HIGH TECHNOLOGY CRIMES

LAW ENFORCEMENT'S

NEW CHALLENGE

by

Daryll Thomann

COMMAND COLLEGE CLASS XIV
PEACE OFFICER STANDARDS AND TRAINING (POST)

Sacramento, California
June 1992

Order# 14-0287

This Command College Independent Study Project is a FUTURES study of a particular emerging issue in law enforcement. Its purpose is NOT to predict the future, but rather to project a number of possible scenarios for strategic planning consideration.

Defining the future differs from analyzing the past because the future has not yet happened. In this project, useful alternatives have been formulated systematically so that the planner can respond to a range of possible future environments.

Managing the future means influencing the future--creating it, constraining it, adapting to it. A futures study points the way.

The views and conclusions expressed in this Command College project are those of the author and are not necessarily those of the Commission on Peace Officer Standards and Training (POST).

"The trouble with the future is that it
usually arrives before we're ready for it."
— Arnold H. Glasow

ACKNOWLEDGEMENTS

I would like to thank the Commission on Peace Officer Standards and Training for the opportunity to participate in the Command College.

Those that participated in all the groups, panels and discussions that contributed to the study.

To Dr. Dorothy Harris, for her patience, hospitality, and willingness to give her time during the preparation of this study.

To Chief Manuel E. Ortega, Captain James Robertson and the city of Placentia for providing the time and encouragement to complete the study.

Finally, a very special thanks to my fiance, Brenda, who gave encouragement all the way through the program and study project, and who gave up much of our time so that the study could be completed.

WHAT WILL BE THE STATUS OF THE MANAGEMENT OF THE INVESTIGATION OF COMPUTER CRIMES BY THE YEAR 2001?

by
DARYLL THOMANN
COMMAND COLLEGE CLASS XIV
PEACE OFFICER STANDARDS AND TRAINING (POST)
JUNE 1992

Executive Summary

SECTION ONE -- A FUTURES STUDY

The main issue of the study is: What will be the status of management of the investigation of computer crimes by the year 2001? Sub-issue questions are: (1) What will be the financial impact of investigation of computer crimes on the budget; (2) What will be the need for specialist personnel; (3) What will be the legal changes in investigation regarding federal vs. municipal responsibilities? Research revealed that computer-related crime is one of the most challenging problems facing American industry today. It is also one of the most serious crimes that law enforcement will face in the future as it continues to escalate at a dramatic rate. Expert panel groups and interviews provided insight into challenges facing managers in the future. Three of the more important issue-related Trends were forecast as follows: (1) Level of retention of expertise of investigation of computer crimes; (2) Level of specialized training for law enforcement; (3) Level of working/sharing relationship between law enforcement and the private sector. Events with a strong possibility of occurring and a substantial impact on the issue were forecast as (1) Significant event or major catastrophe which would cause public awareness and outrage; (2) Establishment of federal guidelines that would mandate federal involvement in computer crime investigations; (3) Law enforcement action resulting in "bad case" law. Three scenarios were developed from the forecasts. The normative scenario describes a desired and attainable situation in which establishment of computer crime investigation units are stressed and positive results are emphasized.

SECTION TWO -- A STRATEGIC PLAN

Using the normative scenario, a strategic plan is developed for Placentia, a southern California city, that could be used for other cities with populations around 50,000. Strengths, weaknesses, threats and opportunities are identified. Stakeholders, such as the Chief of Police, managers, POA, business community, City Manager and others are evaluated. Recommended policies include: establishment of a task-force to assess current and projected needs for managing computer crimes; encouragement of community input; and formation of a steering committee to implement the development of a computer crime investigation unit in phases over a four-to-five year period.

SECTION THREE -- TRANSITION MANAGEMENT

The current commitment of the critical mass stakeholders compared to the desired commitment to the strategy is evaluated. Critical mass stakeholders are the Chief of Police, management personnel, City Manager and the POA. Some negotiations with stakeholders will be necessary to overcome resistance and provide an acceptable framework for the program. The management structure is a strong project manager and steering committee. Implementation technologies including responsibility charting, instilling the vision, milestone recognition, and sharing of information, were offered as possible tools to help manage the change process.

SECTION FOUR -- CONCLUSIONS, RECOMMENDATIONS AND FUTURE IMPLICATIONS

The issue and sub-issue questions are answered.

Main Issue: The trend toward privatization will play an important part in determining who will do the majority of the investigation of computer crime. If law enforcement continues to be ill trained and lack proper expertise and equipment, corporations' confidence in their ability will continue to decline. A strategic plan for enforcement is crucial for public law enforcement to manage the future.

Sub-issue 1: The cost of training and equipment become less significant when prorated over the years of their usefulness and product life. The diverting of human resources from traditional duties to computer crime investigation will account for approximately eighty-five percent of the projected costs and will be influenced by the calls for service by victims of computer crime.

Sub-issue 2: Currently the need for specialized personnel is imperative. As technology advances at an ever increasing rate, specialized technology requirements for personnel will diminish, eventually being insignificant as computers become voice actuated.

Sub-issue 3: There is little support for the theory that federal legislation would be enacted to mandate more federal responsibility to investigate computer crime. It would be more likely that a high dollar figure would be required for federal involvement as the magnitude of crimes increase to a saturation point beyond what the federal authorities could handle.

Recommended actions include, but are not limited to: determination of level of commitment, from executive level, to be responsive to victims of computer-related crimes; encouragement of the use of computers and provision of more computers for daily functions to increase computer literacy; provide sufficient training for investigators to proficiently handle computer investigations; coordination of efforts with prosecuting agencies; establish computer crime unit when justified by service demands; and establishment of a regional computer crime task-force when needs exceed the ability of a majority of the local departments.

INTRODUCTION

A short background on computer crime issues, where we are now, and a glimpse at the future.

