he knew that perhaps the programs were a pirated version of the copyrighted originals, and perhaps it was slightly unethical for a police chief to obtain these devices even for departmental uses, but then, everyone was doing it, and his intentions were noble! A year ago he would have been too timid to join a user's group or to use a modem to tie into various electronic bulletin boards, today it seemed like a natural progression for a forward thinking executive.

When he was a child he had dreamed of being a cowboy

and saving the west with his blazing sixshooter. His weaponry now was a computer terminal and a keyboard with which he could send messages to any member of his department, even those elusive undercover narcotics officers whom he often only saw on paydays when they came in to collect their bounty. Yes, he had surrendered his sixshooter for a new, more powerful weapon, the computer, he was...a "Computer Cowboy", here to save the west! It hadn't been all that difficult a decision to make, changing to a computer driven department.

Change for Chief Williams was always done the same way, first you had to show him why he should change. Then you had to show him how to change. Finally you had to show him that he could change and what was in it for him. Once these items were accomplished there was no holding him back. He often jumped into a situation with both feet before testing the water. So it had been with computers, but then again this was Chief Williams' style and if he lacked anything it certainly was not style!

Reflecting, he thought that the only really difficult thing about this whole change was learning how to say no to those panhandlers of paranoia who constantly kept trying to sell him "protection" for his computer system.

Security consultants to him made it sound like a mine field out there with, some cloak and dagger character waiting in every darkened doorway. "Protection" he laughed, "what the hell business do they think I'm in for

Chris' sake? Protection, why I've been doing that for nearly 31 years! I ought to by God know something about protection"! He then thought of the look on the City Manager's face when he had presented him with a bill for $17,356 for security hardware and burglar alarm devices the chief had installed in the computer room. "That ought to keep the crooks away from our computer main frame".

It amazed even him to think just how confident he was feeling. Perhaps this feeling was heightened because he knew that his narcotics unit had been using the new technology to ensnare one of the biggest dope dealers on the west coast and he was awaiting the good news of the arrests via the electronic mail system he insisted be used to keep him completely up to date to every detail as it occurred.

He sat back in his overstuffed chair and waited for the good news. Shortly before noon, the estimated time when Detective Thomkins was supposed to reveal his identity to the dope dealer who would be surrounded by other officers from Chief Williams' department, a rather peculiar event took place on the computer screen. A little masked figure, much like those he had seen on nintendo games, appeared . The masked figure was being chased by a another figure obviously dressed like a cop, all the time this was occurring the tune of "pop goes the weasel" was playing. "How ingenious" he thought as he sat transfixed to the images on the screen. He was thoroughly amused as he

watched the chase played out until suddenly the little masked figure stopped in his tracks, turned, drew and fired a pistol at the pursuing police figure. The whole screen lit-up with the single word, "bang". As the word "bang" dissolved from the screen, a large tombstone with the name "Thomkins" and the dates 1970-1998 appeared in its place. Stunned, the chief sat there, unable to move as the full meaning of the charade became apparent to him. His mind filled with a hundred questions almost simultaneously, the most dreaded of all was "how". " How did they know"? The question was rhetorical, because in the pit of his stomach he knew the answer was one he did not want to hear.

He had protected his computers the way he had protected everything else. He used casehardened locks, burglar alarms and video monitors to secure the computer room but he hadn't put up even the slightest resistance to intrusion from outside the department via the phone lines. In fact, he knew that his own infatuation with bulletin boards, pirated programs, and the like had made the city's personnel information records easy pickings for the sophisticated crooks of today. The realization of the consequences of his lack of foresight grew within him and became a consuming ache. Suddenly he no longer felt like the savior of the west. He knew it was time for this computer cowboy to turn in his spurs.

SCENARIO No. 2-NORMATIVE

(Desired and Attainable)

Chief Williams sat at his computer terminal and entered his personal identification number. As the screen came alive he marveled at the new technology available to law enforcement officers today. He was a cautious man by nature, slow to impress and one who tended to consider nearly every option before being moved to adopt one position or another. Once convinced of the data he was very decisive. At first he had been intimidated by the proliferation of electronic data that seemed to suddenly surround him yet he was astute enough to know that those who stand in the way of progress are most likely doomed to be run over by it. He was not about to let that happen to him.

While it could not be said that Chief Williams ran out to embrace the tide of new technology that rushed towards him, neither did he turn from it or over look its potential abuses. It had always been his experience that too much of anything is not good for you. When the City Manager, Wayne Stuart, had suggested in 1997 that all records within the city be computerized Chief Williams did not refuse. He did however hire a consultant at the cost of $17,356 to the

City for the purposes of insuring that personnel files and classified information could be accessed only after a P.I.N. (personal identification number) and password had been properly entered into the terminal. Outside information users required the same security measures and a phone call had to be made to the on-duty Watch Commander so that an access switch would manually be turned on. The person seeking access had to know the password and provide an access code number to gain entry into the system. Even after access was gained into the system each officers' personnel records were coded under a different name than his real one and this information was in the hands of only a trusted few. As a final precaution a black-box device was placed on the in-coming trunk link and anyone seeking access would have their phone line jammed open until a trace was made and an automatic disconnect device was employed that prohibited any calls from a pay phone.

Chief Williams knew that there were other steps that could, should, and would be taken to help protect the computer system and he weighed these measures against their fiscal implications. His precautions caused him to be given the unfair label of "Paranoid Patrick Williams" but he simply shrugged off such insults. He was a good old fashioned cop trying to face the future with optimism but preparedness.

Today he waited anxiously by the computer for news of a drug bust that his department had been working on. The

arrest was to be made at the posh Sea Cliff Towers condominium complex, a 1700 unit development located in the exclusive beach community of Marina Del Sol. While he waited, the on-duty Watch Commander, Lieutenant Franklin Lewis, received an outside call requesting access to the departments' computer informations system. The caller did not have the proper password, though he did have the correct code. Lt. Lewis thought for a moment and decided not to turn on the access switch which would have given him access to information in the departments computers. Instead he waited for the automatic tracing device to give him the location of the caller. He noted that the caller had hung-up almost immediately after access was denied, and his concerns were heightened when the address check of the telephone number came back to the Sea Cliff Towers in Marina Del Sol. He immediately called the detective division commander who in turn called the back-up units sent to assist Detective Thomkins with the arrest.

Thomkins left the complex with one of the dope dealer's body guards, ostensibly to retrieve the money for the narcotics transaction from the trunk of his vehicle. As Thomkins bent over into the trunk of his undercover car he heard the unmistakable sound of someone racking a shell into the chamber of a shotgun. His fear changed to confusion as he next heard the sound of a dozen or so additional shotguns being "racked" and the firm, commanding voice of his back-up officer ordering the bodyguard to put

down the sawed-off shotgun he had intended to use on Thomkins.

The dope dealer had suspected Thomkins was a narcotics officer and had attempted to get information on him through the police department. When this failed he had his hacker attack the City's personnel records and the payroll ledgers confirmed the doper's suspicions. He then ordered the bodyguard to kill Thomkins. Thanks to some basic computer safeguards and the quick thinking of Lt. Lewis, a tragedy was narrowly avoided.

The success of the police department's modest yet effective computer security systems have convinced both the Chief and the City Manager that an ounce of prevention is worth a pound of cure. The security measures will be enhanced in short order!

SCENARIO 3

(Hypothetical "What If?")

Chief Williams sat at his computer terminal and entered his personal identification number. As the screen came alive he entered his password and gained access to the security clearance module, a 2 by 2 inch box appeared on the screen. The Chief placed his right thumb on the box and held it there as the inter-active biometric security scanner read, classified, compared, and stored his print.

The system, Computer Centurion, had been installed at the same time the department's computers were brought on line. The program was expensive, costing over $75,000, but the Chief considered this a good investment compared to the potential cost of failing to provide security for his software. Earlier that year (1998) he had "retina" identification devices installed on all doors leading to sensitive or classified information processors.

Chief Williams had taken a good deal of ribbing from other department heads within the city but repeated incidents of security breaches into law enforcement and private business systems continued to focus public attention on the need for such devices. Perhaps the most persuasive of all events that affected the utilization of security measures was the recent U.S. Supreme Court decision, **Elester vs. The City of Bellmont Police Department** which was settled as Chief Williams and City Manager, Wayne Stuart, were employing an outside professional consultant to advise them on exactly how to secure their new computer network. That case had been settled for a hefty 1.3 million dollars and included punitive damages of $75,000 and $50,000 respectively against the chief and city manager of the City of Bellmont for their negligence.

By consensus it seemed clear to police chiefs' organizations throughout the nation that computer security systems were cost effective. This prompted Chief Williams

and City Manager Stuart to interview and select Dr. Raymond Flowers who had been a program designer, analyst and security specialist for International Business Incorporated before forming his own corporation, Hi-Tech Security Inc..

During the past five years, Dr. Flowers had seen a proliferation in the number of incidents of security intrusions into confidential computer systems of both the municipal and private sector. It still amazed him how some police executive managers regarded computer security much the same way one would think of building security. "If you want to secure something get a good casehardened brass lock, if that doesn't do it, get a bigger lock, if it still isn't secured then buy yourself a guard dog!" he had once been told by a police chief from a well known east coast city. It wasn't more than four months before one of that chief's own disgruntled employees took advantage of his stubbornness and ignorance of security to plant a "timebomb" in the records management program of his department. One day the department functioned as a normal police agency, and the next day it was brought to its knees by a still unknown employee who had introduced a rogue program into the system and wiped clean the entire police records. As Dr. Flower had guessed, the chief had not taken the precaution of backing-up his records systems with duplicate disks. He also had failed to properly plan for his retirement which the city manager and the entire

council strongly suggested he do, commenting "Police Science, and technology have generally passed the Chief by. We wish him well in his new career." Flower learned that he had become a store security agent, who's only duty was to visually check for shoplifters and take stolen bicycle reports from children who frequented "Uncle Al's Toy Emporium".

By comparison Chief Wiliams was a breath of fresh air. Though cautious, Williams was bright and analytical. He was certainly decisive, as most executives tend to be, but Flower was impressed by his ability to quickly assimilate information and remain flexible on an issue until all obtainable facts were studied. The mere fact that the chief was willing to utilize the services of an outside professional consultant indicated to Flower that Williams realized that computer security was beyond the expertise of all but a few police executives. The growing trend of employing outside consultants indicated that Chief Williams was not alone. The rising rate of detection and conviction of would-be systems intruders and the dramatic decrease in successful security breaches points to the fact that an ounce of prevention truly is worth a pound of cure!

OBJECTIVE II:

STRATEGIC PLANNING

OBJECTIVE II:

STRATEGIC PLANNING

STATEMENT

The purpose of this section is to develop a mission statement, plans, and policies that will enable us to anticipate the future, and work with the trends to direct events which we want to occur, while limiting the possibility of non-desirable events from occurring. Since the future is a maze of unknown or yet-undecided scenarios, the task for this researcher was to create a climate conducive to the best possible scenario occurring. If this fails law enforcement may well see the "worst case" scenario (feared but possible) occur.

METHODS: IDENTIFICATION

The development of a Strategic Management Plan is accomplished through the use of a WOTS-UP Analysis, a Capability Analysis, a Stakeholder Analysis, and the identification of Snaildarters . In addition to the aforementioned, a SAST (Strategic Assumption Surfacing Technique), and a Modified Policy Delphi panel were utilized.

METHODS: IMPLEMENTATION

In order to develop a macro and micro mission

statement a model law enforcement agency must be employed. For the purposes of this study the model used is a medium sized Southern California law enforcement agency serving a predominately homogeneous, residential community located in an urbanized area of Orange County, California. The trends and events discussed in Objective I are such that they affect all law enforcement. Therefore the use of nearly any law enforcement agency will have application to other agencies of generally the same composite.

MISSION STATEMENT

The Mission Statement of an organization is a critical part of its policy. The Mission Statement sets the values and defines the measurements by which an organization is measured. It provides the direction for an organization. The following are the Macro and Micro Mission Statements for a medium sized police department with regards to the issue of computer information security systems:

The Macro Mission is to insure and enhance the security capabilities of the police department's information-processing systems.

The above statement encompasses the idea of both area and software security. The means by which this mission is accomplished will include a wide range of methods and devices.

The Micro Mission Statement of an organization is a statement or series of statements which details the issues encompassed in the Macro Mission Statement. The Micro

Mission Statements for the issue under study are as follows:

1. Provide hardware security for all computer devices.
2. Provide software security programs for all personal and main-frame computers.
3. Develop security codes for access to and level of programs available to the user.
4. Secure all landlines and modems with access to the computer system.
5. Develop comprehensive policy and procedures for regulating the activities of all employees and vendors with access to the city's information-processing system.

SITUATIONAL ANALYSIS

The purpose of a **WOTS-UP** Analysis panel is to examine the data presented in the evaluations of the trends and events and the cross-impact analysis and to assess the potential actors and reactors that may occur in the future. WOTS-UP is an acronym for weakness, opportunities, threats, strengths and underlying planning. In order to provide a framework for the situation audit, the information in this section was taken from input by the members of the Modified Delphi Panel as well as selected members of local municipal law enforcement agencies. A "brainstorming" session was conducted and the resulting weaknesses, opportunities, threats, and strengths were identified.

Weaknesses

With regards to the issue of concern in this study, providing security for law enforcement information-processing systems, six main weakness were identified by the group.

Although computers can simplify difficult tasks and generally make life easier for police agencies, programming and maintenance of these systems can be a complex matter. The group felt that the rapid proliferation of computer technology has left law enforcement lagging behind. There is a real or perceived lack of technical expertise in computer technology within law enforcement.

Coupled with the aforementioned lack of expertise, the panel listed the lack of financial resources as a weakness in providing security systems to law enforcement computer systems. The trends and events analysis point out that such devices may be cost effective in lieu of the potential cost of defending or losing a civil suit for negligence for failure to secure sensitive or confidential information.

The location of computers was named as a weakness since most are kept in a variety of offices scattered throughout the department. There is less chance of a clandestine use of a computer being discovered if the location of these devices is decentralized. Some departments are even known to have computers in areas which, while they are almost always attended by police personnel, are accessible to the public.

There is a tendency to be lax in the area of computer security hardware. Police personnel prefer to think that these machines are safe since they are located within the police department building. Security for these devices is minimal. In addition to this, aside from access codes, there is virtually no security on access to computer information systems. Finally, the panel felt that the systems themselves were highly vulnerable since no security software is employed to routinely sweep the data programs and other sources of potential contamination. Law enforcement information-processing systems are highly vulnerable to sabotage from within the organization as well.

Opportunities

The implementation of a strategic plan to insure the proper security of a law enforcement agency's information-processing system would create immediate opportunities both internally and external of the organization. One of the perceived benefits is that the implementation of such a plan would create or enhance the feeling of security the public has with regard to law enforcement. It was widely felt among the panelists that the endeavor to improve the security systems of a local law enforcement agency would have a significant "spin-off" effect of technology usable throughout the city. Panelist agreed that the interaction of technologists and those trained in law enforcement would

serve to lessen the distrust that sometimes exists between police officers and non-sworn personnel. In addition to this, it is a widely held belief that police departments by and large under-utilize the technology available to them. The capabilities that already exist, yet remain untapped, are a technological as well as an economical waste.