SECTION ONE: DEFINING THE FUTURE

What will influence the management of computer crime for law enforcement by the year 2001?

SECTION TWO: STRATEGIC PLAN

A strategic plan for managing computer crime by California Law Enforcement in general, and the city of Placentia in particular.

SECTION THREE: TRANSITION MANAGEMENT

"Getting from here to there" - Managing the transition from accidental management development to programmed management development.

SECTION FOUR: CONCLUSIONS, RECOMMENDATIONS AND FUTURE IMPLICATIONS

Today's reality, Tomorrow's Visions -- accepting the challenge.

CONTENTS

APPENDIXES

TABLES

GLOSSARY OF TECHNICAL TERMS

ARTIFICIAL INTELLIGENCE: The automation of human reasoning and senses.

ATM (Automatic Teller Machine): A device provided by banks for depositing and withdrawing money.

BULLETIN BOARD SYSTEMS (BBS): A computer accessible by telephone, used like a bulletin board to leave messages for others to see.

DATA BASE: A computer application program or set of programs that provides storage, retrieval, updating, management, and maintenance of one or more data bases.

DOWNLOAD: To transfer files from a remote computer system to the user's system.

HACKER: A person who views and uses computers as objects of exploration and exploitation.

HARDWARE: The computer and all related or attached machinery, such as mechanical, magnetic, electrical, and electronic devices, used in data processing.

LAPTOP COMPUTER: A microcomputer that folds into or is contained in an easily carried case about the size of an attache case.

LOGIC BOMB: Computer instructions residing in a computer (usually within a Trojan horse program) that, when executed, determines conditions or states of a computer system that facilitates or triggers the perpetration of an unintended act.

MODEM (MOdulator-DEModulator): A device that modulates and demodulates signals transmitted over data telecommunication facilities and that converts between analog and digital representation data. It functions between a digital computer and an analog communication circuit.

PALMTOP COMPUTER: A mini-micro computer that can be held and operated from the palm of your hand.

PC (Personal Computer): A microcomputer with enough memory, I/O devices, and processing capability to be used for small but complete applications and word processing.

PHONE PHREAK (also FREAK): A person who uses switched, dialed-access telephone services as objects for exploration and exploitation.

REMOTE PROCESSING: Data entry and partial or complete processing near the point of origin of a transaction. Remote processing systems typically edit and prepare data input before transmission to a central computer.

SALAMI TECHNIQUE: The unauthorized, covert process of taking small amounts (slices) of money or other numeric value items from many sources, in and with the aid of a computer.

SNAILDARTER: Someone who has the ability to alter or block your course of action.

SOFTWARE: A set of computer programs and procedures sometimes including associated documentation.

TRAP DOOR: A function, capability, or error in a computer program or equipment that facilitates compromise or unintended acts in a computer system.

TROJAN HORSE: Computer instructions secretly inserted in a computer program so that when it is executed, unintended acts are performed.

UPLOAD: Transferring data from a microcomputer or terminal to a mainframe.

VIRUS: A set of computer instructions that propagates copies or versions of itself into computer programs when it is executed.

INTRODUCTION

A LOOK AT THE FUTURE OF COMPUTER CRIME

WHAT WILL BE THE STATUS OF THE MANAGEMENT OF THE INVESTIGATION OF COMPUTER CRIMES BY THE YEAR 2001?

INTRODUCTION

Computer-related crime is one of the most challenging problems facing American industries today.[1] It is also one of the most serious crimes that law enforcement will face in the future[2] as it continues to escalate at a dramatic rate. Thus far very little detection has been made compared to the magnitude of the problem. What detection has taken place, unfortunately, has seldom resulted in prosecution.[3] If this problem is not addressed, computer-related crime will be a threat equal to the crack cocaine epidemic that engulfs this nation today.[4]

Most people are aware of hackers - those who surreptitiously enter computer systems to intentionally and maliciously destroy or steal data. However, the real concern is white-collar criminals, the insiders who have the confidence of management and then reward that confidence with fraud, embezzlement, larceny, and sometimes even sabotage.[5]

Issue Considerations:

Law enforcement administrators are concerned about computer-related crime for many reasons, not the least of which is monetary loss. No one really knows what the present losses are, but informed administrators do know the burden is staggering.[6] The FBI says computer crime is too new a field for the Bureau to have developed any meaningful statistics.[7]

The list of computer-related, white-collar crimes is almost endless. With the help of computers, these criminals are stealing money, property, and confidential information. Some employees are even setting up their own businesses using government or company computer time and equipment.[8]

Defining computer crime:

Computer crime today is any illegal act for which knowledge of computer technology is used to commit the offense.[9] The following chart summarizes the types of computer-related crimes now seen at State and local levels.

Categories of Computer Crime

Internal computer crimes
- Trojan horse
- Logic bombs
- Trap doors
- Viruses

Computer manipulation crimes
- Embezzlement
- Frauds

Hardware/software thefts
- Software piracy
- Thefts of computers
- Thefts of microprocessor chips
- Thefts of trade secrets

Telecommunication crimes
- Phone phreaking
- Hacking
- Illegal bulletin boards
- Misuse of telephone systems

Support of criminal enterprises
- Data bases to support drug distribution
- Data bases to keep records of client transactions
- Money laundering

Examining the issue:

Each day computers are becoming more and more user-friendly, which often means criminal-friendly. If law enforcement doesn't take aggressive action now, what will the situation be like in the year 2000 and beyond? A review of literature, coupled with a series of interviews, was used to seek answers to these and other related questions.

The objective of this paper is to prepare California law enforcement managers for the unique challenges presented by high-technology crimes. This will be accomplished by answering the issue question: **What Will Be The Status Of The Management Of The Investigation Of Computer Crimes By The Year 2001?** Three sub-issues related to the main issue have been selected for attention. These are:

- What will be the financial impact of investigating computer crimes on law enforcement budgets?
- What will be the need for specialist personnel?
- What will be the legal changes in investigation regarding federal vs. municipality responsibilities?