Threats

One of the threats perceived by the panel was the threat posed by a lack of financial resources. Security programs are expensive and the requisite technical skills to implement such programs is not cheaply acquired. Here though, a good argument could be made that such programs are not only strategically sound, but are, in lieu of certain litigation economically sound as well. Another concern of the WOTS-UP group was that opening an agency's system to outside consultants, albeit security specialists, makes it more vulnerable. This fear was overcome through the brainstorming session yet it was duly noted at the time it was first brought up. The major concern of the group was that it (the issue of computer security) would become a political football. If this were to happen the issue would be studied to death and nothing would be resolved or done. All agreed that the best course of action would be gain the confidence of the city administrator and avoid elected politicians on this issue.

Of final concern to the group was the press. There

were two specific areas regarding the press that concerned the panel; first, would they see the attempt to enhance security of computer systems as one more governmental attempt to shield information from the public? Secondly, would the treatment of the issue given by the press be fair and unprejudicial. The press could exploit the issue and do an expose' on it which might encourage hackers and criminals alike to attempt to violate the computer information system.

Strengths

The strengths of any law enforcement agency are the people within and outside of the organization that offer leadership and support. Organizations such as POST act as quality control agencies concerned with insuring the continual improvement of skill levels possessed by law enforcement officers. This constant vigilance is surely a strength. Truly, public opinion is a powerful force, one which can be a strong ally or menacing opponent. The public climate is currently strongly in favor of law enforcement.

The Underlying Planning, as discussed in the following pages was entered into with a strong idea as to the strengths and weaknesses surrounding the issue of enhancing security systems for the police department's informations system. The next step was to do a "Capability" analysis. Again members of the department were involved in providing the information for this phase.

Organization
Capabilities and Resources

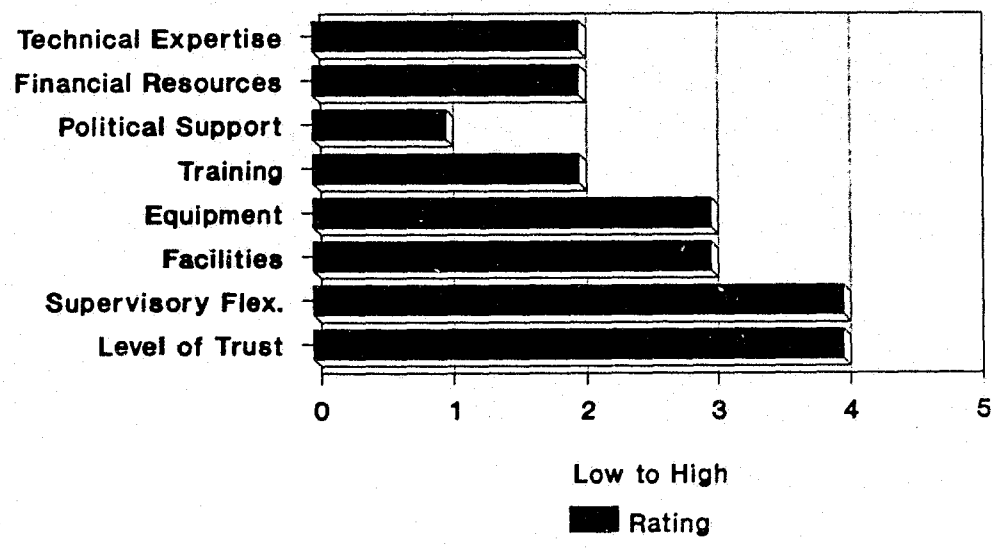


CHART 1

Capability Analysis

An analysis of the department to determine the ability it possesses to change (or the lack thereof) was conducted. The results are reflected in the above Organization Capabilities and Resources Chart. Members of the city's police department were polled in eight areas. The areas included technical expertise, financial resources (availability of financial resources from the city's general fund), political support, training, equipment, facilities, supervisory slexibility, and level of trust. The scores ranged from a low of 1 to a high of 4. The data provided would seem to indicate that it is felt that there would be little support from elected officials for enhanced security devices, yet supervisory flexibility and the level of trust are very high.

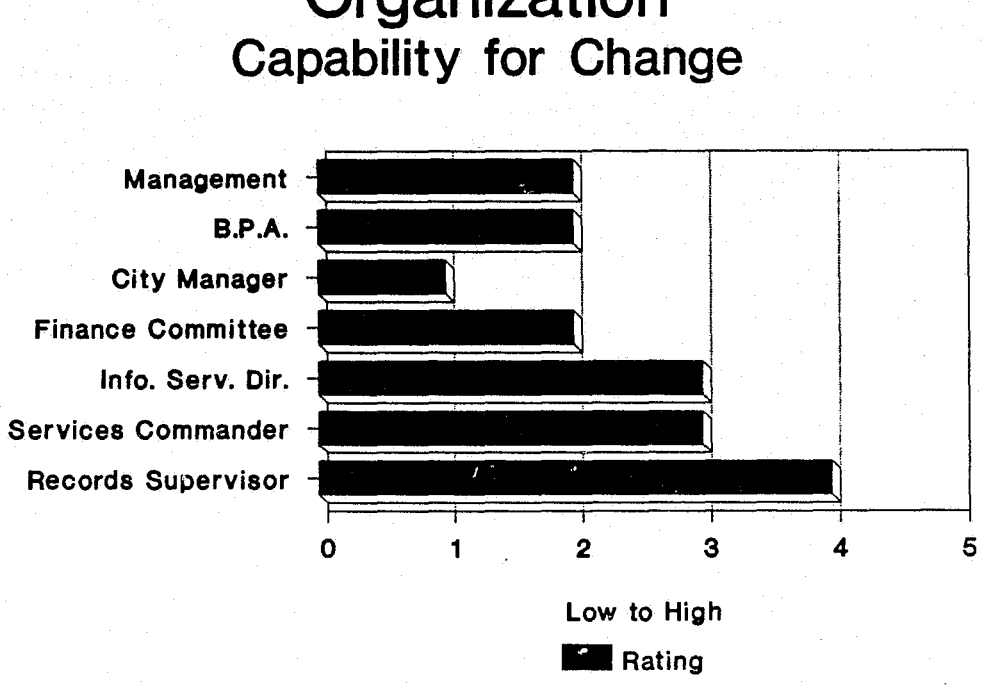


CHART 2

Organization Capability for Change

Next the group was asked to rate the "Capability for Change" within the organization. The results of this survey are displayed on the above "Organization Capability for Change Chart". This city is fortunate here in many regards, note the high ratings given to management (within the police department), the city manager (who is relatively new to the city and progressive), and the information services director, who will be affected by any action taken on the issue under study. Only the finance committee, and records supervisor received marks below neutral (on a scale of 1 to 5, 2.5 being the median). The B.P.A. (Benevolent Police Association) is relatively neutral on this issue. This association is comprised of line officers from entry level to the rank of sergeant and dispatch personnel.

Strategic Assumption Surfacing Technique

A Strategic Assumption Surfacing Technique (SAST) is a method used to identify those persons or organizations who are likely to be affected by the issue under study. These people or organizations are impacted by the issue either positively or negatively or who otherwise have a concern with the issue, (stakeholders). For this task the same group used in the WOTS-UP Analysis was given an explanation of the exercise and asked to identify the stakeholders. The purpose of this phase was two fold: first, to identify all potential "stakeholders" and "snaildarters" (those non-obvious stakeholders who could cause potential difficulties). Secondly the group was asked to reduce the list from the original fifteen stakeholders identified to the eight most important and "snaildarters." The following were identified as stakeholders:

+ Chief of Police
+ Information Services Director
+ City Manager
+ Orange County Communications
Public at large
* American Civil Liberties Union
+ Benevolent Police Association
Regional A T & T Office
Records Supervisor
+ Finance Committee
City Attorney
Software Vendors
* The Press
+ Computer Consult.
+ Services Div. Commander

From this initial list of fifteen, eight were selected for inclusion in this phase of the study. Those stakeholders with a + sign were felt to be the most

impacted by the issue. The "snaildarters" in the list of stakeholders are identified by an *. The press (print media) were identified as a snaildarter here, not because of their influence on the public or the publicity they generate, these are indirect involvements with the police department. The press was listed as a "snaildarter" because of their potential direct involvement with the issue as discussed further on in this study.

Stakeholder Analysis

The purpose of this section is to identify the positions most likely to be taken by the remaining stakeholder. They are listed here in no particular order.

The Chief of Police

Charged with the responsibility to oversee the entire department, the chief is the department head of the police agency. He is concerned with the long term as well as the day-to-day operation of the department. This includes facilities and systems security. He is an independent thinker; none the less, he is also a member of the city's management team and therefore has to respond to the needs and desires of the city council and city manager whenever they do not conflict with statutory mandates. He is open and flexible and one of the more forward thinking managers in the city. He will be supportive of change if it: a) is cost effective, b) streamlines a process, or c) involves

the safety of his subordinates or the general public.

The Information Services Director

This job function is given several different titles and few cities call it by the same name. The function is to oversee the information-processing system city wide. The impetus to change from the status-quo will be great with this person because it is an opportunity to enhance a system that he sees as vulnerable, not to mention enhancing his own job function.

The City Manager

As the chief city administrator, this person is charged with a variety of duties. The issue of insuring and enhancing the security devices for the information-processing systems will pull him in two directions at once. First, he will be forced to admit that the current condition of security is inadequate. Secondly, he will have to balance these needs with a host of other programs calling for expenditures from the city's general fund.

Orange County Communications

Control One, as it is known throughout the county, is the coordinator for all police communications. All radio transmissions go through it before reaching their final destination. While agreeing in principle to the need for increased computer information systems security, they may resent and try to block a change that intrudes or interrupts their access to Brea's communication network.

Benevolent Police Association

This organization is comprised of the rank and file members from within the police department. Entry level through sergeant grade officers and dispatchers are represented here. This group is the chief negotiating unit for the police department. They are vitally concerned with all issue of working conditions and or other issues which affect the work climate of the department. If the issue of enhancing security is shown not to place an additional burden on their duties, then the change will be easily accepted. If, however, the change to a new enhanced computer security system does place a burden on association members, then this issue could become a subject for "meet-and-confer." It does not appear that the burden to be placed on the department would be unreasonable. Training will be the major issue with this organization.

Finance Committee

The Finance Committee is comprised of two city council members, the city manager, and the finance director. The purpose of this committee is to review funding items and requests for expenditures and make recommendations to the whole council. There very well could be some resistance to the expenditures called for by the enhancements to the computer security systems. The need versus the potential costs of failure to make the improvements must be stressed with this group.

Computer Security Consultants

Most modern cities routinely do some minimal contracting with outside consultants. In order to enhance the security systems of the city's computers this contact will have to be increased. Issues of trust, cost, and reliability will have to be addressed.

Services Division Commander

The Services Division Commander has the responsibility for supervising non-uniformed services within the department. This function includes the supervision of records personnel. Since this classification of workers is likely to be the most affected group in the department by enhancement of the information-processing systems, care must be taken to solicit support from this group and assure them that the issue of systems security is not tied to any feeling of distrust for them.

Identification of Snaildarters

As previously mentioned, snaildarters are those persons or groups whose impact on the issue is at first non-obvious. These snaildarters can often create the most difficult barriers to implementing strategic plans to deal with the issue/s at hand.

The American Civil Liberties Union

The A.C.L.U. has, in the past, brought a variety of individual invasion of privacy suits. There is ample reason to believe that this will continue.

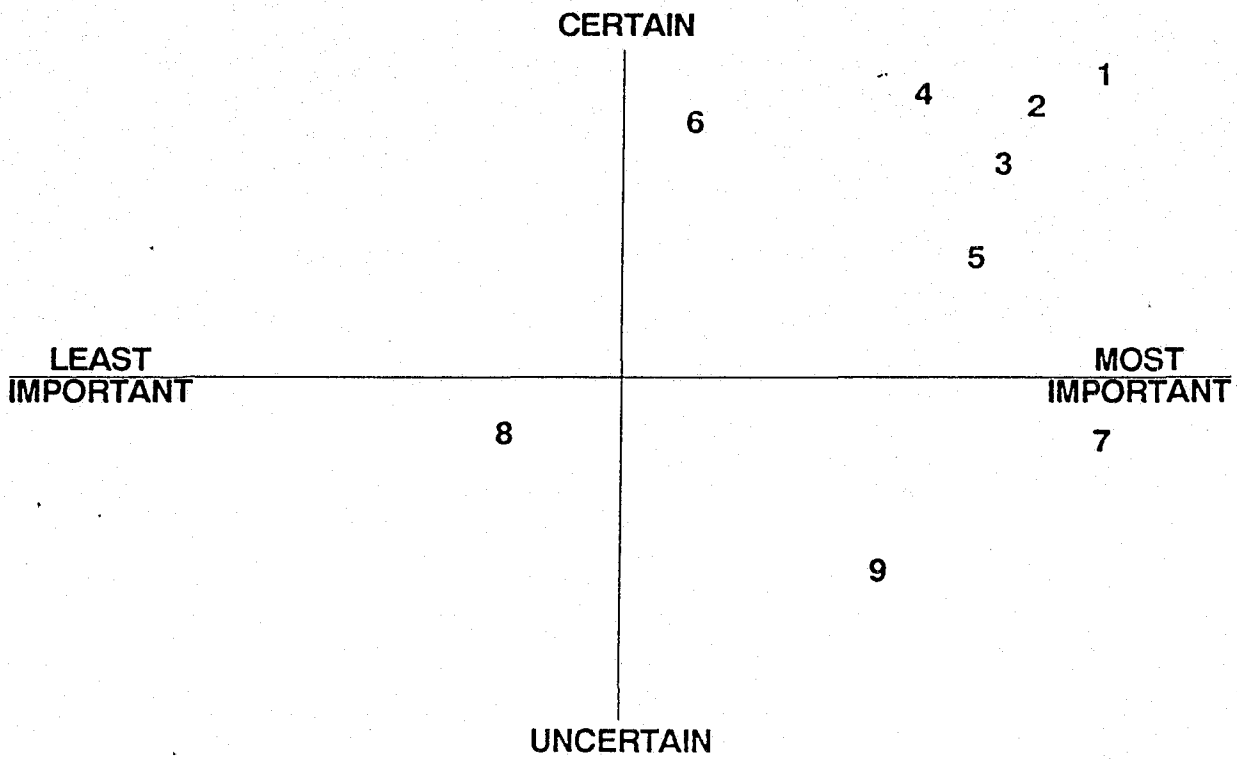
The panel felt that the A.C.L.U., which has always been perceived by law enforcement as overly suspicious and critical of police activities, would be likely to bring suit charging that planned security measures violates the individual privacy of the people since the material stored will include some confidential information about citizens. This is likely to be unsuccessful. This will not, however, stop the A.C.L.U. from bringing such an action to bear. The more serious challenge comes from the other snaildarter, the press.