Financial impact of investigations:

The investigation of high-technology crimes should have a significant impact on police budgets because of the complexity of the cases. Estimates range from four months to a year for thorough investigations.[10] Such cases may extend into several jurisdictions and even into other states; often local telephone and long distance companies must be contacted for help. This help may be difficult to obtain when the company is not the victim and the request takes a long time to fulfill.

As law enforcement personnel become more proficient at investigating computer crime, the business community will be more likely to report more offenses. Certain economic factors (ie., large dollar losses recoverable if crime reports are filed to satisfy insurance claims) will increase the amount of reported crimes.

As the public confidence grows and the reported cases increase, so will the need and demands for more resources to investigate computer crimes. This will require diverting resources that are currently being used in more traditional law enforcement areas.

Obtaining technical expertise:
The experiences of criminal justice agencies now responding to the challenge of computer-related crimes demonstrate the importance of developing investigation and prosecution strategies before major cases are presented. When a computer-related offense is reported, an agency that has no plan for addressing computer-related offenses may seem unresponsive or incompetent due to its lack of knowledge about the crime. In the time it takes the agency to develop the requisite expertise, offenders may disappear or effectively disguise their criminal activities. Victims will be less likely to report in the future. A recent study found that less than twenty sites nationwide had staff available with the training and background necessary to prosecute computer-related crimes. Of those, fewer than half actually dedicated full-time staff members to these activities.[11]

Computer-related crimes can occur anywhere in the country, and they pose unique problems for criminal justice agencies. Most law enforcement and prosecuting agencies do not have staff with the specialized background and training to investigate and prosecute these offenses. Even many large agencies in cities with significant financial resources report that they are not yet organized to address the special challenges of computer crime.

On the other hand, some jurisdictions have developed promising approaches. A few agencies have established dedicated computer crime investigative units. Others assign these cases to an officer trained in conducting computer crime investigations. A number of jurisdictions have created associations and task forces to investigate and prevent computer crime.

Federal versus municipal responsibility issues:

The impact on local and state agencies who are required to conduct detailed investigations will obviously depend on the development of immediate response capabilities and referrals/assistance; without these, few local agencies will be capable of investigating computer crime and will be dependent on federal agency response. It is not expected that local and state agencies will want to rely on and defer to federal agencies because of various political and professional reasons. Nor is it envisioned that the federal government will put forth the necessary resources to develop an entirely federal response to computer crime.

One concern is the degree to which most local law enforcement agencies will remain dependent upon federal law enforcement for the application of such technology. While federal agencies may be able to provide assistance on a case by case basis - as they have traditionally - it is not altogether clear whether they can do so on a continuing basis, even if they viewed that proposition as desirable. That capability would likely require restructuring the nation's law enforcement agencies in ways that heretofore have been viewed as unacceptable by both the public and the law enforcement community.[12]

Scope of the study:

While the numbers are scarce, most experts seem to agree that the computer crime threat can only escalate as computer usage continues to increase. Yet the law enforcement community's response seems to be lagging.

Right now law enforcement is probably ten years ahead of some of the nightmares that are going to befall us, because we're not so totally computer-dependent yet. In 1990 there were 10 million micro-computers in the workplace, with estimates of 34 million by 1994.[13]

The use of computers for committing crime didn't happen, nor will it disappear, overnight. It is a difficult issue and a reality that must be challenged by law enforcement administrators in the future.

After identifying and discussing what is likely to influence law enforcement's investigation of computer crime in the future, this research will provide a management strategy to be used by law enforcement administrators and serve as a catalyst to provoke further study and thought on the issue of managing the investigation of computer crimes.

For ease of reading, the body of this report will be limited to a meaningful summary of the research findings. With few exceptions -- the research data, charts, and graphs have been placed in the appendix. Readers desiring to view that data may do so by turning to the specific appendix cited in the report or by referring to the listing of appendixes.

SECTION I

DEFINING THE FUTURE

The Scanning Process

The environmental scanning process consisted of three phases: a literature review, selected personal interviews, and individual analysis. That process supplied much of the data discussed in the introduction, and was also interpreted to select the sub-issues critical to developing and providing focus on the main issue. All of the scanning techniques contributed to the formation of a Futures Wheel (Appendix A) which depicts the various relationships surrounding the issue and sub-issues. For those who wish to review the specific information, a bibliography of literature reviewed is contained in Appendix B and persons interviewed are listed in Appendix C.

Once data gathering was completed, a substantial amount of information was compiled and analyzed as to its relevance to the issues. Thus, insight was gained in refining and understanding the data, so as to begin to develop trends and events.

Nominal Group Technique (NGT)

A panel was assembled to assist in developing trends and events relevant to the issue. The panel was comprised of seven selected participants in and out of law enforcement, all of whom possessed some level of expertise and degree of familiarity with the subject of the research. (Refer to Appendix E for the group profile). That panel developed candidate lists of 25 trends and 13 events (refer to Appendix F and G). The panel ultimately distilled these lists down to five trends and five events that bear significantly on the study issue.

Identification and Definition of Trends

Trend 1 - Level of Retention of Expertise for Investigation of Computer Crimes: This trend focuses on law enforcement taking a critical look at retention of personnel in specialized assignments. Often, after providing special training to investigators, they are promoted or transferred to patrol where their investigative expertise and technical skills are not utilized.

Trend 2 - Level of Specialized Training for Law Enforcement: What level of training is being provided currently, and assessments of future needs to successfully interdict computer crime.

Trend 3 - Level of Allocation of Funds for Investigation of Computer Crimes: What commitment will management provide to finance and staff high-technology investigation units.