The Press

The history of the relationship that law enforcement in general has had with the media is best described as "checkered." At times the press can be law enforcement's very strongest ally; at other times it can be the toughest opponent. The reason the panel felt that the press was a true snaildarter was that since it is the business of the press to report anything they deem newsworthy, (the press is certainly not a "non-obvious" stakeholder as previously mentioned), yet the challenge from the press will come for an unanticipated reason. One would expect the press to write about the cost of the improved security measures or to do an expose' on the sorry condition of current security systems. This could and should be anticipated. What the panel felt would be the most serious challenge from the press would be a "freedom of information" suit, charging that the police proposal to enhance systems security would affect their

access to information. One does not have to go far to recall the Orange County Register Newspaper's successful suit against Orange County Sheriff Brad Gates. This represents a real threat to implementation.

Having identified the stakeholders, condensing that original list of fifteen stakeholders to eight, and finally identifying the potential "snaildarters", the next task was to construct a "Strategic Assumption Surfacing Techniques Chart" (on the following page). The purpose of this process is to paint a visual picture of where the stakeholders are in relation to the issue. The process starts with "Least Important" on the far left side of the horizontal line. On the right the line moves to "Most Important". These terms are self explanatory. On the top of the vertical line, "Most Certain" is written. As used here, this term indicates that the closer a number is placed to the top of the vertical line, the more "certain" the rater is of the placement. The bottom of this same vertical line is marked "Least Certain". This indicates that the rater is less certain of the placement of the subject as it gets closer to the bottom of the chart. Originally all stakeholders were charted. The chart below reflects only the final eight.



1 CHIEF
2 CITY MANAGER
3 SERVICES DIVISION COMMANDER
4 RECORDS SUPERVISOR
5 CITY FINANCE COMMITTEE
6 INFORMATION SERVICES DIRECTOR
7 B.P.A. (BENEVOLENT POLICE ASSOCIATION)
8 SECURITY CONSULTANTS
9 PRESS (SNAIL DARTERS)

CHART 3

The Strategic Assumption Surfacing Technique Chart

The above chart identifies the stakeholders and charts their positions relative to the issue. Two measurements are obtained by this chart, the stakeholders importance to the issue and the certainty of that assumption.

The Modified Policy Delphi

A Modified Policy Delphi panel was assembled to develop, critique, and select policies designed to create a climate which would reduce the possibility of the worst case scenario from occurring while promoting the chances of the desired and attainable and/ or the hypothetical, best case scenario. As with trends and events these were ranked for a second round using the median. The panel was then asked to explore the pros and cons of each policy. The selected policies are shown below.

Policy Options

1. Background investigations will be done on all city employees who have any clerical or records jobs or who work with the computer system in any capacity.
2. Employees will be trained to recognize and use proper computer procedures designed to minimize the chances of using a contaminated disk.
3. All new records will be backed up on a daily basis.
4. Outside computer security consultants will be employed to design both hardware and software security.
5. Personal identifiers will be enhanced with state-of-the-art biometric identifiers such as voice print, thumb prints, and retina identification.

The major strengths and weaknesses were then

identified for each policy and the desirability and feasibility were charted.

Policy Considerations

The pros and cons of each policy are listed below. These do not represent the only pros and con, simply the major ones.

Policy No. 1- Background Investigations for Employees

Pro: Insures that no applicant with a criminal past becomes an employee who has access to computer systems.

Con: Creates a feeling of distrust.

Policy No. 2- Computer Security Training for Employees

Pro: Offers best chance to avoid a computer virus.

Con: Involves both immediate and on-going costs.

Policy No. 3- Daily Back-up of New Records

Pro: Safety of records and work-in-progress is assured.

Con: Time consuming and costly.

Policy No. 4- Employment of Outside Computer Consultants

Pro: Provides expertise not possessed by police officers.

Con: Could impact morale; would be costly.

Policy No. 5- State-of-the-Art Technological Security Devices

Pro: Controls access best.

Con: Expensive to acquire and keep up.

Implementation Strategies

Having identified the stakeholder, snaildarters, and required policies, attention must be given to the development of a strategic implementation plan. The research has identified the issue as one that will not correct itself without attention from an outside source. Clearly this problem will become untenable unless steps are taken now to insure that in the future this problem becomes manageable if not a non-issue. In order to create a desired climate for orderly change responsibilities and time frames must be attached to the aforementioned policies. The following implementation plan was recommended:

Policy No. 1 Background Investigations for All City Employees

The city manager and the human relations committee will have to make this part of the city's policy. The title above is a little misleading, since only those with any possible access to the computer systems will be required to submit to a background investigation.

The finance committee will have to be made to recognize that this policy is, in the long run, less expensive than a sabotaged information-processing system.

Responsibility: City manager, finance committee, chief of police.

Implementation Time: Immediately and ongoing.

Policy No. 2 Computer Security Training for Employees

There will need to be an extensive training period for city employees, most particularly those who have been with the city the longest. Clerical personnel and officers alike who have been at their jobs the longest were educated under a system that did not know computers.

Responsibility: City Manager, all department heads, information services director.

Implementation Time: One month and ongoing.

Policy No. 3 Daily Back up of New Records

There may be many challenges to a law enforcement information-processing system. Not all of these challenges will come from man. A natural disaster could easily wipe-out such a system and particularly in California this should be of concern to any police manager.

Responsibility: Services division commander, chief of police, records supervisor.

Implementation Time: One month, ongoing.

Policy No. 4 Employment of Outside Computer Consultants

Lacking the expertise to solve the issue of computer security within its own workforce, the city will have to contract with reliable outside computer consultants who are experts in the area of computer security.

Responsibility: City manager, finance committee, information services director.

Implementation Time: Six months, then on a quarterly basis.

Policy No. 5 State-of-the-Art Technological Security Devices

There is much on the market today that bears investigating. There are voice analyzers, thumb print readers, palm graphics, and retina identifiers, just to name a few. The suggestion as to which systems are best employed and where, is an area best left to the professional consultants.

Responsibility: Consultants, Information Services Director, Finance Committee.

Implementation Time: Three months for hardware security, six months for the Hi-Tech software security.

Program Objectives

The purpose of this study is to encourage change from the current laissez-faire approach to law enforcement's computer information-processing networks to a more guarded but secure system. The identified objectives were:

1. Heighten the awareness of those in key leadership positions so that the proposed change can be seen as necessary and desirable.
2. Enhance the screening and training of city personnel with access to the computer systems.
3. Develop comprehensive policy and procedures to to assure adherence to sound security practices.
4. Purchase state-of-the-art security hardware and software to prevent unauthorized intrusions in-

to the information system.

If and when these objectives are met the issue of inadequate computer security for law enforcement information systems will be well on its way to being controlled. The word used here is controlled, not solved, because as has been pointed out by research law enforcement tends to lag behind in the application of technology. Meeting these objectives will keep honest people honest (i.e. the "mischievious hacker" with no criminal intent) but it won't settle the issue of computer security for all times. This is why a constant vigilance must be kept on this powerful tool.

OBJECTIVE III:

TRANSITION MANAGEMENT PLAN

OBJECTIVE III:

TRANSITION MANAGEMENT PLAN

STATEMENT

The third objective of this study is to develop a transition management plan which will assist with the over all implementation of the strategic plan for securing law enforcement computer information-systems from potential abuses. The goal of this process is to guide the transition into the desired future state. The wants and concerns of the stakeholders are taken into account here.

METHODS: IDENTIFICATION

The recommended policy changes and considerations listed in the strategic plan will require a transition plan for successful implementation. Using the WOTS-UP Group, the process recommended is as follows:

1. The critical mass is identified to determine who is instrumental in affecting change.

2. A readiness and capability analysis is done to determine the present state of the organization relative to ability to change.

3. A commitment planning process is used to determine the commitment levels of critical mass members.

4. A key leadership assement tool is used to ascertain top management's ability to change.

5. Implementation tools are selected for use by the

transition management team.

6. A map of the process is designed to guide the transition.

METHODS: IMPLEMENTATION

Where change is concerned, success is not a gift, it is a product of hard work and careful planning. One of the most critical phases of implementing change is that time period known as the transition period. The better the planning for this phase the more likely there will be a smooth transition.

The vehicles used to determine the actors and reactors as well as the direction of movement each must take have been discussed. The following section details these methods.

Critical Mass

The critical mass as defined here is that minimum number of actors needed to successfully influence the occurrence of the events necessary to deal with the issue at hand. While the delphi panel originally identified fifteen stakeholders, some of these stakeholders are more important than others and some can exert influence over others due to their relationships, employment, or personal strengths. For example, in dealing with an issue that concerns the chief of police, the records supervisor, division commander, the police officer's association etc., it may only be necessary to win two people over to the plan to assure the success. Presumably the chief exerts influence on the division commander who, in turn,influences

the records supervisor. The president of the police officers association may very well be all that is needed to swing the support of that organization to a desired cause. This is how the critical mass is determined. For the issue of enhancing computer security systems for the police department, the critical mass analysis is contained on the following pages.

City Manager

In any situation that requires expenditures from the general fund, city-wide training, or the hiring of outside consultants, the city manager will be critically involved. By his very position, the city manager has influence over department heads and councilmembers. Initially, the full council was identified as stakeholders; they are not part of the critical mass because their support can be gained by a favorable report from the city manager.

Chief of Police

As mentioned earlier, a number of police department supervisors and line personnel will be affected by the implementation of new security measures. Certainly the records supervisor will be affected; likewise, so will the division commander. Both of these are likely to be influenced by the chief of police. Additionally the chief will, through his leadership, set the tone for acceptance of the change throughout the department.

Finance Committee

While the finance committee is comprised of both

council members and city staff, and presumably influenced by the city manager, it is the "watch dog" of the city's purse strings and therefore not necessarily under the control of the city manager. As is the case with all entities charged with such responsibility it will be reluctant to implement any change that costs money unless and until either the change is proven cost-effective or it deals with a safety matter. The finance committee is therefore part of the critical mass.

Security Consultants

Since this group is likely to be eager for employment it would seem that there are a host of actors that would influence this group thereby taking them out of the critical mass. Since this group is "outside" the city employee rolls, there may be less influence here than first thought. The primary concern of this group will likely be security not cost or other city issues.

Police Officer's Association

The officer's association in any law enforcement agency is likely to be led by a line officer. The chief of police may be able to exercise some external influence on the organization, but the true power of such groups are its elected leaders. With regard to the anticipated changes in procedures, training and skill levels required to make security for computer information systems a reality, the police officer's association have to let it happen if not help it happen.

COMMITMENT PLANNING CHART

	POSITION ON THE ISSUE			
	BLOCK IT	LET IT HAPPEN	HELP IT HAPPEN	MAKE IT HAPPEN
CITY MANAGER			O	X
CHIEF OF POLICE			O	X
POLICE ASSOCIATION		O	X	
FINANCE COMMITTEE	O		X	
CONTROL I	O	X		
CONSULTANTS			X	O
PRESS	O	X		

O=CURRENT POSITION X=DESIRED POSITION

CHART 4

The City Manager

As the above chart shows, with regard to the issue of enhancing the security of the city's computer informational systems, the city manager will already be in the "help it happen" mode. If this endeavor is to be a success however, he will have to be one of the people that "makes it happen". This will require a slightly stronger commitment on his part.

The Police Chief

As was the case with the city manager, the police chief is already in the "help it happen" mode. Since the

vast majority of items concerned with the issue of computer security directly involve the police department, it is imperative that he stay in this mode if not move to a "make it happen" position.

The Finance Committee

The purpose of a finance committee is to be the watch dog of the city's purse strings. Operating out of that bias, the finance committee will be in a "block it" mode concerning the enhancements to the computer security system. In order for this proposal to be a success, the finance committee will have to move all the way to the "help it happen" mode. There are two arguments that can be employed to get the desired movement. First, the fact that these enhancements will offer greater security to the public by minimizing the opportunity someone might have of getting confidential information; and secondly, if such information is obtained a costly law suit could and most likely would result in a major settlement for the plaintiff. This cost-effective argument would seem to address the purpose of the committee.

Control I

Although not directly involved with the security issues of individual police department information systems, this agency is the hub of the entire county communications network. Like many large agencies they must be prompted to move before any action is taken place. They will most likely be in the "block it" mode using the old axiom "if it

isn't broken, don't fix it!" The same tactics taken with the finance committee would be used here except that the emphasis will be on the area of "officer safety." This they understand.

Security Consultants

Since the issue being dealt with here is the very substance of the consultant's employment, they will be eager to make the program happen. This could present a problem of a different nature. If the consultants come on too strong, the finance committee may be dissuaded to use them. Methods used by this group must not include "high-pressure" sales tactics. For this reason it would be better if the consultants were to lessen their posture on the issue in order to insure movement by other units.

The Press

As previously stated, the press, while not directly involved with the issue, will have an effect on public opinion. Since this project will require the expenditure of public funds, it makes good sense to seek their support. The press may see this issue as infringing on their freedom of information. A possible tactic would be to design a program whereby the daily log information and non-confidential reports, along with the names and pertinent information about arrestees and area crime is accessible to the media from their office computers. Under current conditions this is not feasible. A program such as this should move the press to at least the "let it happen" mode.

Recommended Strategy

The recommended strategy for solving the problem of inadequate computer security will involve a number parts. The plan will include but not be limited to training, the development and enforcement of policies and procedures, utilization of expert consultants, and the installation of security hardware and software. In order for this plan to work the following steps are recommended:

1. The first step in this plan is to heighten the awareness of the problem of inadequate computer security. This can be done by citing the growing number of documented incidents where a computer information system has been breached. A well-researched and annotated staff report defining the situation with regard to computer security intrusions, a comprehensive examination of the department's own procedures, and a possible future scenario should raise the consciousness of the organization.

2. The next step in this plan is to train all city employees who have any job function which could possibly utilize the computers to be security conscious. This includes training in the care and use of computers. It is not unusual for a person who has access to a computer at work to run personal programs on city computers at break time, during lunch, or after hours. Something as innocuous as a tutorial math program could contain a computer "Worm, Trojan Horse, Mole," or other potentially destructive device hidden in the disk. This step will also include the

introduction of background investigations for all City employees with computer access.

3. Step three is to develop comprehensive policies and procedures for employee conduct with respect to the use and care of computers and the attending software. Inherent in these policies is the understanding that such policies will be enforced.

4. Step four is the formation of a task force with enough expertise to understand the complexities of the issue and select the best available security consultants.

5. Step five is carried-out by the computer security consultants and involves surveying the department, ascertaining the training needs, and making recommendations for the purchase of both hardware and software security devices. The actual selection of these devices will be made by the city task force as a measure of insuring the secrecy of the devices being used.

6. The final step will be the installation of the security devices and the implementation of the policies and procedures. The implementation will require some guidance to be completed in a timely and orderly fashion. For this purpose a time-line is a valuable tool.

Responsibility Charting

As mentioned earlier, the most difficult phase of change is that time between the formulation of a strategic plan and the implementation of that plan. This time frame is the transition phase and to navigate through its often

rough waters requires a transition management plan. It is not enough to know what the issues are; successful problem solving requires that the roles and tasks of the actors be clearly defined.

Responsibility Charting is a method designed to identify these areas. The implimentation of the aforementioned steps will require a determination as to who is responsible for each of the tasks. The responsibility chart labels the task and indicates what is expected of the critical mass members (as previously identified).

For this purpose the RASI system was used. RASI is an acronym for:

R= Responsibility for ensuring the completion of the task.

A= Approval is necessary from this person or group.

S= Support of this group or person is essential.