Trend 4 - Level of Use of Computer as Accessible Tools for Criminal Activity: This trend is defined as the volume of crime committed through the use of a computer.

Trend 5 - Level of Working/Sharing Relationships Between Law Enforcement and the Private Sector: The sharing of information, expertise, and resources as a practice acceptable by both sides.

Identification and Definition of Events

Event 1 - Significant Event or Major Catastrophe: An incident like a major system (financial, terrorist, or military) security breach which would cause public outrage and increased awareness of the magnitude of damage that can occur from computer literate criminals, focussing attention on more enforcement efforts.

Event 2 - Establishment of Specific Federal Guidelines Statutes for Computer Crimes Requiring Federal Involvement: Federal legislation or crime bill enactment that would remove the burden of investigating computer crime by state or municipal agencies by affixing the responsibility to federal agencies.

Event 3 - Establishment of a Centralized Investigation Agency: A Regionalization approach on a county basis is established, requiring municipal agencies to share the cost of funding and providing manpower for the investigation and enforcement of computer related crimes.

Event 4 - Passage of a Special Interest Initiative - Freedom of Information Act: This new legislation allows hackers the right to access systems to obtain information.

Event 5 - Law Enforcement Actions Resulting in "Bad Case" Law: Bad searches/seizures during computer crime investigation that would hamper or restrict law enforcements' ability to investigate and enforce computer crimes.

Trends

The same panel, using their own expertise and opinions, were asked to use a ratio scale to forecast trend levels. Today's value (the present) was equal to 100. An estimate equal to today would be 100, less than today would be less than 100, and greater than today would be more than 100. The forecast included past estimates (five years ago), and both nominal and normative estimates for the future (five and ten years from now). Table 1 depicts the results of the NGT panel's trend forecast (using panel median values). Graphs of trend levels are contained in Appendix H.

Table 1
TREND EVALUATION

		LEVEL OF THE TREND ** (TODAY = 100)			
TREND #		FIVE YEARS AGO	TODAY	* FIVE YEARS FROM NOW	* TEN YEARS FROM NOW
1	RETENTION OF EXPERTISE BY LAW ENFORCEMENT	23	100	175 550	250 800
2	LEVEL OF SPECIALIZED TRAINING	10	100	250 650	300 800
3	LEVEL OF ALLOCATION OF FUNDS	18	100	150 400	250 500
4	COMPUTER AS ACCESSIBLE TOOLS FOR CRIMINALS	25	100	300 150	700 200
5	WORKING/SHARING RELATIONSHIP BETWEEN LAW ENFORCEMENT AND PRIVATE SECTOR	18	100	250 600	300 800

** PANEL MEDIANS N=7

* FIVE YEARS FROM NOW "WILL BE"/"SHOULD BE"

* TEN YEARS FROM NOW "WILL BE"/"SHOULD BE"

The following is a brief analysis of the panel evaluation of the trends:

Trend 1 - Level of Retention of Expertise for Investigation of Computer Crimes: The table shows general agreement that the forecasted trend will increase over the next ten years. The greatest variation is seen between the nominal and normative forecast. The "should be" (normative forecast) was substantially higher than the "will be" (nominal forecast) based on some panelists' assumptions that law enforcement will not be able to handle the magnitude and complexity of computer crimes, especially if it does not address retention in assignment problems associated with its current promotional process. The divergence between the high and median forecast is explained by the difference in background of the panelist involved. The majority of the panelists were grouped around the median forecast.

Trend 2 - Level of Specialized Training for Law Enforcement: Computer training for law enforcement according to the panel has had considerable change and will continue. However, most panelists felt that it was far below where it should be, as indicated by the normative forecast. The majority of the panelists were grouped around the median score. The panel did feel that a majority of the change has occurred over the past five years, most of which was towards the later of this time period. They felt this recent surge indicates that a need has been identified and as the trend increases, computer crimes investigations may become more efficient. The panelists were not very optimistic about this as indicated by the high variation between the nominal and normative forecasts.

Trend 3 - Level of Allocation of Funds for Investigation of Computer Crimes: The panel felt that if law enforcement was going to be effective in investigating computer crimes that it would take a major commitment of resources and funds. According to their forecasts, there has been a constant rise in this trend over the past five years. The panel median indicates a slight increase of this trend over the next five and ten years. The majority of the panelists ratings were clustered between the high and median forecasts. Only slight variation is seen between the nominal and normative forecast. This may indicate that the panel felt confident that the future will be managed well.

Trend 4 - Level of use of Computers as Accessible Tools for Criminal Activity: This trend was rated by the panel to have the overall most significant median increases over the fifteen year period. This was the only trend picked by the panel with a "should be" (nominal) projection lower than the "will be" (normative). The great disparity in the median and low score was attributed to one panelist as the majority of the forecasts were clustered around the median nominal forecast. Both the nominal and normative forecasts indicate a significant increase in the panel's high and median predictions.

Trend 5 - Level of Working/Sharing Relationship Between Law Enforcement and the Private Sector: This relationship is felt to be crucial for law enforcement which is far behind the private sector in the area of expertise and available resources for investigating computer-related crime. Generally law enforcement has viewed the privatization of police service as being inferior and less professional, and has failed to give proper acknowledgement and recognition even when deserved. This is not the case with computer crime investigation, which in fact is just the opposite. For a change, law enforcement will be the pursuer of establishing a working relationship with private agencies and corporations involved in computer-related investigations. The panel was somewhat divided and possibly biased in their forecasts as to the feasibility of a shared working relationship. Those of the panel that had a high level of need for additional resources were clustered closer to the high forecast. The three panelists from the private sector had a significantly closer forecast between their nominal and normative predictions, and one's forecasts were the same for his normative and nominal forecasts, which could be indicative of the private sector's view of this trend.

Events

The NGT panel also forecasted the five events. The group rated each event by probability of occurrence (0 to 100 percent) for five and ten years from now.