I= No responsibility attached here, neither approval nor support is necessary. Subject/s must be kept informed.

Responsibility Charting not only identifies who is responsible for what, it also illustrates the interplay between the parties who make up the critical mass. Included in this RASI evaluation are two members who were not listed as critical mass members. Their inclusion on is chart is only to give a realistic assessment as to who will do the tasks listed under "decision."

RESPONSIBILITY CHART

R = Responsibility (not necessarily authority)
A = Approval (right to veto)
S = Support (put resources toward)
I = Inform (to be consulted)
- = Irrelevant to this Item

Actors

Decision	CITY MANGER	POLICE CHIEF	PEACE OFF. ASC.	FINANCE COMM.	CONTROL ONE	CONSUL- TANTS	SER. DIV. COM.		
CITY EMPLOYEE BACKROUNDS	A	R	S	I	-	-	S		
EMPLOYEE TRAINING	A	R	S	S	I	R	R		
BACK-UP RECORDS	A	S	S	S	I	I	R.		
HIRE CONSULTANTS	R	S	S	A	-	-	S		
TECHNOLOGIC ADVICE	R	R	S	A	I	A	S		

CHART 5

Readiness Assessment

In order to measure the readiness of key leaders, two tools were employed. The first tool used was an assessment tool developed by Dr. Ruben T. Harris in 1981, and who was kind enough to allow utilization of this tool by Command College researchers. Leadership's readiness was assessed by three dimensions. The first dimension measures the awareness of key leader's with regards to the current climate of their organization, the understanding of the relationships involved, and the complexity of the structure of the organization.

The second dimension measured deals with the motivation of those leader's with regards to willingness to act, willingness to plan, willingness to share responsibility (something many leaders find difficult to do), and willingness to make achievement of the "vision" (task to be accomplished or change to be made) a top priority.

The third dimension measured by this tool deals with the skills and resources possessed by the leaders of the organization. These skills include the skill to effectively employ non-authority power bases. They also include resources to time, budget, information, and people. A high value is placed on interpersonal skills. Also measured is the skill to know when to activate contingency plans. The following chart enumerates these skills and evaluates the key leadership accordingly.

ASSESSING YOUR ORGANIZATION'S (KEY LEADER'S) READINESS FOR MAJOR CHANGE

	VERY LITTLE DEGREE	LITTLE DEGREE	SOME DEGREE	GREAT DEGREE	VERY GREAT DEGREE	DO NOT KNOW
AWARENESS DIMENSIONS	1	2	3	4	5	0
1. Awareness of the nature of the orgnization's current environment				X		
2. Understandin of the nature on inter-relationships among organizational dimensions (e.g. people, culture, structure, technology, etc.)			X			
3. Appreciation that the change situation has some unique characteristics			X			
4. Appreciation of the complexity of the inter-relationships				X		
MOTIVATIONAL DIMENSIONS	1	2	3	4	5	0
5. Willing to specify a detailed "vision"					X	
6. Willing to act under uncertainty			X			
7. willing to make contingency plans					X	
8. Willing to activate contingency plans				X		
9. Willing to make the vision a priority					X	
10. Willing to assess own theory of behavior			X			
11. Willing to increase dissatisfaction with current situation			X			
12. Willing to use non-authority based influence			X			
13. Willing to share responsibility for change			X			
SKILL AND RESOURCE DIMENSIONS	1	2	3	4	5	0
14. Possesses conceptual skills for the future				X		
15. Possesses assessment skills knowing when to activate contingency plans				X		
16. Possesses interpersonal skills to effectively employ non-authority power base			X			
17. Possesses personal relationships with other key leaders in the organization				X		
18. Possesses ready access to resources (time, budget, information, people etc.)				X		

CHART 6

The Readiness/Capability Chart

This form is utilized to ascertain the readiness and capability that members of the critical mass have for change. The directions are self explanatory.

READINESS / CAPABILITY CHART

	Readiness			Capability		
	High	Medium	Low	High	Medium	Low
1. CITY MANAGER	X			X		
2. CHIEF OF POLICE	X			X		
3. POLICE OFF. ASSOC.		X			X	
4. FINANCE COMMITTEE			X		X	
5. CONTROL I			X		X	
6. CONSULTANTS	X			X		
7. PRESS			X		X	

CHART 7

Instructions

Fill in the following chart as it applies to the issue of enhancing computer information systems security. In the left-hand column, list the individual or groups who are critical to your change efforts. Then rank each (high, medium, or low) according to their readiness and capability with respect to change.

IMPLEMENTATION TECHNOLOGIES AND SECTION SUMMATION

The purpose of this section is to suggest some tools which will enable the management team to span the gray area between strategic planning and transition management. This often the most difficult time for any plan for change. The goals must be constantly revitalized and clearly defined means of measurements must be established.

Team Building Workshops

To insure that all members of the transition team have a clear understanding of the tasks before them it is often helpful to hold one or more "team building workshops". The design of these workshops is to put aside petty differences and work toward a common goal. Often personality profiles are tested and discussed to help team members know what motivates their fellow teammates.

Setting The Goal

Each member of the team has to have a clear understanding of the goal before them. Once the goal is defined it must be constantly revitalized to prevent members from losing interest, particularly on long term goals.

Establish Clear Measurement Criteria

A sure way to lose a group of well-intentioned workers is to fail to keep the message before them. The message will fall on deaf ears if it is not clearly defined and measurable. The goal must be defined with specificity. To assure compliance there should be regular check and balances applied to make sure those who have a role in the matter are meeting their obligations.

Education and Training

The movement from the past to the future will be greatly facilitated if those whose help is needed have been educated as to the issues surrounding problem. Training serves another purpose, it says to the person being trained "the organization must hold some value in me to spend this time training me."

Feedback

Most any person supervised would rather have corrective feedback than no communication at all. Failure to communicate is a major stumbling block to what would otherwise be a successful program. Research advocates regular meetings with specific agendas to bridge the communication gap.

Evaluation

Finally after the team building workshops, the goal setting, the training, and the communication, an honest appraisal must be conducted. The purpose is not to fix

blame if something went wrong nor to take the credit for the success, but to do a fair summation of how the team expectations were met. This will result in fine tuning the outcome of the current project and establish a sound precedence for the next challenge.

SUMMARY

Objective I: Defining the Future

This section of the study defined the issue under consideration in this research, stated the sub-issues, and gave the purpose for the study. The introduction material revealed the fragile state of computer security and drew attention to the vulnerability of law enforcement information-processing systems to attack from within or outside the organization.

Trends and events were analyzed for their impact on the issue under study. Future scenarios were developed with the information gathered.

Objective II: Strategic Planning

In this section the methodology and strategies were discussed. Macro and micro mission statements were developed, stakeholders were analyzed and policy options were identified. Implementation strategies were also developed.

Objective III: Transition Management Plan

The strategic planning section tells how to get from the present to the future, the transition management section tells who will be needed to get to the future and

how they will be utilized. The identification of the critical mass, the readiness and capabilities chart, and the assessment analysis are the tools used to assess those needed to move the status quo to a changed position.

CONCLUSIONS

Experts in the field of computer security whom the researcher interviewed all agreed that law enforcement, thus far, has been fortunate not to have suffered any major loss of computer systems information or to have had those systems violated in a significant manner. Perhaps even now this is occurring undetected because as a profession law enforcement has not yet accepted its vulnerability to such unauthorized intrusions. It is the hope of this researcher that by exposing the possibility of a future serious breach in the law enforcement information network, such an occurrence can be avoided.

Major universities, multi-national corporations, and this country's defense networks have all fallen victim to unauthorized intrusion by outside sources; it is foolhearty to believe that such a fate can not befall law enforcement.