In addition to this information, the group also listed years until the probability first exceeds zero, and the positive and negative impact of the event on the issue. Table 2 depicts the results, using the panel medians of the events forecasted. Graphs of the events are contained in Appendix I.

Table 2
EVENT EVALUATION

EVENT #	EVENT STATEMENT (ABBREVIATED)	* YEARS UNTIL PROBABILITY FIRST EXCEEDS ZERO	PROBABILITY		IMPACT ON THE ISSUE AREA IF THE ISSUE OCCURRED	
			FIVE YEARS FROM NOW (0-100)	TEN YEARS FROM NOW (0)-100)	POSITIVE (0)-10)	NEGATIVE (0-10)
1	SIGNIFICANT EVENT (MAJOR CATASTROPHE)	1	55	75	9	2
2	FEDERAL CHANGE FOR ENFORCEMENT	3	25	50	8	3
3	ESTABLISHMENT OF CENTRALIZED INVESTIGATION	4	25	50	7	1
4	SPECIAL INTEREST INITIATIVE (FREEDOM OF INFORMATION)	2	55	65	0	9
5	LAW ENFORCEMENT ACTION RESULTING IN "BAD CASE LAW"	1	70	85	0	8

* PANELS MEDIANS N=7

The following is a brief analysis of the panel's evaluation of the events:

With the exception of events two and three, all showed a strong degree of probable occurrence with significant impacts on the issues being studied. Events two and three, though given only a fifty percent probability of occurring or not, also proved to significantly impact the issue.

Event 1 - Significant Event or Major Catastrophe: The graph indicates that a significant event (major catastrophe) has a very high probability of occurring. The low forecast stated a twenty-five percent chance of occurrence by the fifth year, with the high forecast predicting seventy percent by the fifth year. The panel median suggests a fifty-five percent chance by year five, while all increased approximately an additional twenty percent by year ten. The panel agreed that there would be both positive and negative impacts. Discussion revealed that the positive impact would be derived from the realization by law enforcement management that computer crimes should receive more emphasis and a higher priority attention. The negative impacts were related to the potential financial loss to those victimized.

Event 2 - Establishment of Specific Federal Guidelines for Law Enforcement Requiring Federal Involvement in Computer Crimes: This graph indicates the probability of Federal Statutes being enacted that would mandate current state violations for federal responsibility. The probability of this occurring was not very high. For year ten, the low forecast was a twenty percent chance of occurrence. The panel median and the high forecast were significantly higher but were only given a fifty and sixty percent chance of occurrence respectively by year ten. The panel saw both a positive and negative potential with this event. The panel felt if municipal law enforcement had a choice, they would rather see more responsibility going to the federal government who they felt had more resources to deal with computer crimes.

Event 3 - Establishment of a Centralized Investigation Agency: This graph indicates that the establishment of centralized investigation units has only twenty-five percent chance of occurring as shown by their median forecasts for the first five years, and a fifty percent probability for the ten-year time line. The panel viewed this with mixed emotion, they saw this as a viable alternative for smaller municipal agencies such as Placentia, but highly unlikely for larger police agencies. The low forecast did not exceed the probability of zero until year two, and leveled out to a fifteen percent probability for the five and ten year time lines. The high forecast time line did not start until the fifth year where it was given a forty-five percent chance of occurring and sixty percent by the ten-year time line. The majority of the panel felt this would have a high positive impact.

Event 4 - A Special Interest Initiative is Passed - Freedom of Information Act: The graph on the probability of a special interest initiative (freedom of information act) occurring shows a high degree of divergence between the high and low forecast for the five-and ten-year time line. The panel medians for both time lines forecast only a fifty-fifty chance of occurring by year five, and a sixty-five percent by the tenth year. All agreed that should this occur, the positive impacts would far outweigh the negative. The panelists felt that should such an event occur, law enforcement would be less impacted as some of the current violations would be decriminalized.

Event 5 - Law Enforcement Actions Resulting in "Bad Case" Law: The graph on a law enforcement action resulting in "bad case" law, shows a strong probability of occurrence as early as the fourth year where the high forecast exceeds the sixty percent probability, and continues to escalate to ninety percent at the five year line and ninety five percent by the tenth year. The median forecast aligns just slightly below the high, with a eighty-five percent chance of occurring by the ten-year time line. All the panel agreed that if this should occur, the impact would be very strong and negative.

Cross Impact Analysis

The researcher and two associates performed a cross impact analysis. The purpose of a cross impact analysis is to assess how each forecasted event, if it occurred, would impact the other events and the trends. The results show which events are actors (greatest impact upon the other events and the trends) and which events and trends were reactors (most impacted by the events). The results are helpful in selecting trends and events to develop scenarios of the future. Table 3 depicts median scores.

Table 3
CROSS-IMPACT EVALUATION

MATRIX

(PANEL MEDIANS, N=3) MEDIUM IMPACT (% CHANGE + OR -)

**	E1	E2	E3	E4	E5	T1	T2	T3	T4	T5	"Impact Totals"
E1	X	-15	+15	+ 5	0	+15	+10	+30	0	+30	7
E2	-15	X	-20	+20	+10	+25	+10	+20	0	+15	8
E3	+10	-15	X	-5	+15	+20	+20	+15	0	+15	8
E4	-10	0	-10	X	0	0	- 5	- 5	-20	0	5
E5	+10	+10	+15	0	X	+10	+15	+10	+10	+ 5	8

"Impacted" Totals

E1	E2	E3	E4	E5	T1	T2	T3	T4	T5
4	3	4	3	2	4	5	5	2	4

** LEGEND

E1	SIGNIFICANT EVENT (CATASTROPHE)	T1	RETENTION OF EXPERTISE BY LAW ENFORCEMENT
E2	FEDERAL STATUTE FOR ENFORCEMENT	T2	LEVEL OF SPECIALIZED TRAINING
E3	ESTABLISHMENT OF CENTRALIZED INVESTIGATION AGENCY	T3	LEVEL OF ALLOCATION OF FUNDS
E4	SPECIAL INTEREST INITIATIVE (FREEDOM OF INFORMATION)	T4	COMPUTERS AS ACCESSIBLE TOOLS FOR CRIMINALS
E5	LAW ENFORCEMENT ACTION RESULTING IN "BAD CASE" LAW	T5	WORKING SHARING RELATIONSHIP BETWEEN LAW ENFORCEMENT AND PRIVATE SECTOR

Actor events should be the focus of policy action. By evaluating how each actor event affected the other events and trends, policies can be directed with the objective of making the event more likely or less likely to occur.

The following is a brief interpretation of the cross impact analysis:

Event 1 - Significant Event or Major Catastrophe: This was identified as an actor event and has the impact of increasing the probability of three of the other four events and four of the five trends. The probability of developing a closer working relationship with the private sector and allocation of funds to enhance computer crime investigations are both significantly enhanced. Law enforcement would view this event as negative, but it would instantly highlight the vulnerability of computer security. Political pressure and funding would be focused immediately to minimize further incidents and losses.

Event 2 - Establishment of Specific Federal Guideline Statutes for Computer Crimes Requiring Federal Involvement: An actor event, this would impact all the other events and four of the trends, increasing their probabilities. Should this event materialize it would minimize the impact on municipal and state enforcement agencies. Federal government would be required to take on more responsibility in the area of computer-related crime enforcement. Most panelists believed that if the reverse took place, local law enforcement would be drastically impacted, taking years to successfully meet the new demands.

Event 3 - Establishment of a Centralized Investigation Agency: This event would have a slight potential of decreasing the probability of the remaining events, especially if the idea became widespread and acted in a proactive capacity instead of reactive. It would impact four of the five trends which would all be enhanced significantly by the development and momentum that would occur with the implementation of a centralized investigation unit.

Event 4 - Special Interest Initiative is Passed - Freedom of Information Act: The occurrences of this event would decriminalize certain acts which are currently unlawful. Should it happen, two events and three trends could be less impacted as it would reduce the need to investigate acts that are presently illegal. Hardest hit was (T4), however this reduction would not be viewed as significantly favorable, as there would be no real reduction in accessibility. This change would be brought about by simple changing the current laws which protect copyrights, and public air waves. This will become a more complicated issue in the future, as cellular modems become common place in the business industry.

Event 5 - Law Enforcement Action Resulting in "Bad Case" Law: The occurrence of this event increased the probability of three events and five trends. There is little doubt that this event will occur, the real concern is to what degree and how often. As defense attorneys become more familiar with computer crime court tactics, they will also find new ways to suppress evidence and to defend their clients. On a more positive note, with the exception of (T4), increases in the trends would work at reducing the magnitude and occurrences of (E5).

SCENARIOS

The final segment section is the development of alternative scenarios - a glimpse into possible futures - based on the Trends and Events forecasts. The purpose of scenarios is that of providing planners with some windows into the future.

The three forecasting scenarios presented are Exploratory (nominal or "surprise free"); the Hypothetical ("what if"); and the Normative ("desired and attainable").

Exploratory (Nominal) Scenario

PRESIDENTIAL ELECTION OVERTURNED - ACTIVIST GROUP ADMITS COMPUTER RESULTS MANIPULATION, Orange County Register, November 1, 1996

STATE REPORTS COMPUTER CRIMES UP 40 PERCENT IN TWO YEARS, PLACENTIA EVEN HIGHER, Placentia Weekly News, June 5, 1997

Remember back in 1991, when everyone started to recognize for the first time, that computer crimes was an emerging issue for law enforcement? With new technology and mass production, computers were affordable to the majority of the population. Unfortunately not all of the computers were used for lawful purposes. As usual, all law enforcement in general did was simply "just talk about it." Due to the complexity of the crimes, and the insignificant amount reported to the police, most agencies failed to address the problem, even though the financial impact to those victimized was often astronomical.

Only one police agency in Orange County had an investigator working full time in the computer crime field. There were only three schools that provided any type of significant training for law enforcement, none of which were located in California. Several police agencies in Orange County sent a few investigators for training, but there was no real focus or commitment by their agencies. They were often promoted or transferred to other assignments where their knowledge on computer crimes was of no value.

Many agencies were facing budget cuts due to the recession, and revenue shortfalls. Positions were not being filled and programs were being cut. The more visible crimes received priority and computer crimes were put on the back shelf.

Most municipal law enforcement agencies felt that computer crime was a problem better handled at a County, State, or Federal Level. Most county and state agencies lacked the resources or experience to investigate these crimes; therefore, relied on the F.B.I. to cope with the problem. Unfortunately, the F.B.I., plagued with an increase of computer based crimes, would not investigate offenses where the loss was less than one million dollars.

The recent presidential election results, manipulated through unauthorized access by left wing activists, has drastically disrupted our government. The estimated costs to untangle the damage or conduct another election are staggering, and will leave future election results questionable as to their authenticity.

It's the turn of the century and the Placentia Police Department, like the majority of Orange County police agencies' still does not investigate computer crimes. Three more national banks failed this year due to the losses from untraceable electronic computer fund transfers. Computer crime losses have risen from $3 - $5 billion in 1990, to an estimated $12 - $15 billion this year (2000), according to the F.B.I. statistics.