Research indicates that by the end of this year (1990) there will be close to five million computers in this country. With a modem, an enterprising person can tap virtually unlimited informational systems. Law enforcement informational networks must not be one of those sources accessible to criminals and would-be hackers simply because no one believed it could happen to them.

IMPLICATIONS

By all expert accounts, security of information will be a growing problem for the public as well as law enforcement. The rapid proliferation of personal computers, modems, and software technology will force the next generation of law enforcement officers to become more and more computer literate. The technical skills required in the coming decade will make some inflexible officers obsolete, it will enhance the professional image of the police officer, and it may even create a two tier system of officers. One classification of officer may work in a strictly enforcement capacity, the other may be utilized for his/her technical skills. Such a division may be forced on law enforcement, but it would be better to elevate the skill levels of all officers rather than label some as "enforcers" and others as technicians. All officers will have increasing access to computer information and all should be made absolutely aware of the security issues surrounding such technology.

The implications are that the future of law enforcement will be closely tied to its ability to store, retrieve, assimilate, and protect information. The potential utilization of new technology is enormous, but so is the attendant responsibility.

END NOTES

1. Cornish, Edward. "Global Solutions to World Problems", Future Study. Bethesda, Md., 1984.

2. Koehn, Hank, Future Scan, issue no.411, January 7th, 1985.

3. Albanese, Jay S. "Tomorrow's Thieves", The Futurist. September-October 1988, pg.26.

4. Koehn, Hank, Future Scan, issue no. 411, January 7th, 1985.

5. Ibid.

6. Cone, Edward. "Crime and Punishment", Information Week. May 7th, 1990. p.33.

7. Liebs, Scott. "The Value of Security. Information Week. June 4th, 1990. p.36.

8. Bloombecker, J.J. "Buck". "Security Complex", Information Week June 4th, 1990. p.36

9. Ibid.

10. Baker, Richard H. The Computer Security Handbook. Tab Books Inc., Blue Ridge Summit, Pa. 1985 p.1.

BIBLIOGRAPHY

BAKER, RICHARD H. "THE COMPUTER SECURITY HANDBOOK", TAB BOOKS INC., BLUE RIDGE SUMMIT, PA., 1985.

BOUCHER, NORMAN. "THE SHADOW HAWK KNOWS." P C COMPUTING MAGAZINE, NOVEMBER 1988.

BRODY, HERB. "HIGH ANXIETY OVER P C SECURITY." P C COMPUTING MAGAZINE, NOVEMBER 1988.

BRUNNER, JOHN. "THE SHOCKWAVE RIDER", HARPER AND ROW PUBLISHERS, NEW YORK, 1975.

CONE, EDWARD. "CRIME AND PUNISHMENT; INSIDE INTERPOL'S COMPUTER DIVISION", INFORMATION WEEK MAGAZINE, MAY 7, 1990.

CORNISH, EDWARD. FUTURE STUDY, "GLOBAL SOLUTIONS TO WORLD PROBLEMS.", WORLD FUTURE SOCIETY PUBLICATION, BETHESDA, MD. 1984.

HIGHLAND, HAROLD JOSEPH. "PROTECTING YOUR MICROCOMPUTER SYSTEM", WILEY PRESS, NEW JERSEY, 1984.

KOONTZ, DEAN R. NIGHT HAWK, BERKLEY PUBLISHING, NEW YORK, 1985.

LIEBS, SCOTT. "JUDGMENT DAY", INFORMATION WEEK MAGAZINE, MAY 7, 1990.

MOULTON, ROLF T. "COMPUTER SECURITY HANDBOOK: STRATEGIES AND TECHNIQUES FOR PREVENTING LOSS OR THEFT", PRENTICE-HALL PUBLISHERS, NEW YORK, 1986.

STOLL, CLIFFORD. "THE CUCKOO'S EGG", DOUBLEDAY, NEW YORK, 1990.

APPENDIX A

MODIFIED CONVENTIONAL DELPHI PANEL

1. Program Analyst City of Los Angeles, CA
2. Information Services Manager, City of Brea, CA
3. Information Services Technician, City of Brea, CA
4. Instructor of Computer Programming, University of Idaho, ID
5. Systems Analyst, Jet Propulsion Laboratories, Pasadena, CA
6. Vice President of PRC Tiburon Users Group, Brea, CA
7. City Administrator, Yorba Linda, CA
8. Criminal Justice Instructor, Fullerton, CA
9. Special Investigator U.S. Treasury Department, Long Beach, CA
10. Computer Security Specialist, Security Pacific Bank, Brea, CA
11. Consultant Instructor at I.B.M., Chicago, Ill

APPENDIX B

TRENDS

1. Technology will continue to advance at or greater than speeds currently experienced.

2. Technology will continue to compete with social programs for public funds.

3. Municipal governments will be slow to respond to potential pitfalls of information exchanges.

4. Increased incidents of breaches in computer information systems will continue to focus public attention on the issue.

5. Fear of unnecessary governmental intrusion into private matters will cause legal challenges to hinder computer security efforts.

6. New and more advanced methods of providing security to computer systems will continue to become available.

7. Criminal elements will become increasingly able to penetrate, alter, obliterate or contaminate law enforcement information systems.

8. Municipal law enforcement agencies will become less and less able to cope with security breaches.

9. The trend to seek technological assistance and consultations with the private sector professionals will accelerate.

10. Joint information systems will continue to increase due to the economic feasibility of such ventures.

11. The need for law enforcement officers with higher educations, especially those who are computer literate, will be acute.

12. There will be a proliferation of P.C.s and home workers will have new and enhanced access to informational systems.

13. Law enforcements application of available technology will lag behind the innovative uses discovered by criminal elements.

APPENDIX C

EVENTS

1. Displaced or disgruntled employee sabotages a law enforcement information system.

2. Law enforcement computer systems suffer an attack by right or left wing extremist groups whose aim it is to disrupt or destroy information possessed by police agencies.

3. A municipal agency loses its information system and has failed to adequately back-up its computer files.

4. A natural disaster of county or state-wide proportions occurs destroying or temporarily disrupts an information systems.

5. A system is designed which is masked by an innocuous looking program and when it is used in any computer it captures the passwords and identifiers which grant access to the user's computer this information is then sent by mailbridge or modem to the system designer for their own clandestine use.

6. Organized crime puts a bounty on information contained in law enforcement computer records systems.

7. Sensitive or confidential information is obtained by tapping into a police agency's computer system and this information is used to perpetrate a crime.

8. Confidential information is revealed when an unauthorized intrusion into police records is made on an unsecured system and results in the person named in that information bringing a successful negligence action against the police department.

9. The American Civil Liberties Union brings an action requiring all governmental agencies to allow freedom of information to all computer records unless national security or the identity of a juvenile is at risk.

10. A voter's initiative is passed requiring both physical and program software security measures be provided on all governmental informational systems of a confidential nature.

11. It becomes more cost effective to secure information systems than to risk a suit for failure to do so.

APPENDIX D

MODIFIED POLICY DELPHI GROUP

1. Systems Analyst, Jet Propulsion Laboratories, Pasadena, CA
2. Information Services Analyst, Brea, CA
3. Computer Security Consultant, Security Pacific Bank, Brea, CA
4. Special Investigator U.S. Treasury Department, Long Beach, CA
5. Police Manager Los Angeles Police Department, Los Angeles, CA
6. Computer Program Consultant, Palos Verdes, CA

APPENDIX E

WOTS-UP GROUP

1. Police Manager Los Angeles Police Department, Los Angeles, CA
2. Computer Security Consultant, Security Pacific Bank, Brea, CA
3. Information Services Analyst, Brea, CA
4. Special Investigator U.S. Treasury Department, Long Beach, CA
5. Systems Analyst, Jet Propulsion Laboratories, Pasadena, CA