Hypothetical Scenario

POST MANDATES COMPUTER CRIME TRAINING, PORAC News, December 3, 1995

STATE OFFICIALS STUNNED, NEW FEDERAL LAW TO DUMP MAJORITY OF COMPUTER CRIMES TO LOCAL LEVEL, Los Angeles Times, September 22, 1997

ESCALATING COMPUTER CRIMES LOSSES CAUSING MANY PLACENTIA BUSINESSES TO MOVE ELSEWHERE, Placentia Weekly News, May 12, 1998

In retrospect, the past ten years have been quite eventful in the issue area. It probably began in 1993 when the California Police Chiefs and POST recognized the critical need for specialized training to combat the ever increasing number of computer crimes. This freed up state funds to develop the needed training, making it affordable for all municipal agencies, and a push was on to make computer crime investigation mandatory training for all municipal police agencies. Many, however, including Placentia, did not.

By late 1995, POST had decided that in order to keep abreast of the specialized training needs and spiraling computer crimes committed, it placed computer crime investigation courses in the "must complete" category for cities with populations over 50,000. The Placentia police managers were concerned over the issue but decided to ignore it, and continued to prioritize other areas. After all, the cities population was a few hundred under the cut off figure, even though they refuted the census report when it was to their advantage.

Most agencies were stunned in September 1997, when the federal government advocated to state and municipal law enforcement all computer crimes with a loss under one million dollars.

The City of Placentia was struck hard, as many business were complaining about moving their businesses out of the city. They felt their taxes were not being spent where it did them the most good, combating their computer crime losses. They were forced to expend additional funds to hire private investigation agencies. As the investigations were often lengthy and costly, they eventually did not investigate the loss, and would simply pass it on to the consumer. They began to lose customers because they could not remain competitive with businesses in bordering larger cities, who were more responsive to the business owners' plight.

The city once known as a "pleasant place to live," has lost its appeal and now it's known as a "place to leave."

Normative Scenario

PLACENTIA POLICE AND PRIVATE SECTOR JOIN HANDS TO COMBAT COMPUTER CRIMES, PORAC News, August 20, 1994

COMPUTER CRIME INVESTIGATION CLASS NOW OFFERED BY POST, PORAC News, July 1, 1995

CHIEF LAUDS STATE FUNDING PROGRAM FOR COMBATING COMPUTER CRIMES, Orange County Register, June 27, 1998

For the most part, the past ten years were good to the Placentia Police Department. Forward thinking had turned some potential harmful events into opportunities for improvement. In July, 1995, POST recognized the need for specialized training for computer crime investigation and started the first comprehensive training class. The City of Placentia took advantage of this training opportunity by sending an investigator to the first available session. The city started to focus it's efforts on computer crimes, a problem that was obviously going to have a significant impact on the city. This commitment was made in spite of budget problems at the time and pressure from local interest groups to place our resources elsewhere. Local corporations and businesses owners met with city officials to better understand each others capabilities and needs regarding computer crime and enforcement strategies.

The governor approved grant funds in 1998 to be used exclusively for establishing computer crime investigation units in municipal police agencies. A bill was passed legislating tougher sentences and fines for those convicted of using a computer during the commission of a crime.

In 1999 the Orange County Chiefs of Police Association, finally convinced that computer investigation resources were better spent by pooling them, formed a Regional High-Tech Task Force to handle the majority of the most complex computer crime cases.

The Placentia Police Department, in addition to its participation with the task force, trained its first investigator back in 1996 to handle some of the less sophisticated computer crimes that affected small local businesses.

Back in 1991 we thought we knew what was in store for us down the road. Had we not prepared we really would have been inundated today. We knew the emerging problem back then was going to have a significant impact on our department, and law enforcement in general, but we had no idea that we were only looking at the tip of the iceberg. We have not won the battle yet, but we have seen many promising changes in the past ten years in how law enforcement, the private sector, and the judicial system have worked together successfully toward a common goal.

SECTION II

STRATEGIC MANAGEMENT

Strategic planning is defined as: "A structured approach, sometimes rational and other times not, of bringing anticipations of an unknown future to bear on today's decisions."[13]

This portion of the paper outlines the structure and how anticipations bear on today's decisions. The strategic management plan will be based upon the normative scenario from Section I. The objective of this strategic management plan will be to help make that scenario become a reality.

Subject of Strategic Management Plan

The Placentia Police Department, like many medium-size municipal police agencies within the state, is faced with the problem of diminishing resources and increased demands for service. It is becoming necessary to do more with less.

Management of the Investigation of Computer Crimes is an issue that was critically examined through research analysis. The research focused on the impact of the issue as it relates to California law enforcement and similar agencies the size of Placentia. The research revealed that law enforcement will be faced with an increasing number of computer crimes that will require complex and time-consuming investigations. If the magnitude and complexity of this type of crime increases to the capacity predicted by many, law enforcement will be faced with some challenging decisions in order to effectively deal with the management of computer crimes. Some areas of concern are the development of expertise; retention in investigation assignments to retain and enhance skills; and adequate allocation of funds for computer crime enforcement.

Presented in the following pages is a strategic plan for managing computer crime. An evaluation of the current situation must be an integral part of any strategic plan. For this study, two situational processes were used. The first is the WOTS-UP

Analysis, an acronym for Weaknesses, Opportunities, Threats, Strengths - Underlying Planning, and second, the Strategic Assumption Surfacing Technique or SAST.

STRATEGIC PLAN

Mission Statement

In order to bring about focus to the plan, it is necessary to identify the ultimate goal related to the issue. This is best accomplished by developing a mission statement:

> The police department has the responsibility to participate in providing solutions to problems of controlling high-technology crimes, which threaten the economic stability of businesses in the community.
>
> The police department will provide service to all aspects of the community with sufficient resources to appropriately handle all criminal activity and important issues.

Situational Analysis

Managing computer crimes represents a tremendous challenge to law enforcement as the investigations require a level of expertise that most police departments currently do not possess. Law enforcement will be faced with lengthy investigations that often average between one to two years, and are complicated further with jurisdictional and geographical problems. The use of modems and cellular telephones further complicates law enforcements ability to identify suspects and successfully prosecute the perpetrators of computer crimes.

WOTS-UP Analysis

The first phase of this analysis was a scan for external and internal environmental factors that could impact the Placentia Police Department's ability to achieve the desired goal. This evaluation consists of two segments, an assessment of "opportunities-threats" in the external environment and a "strengths-weaknesses" review of internal conditions at PPD. An opportunity is any favorable condition or trend outside the department environment, and a threat is any unfavorable external situation or trend. Internal strengths are resources that could be used to achieve the desired objective, and weaknesses are conditions that would limit the ability to attain the goal. To obtain the information a group of five managers was assembled and a consensus was reached.

Environment

Opportunities: The area is rich in resources that could be used to maintain the normative scenario. High technology companies with global reputations abound. Several organizations, for example the High-Technology Crime Investigation Association with hundreds of members from private and public entities, are an endless resource. The city council is supportive of progressive law enforcement and the providing of adequate police services. POST has historically provided specialized investigative training based on the demands of police agencies to meet new challenges.

Threats: The unstable California economy and revenue short falls have made it harder to initiate new programs requiring additional personnel and expensive equipment. The increased calls for services and public concern relating to gang and narcotic enforcement is currently receiving an abnormal amount of attention. Resources are dwindling due to this politically sensitive issue and demands from special interest groups. Politicians are increasingly becoming involved in the day-to-day operations of the agency, which could hamper the flexibility of any program designed to reach the desired goal.

Organization Capability

Strengths: The department managers are a very dedicated and intelligent group, most of whom have completed or are currently involved in post graduate work. Placentia far exceeds the State's average for cities participating in POST training, especially in specialized investigative areas. PPD has traditionally been a trend setter in "special investigative units" in many areas that other cities of comparable size failed to address at the early stages of transitional problems. A majority of the field and investigative personnel possess basic computer skills. Several persons have developed outstanding skills in this area and are assisting others to enhance their skills.

Weaknesses: The current internal promotional structure does not lend itself to developing long-range expertise in specialty positions. Promotional opportunities exist in patrol only; therefore investigators promoted, no longer use their specialized investigative talents. Not all police personnel have the aptitude or desire to work the high-tech computer crimes and very little training is currently available. POST currently does not have any significant training in this field.

Other Factors: Currently, very few computer crimes are reported in the city of Placentia and this trend prevails throughout the state. Most businesses handle their computer problems internally or write off the loss to the consumers. They are reluctant to publicly acknowledge their vulnerability and losses for fear of losing clients or prospective customers. Most victims are aware of law enforcement's lack of expertise in this area and usually seek private investigative firms to proceed civilly for restitution, rather than criminally. This trend, if altered, could play a significant role in the demands for future law enforcement services.

Strategic Assumption Surfacing Technique (SAST)

A very important part of any strategic plan is the identification of those persons and groups or constituencies impacted by the issue question. These individuals or groups can be broken down into three sub-issues. They are: (1) those that are impacted by the policy or decision; (2) those that care about what you do and; (3) those that impact or control what you do. Collectively, these are known as "stakeholders." The goal of the SAST is to identify these stakeholders and attempt to clarify or make assumptions as to their position on the issue. The stakeholder identification and analysis of positions was accomplished by a group of three managers, all familiar with the agency, the issue, and local political climate.

Stakeholder Analysis

There are many people who have an interest in how the Placentia Police Department will manage criminal investigations in the future. Some of these "stakeholders" are concerned for economic reasons, while others seek to find a political advantage. Whatever the reason, these stakeholders share a common concern for insuring that their needs are met.

The following list represents only the principal identified stakeholders to the issue of law enforcement managing computer and positions believed to be held by the stakeholders in reference to the issue. For a complete list of all identified stakeholders to the issue and positions believed to be held, see Appendix J. For a graphic display of assumption position, the certainty of each assumption and their importance, see strategic assumption in Appendix K. An assumption is defined as a "basic, deep-rooted, often unstated values and beliefs that individuals or groups might have about the world."[14]

Chief of Police - The Chief will be Conceptually supportive of the issue; reviewing current and future investigative needs; however, must be convinced that gains exceed resource expenditures. Will want an effective monitoring system.

City Manager - The City Manager will support program that will improve employee morale; increase efficient use of resources, and satisfy the city council. May oppose the hiring of additional personnel and start-up costs of high-tech unit.

Administrative Division Commander - The Captain would be supportive when computer crime case load becomes an issue that needs to be addressed by the Detective Bureau which comes under his command. Might oppose if additional manpower is necessary and not addressed.

Placentia Police Officers Association - The POA Would be supportive of a high-tech crime investigation unit as it would allow additional lateral transfer ability. Could be concerned if they felt that developing the new unit would be at the cost of patrol strength, could become a morale issue. May seek to challenge current promotional practices. (Snaildarter)

Patrol Division Commander - Would be supportive if needs are apparent. Could be opposed if manpower becomes a problem, and positions are created at the expense of field patrol strength.

Alternative Strategies

A modified policy delphi process was used to identify alternative strategies. Five additional members were used to join the SAST group which then totaled eight. Each member generated a strategy to deal with the future of the issue. The generated alternative strategies allowed for an appropriate field of selection and enhanced chances of success. Eight strategies were selected for further analysis. The selection was made through the rating process and the choices were based on totals and polarization of scores. The policies were further reduced to four and are listed in order of ranking for a combination of desirability and feasibility. The four strategies were then reviewed for positive and negative factors and are contained in Appendix L.

Recommended Strategies

The pros and cons of each strategy were discussed as those strategies related to each stakeholder. Further, consideration was given to the risk connected with each. The group then rated the strategies and discussed the results. The strategy of choice emerged as a synthesis of strategy one and two for short range implementation, with strong recommendation to pursue the feasibility of strategy number three at a later date.

1. Restructure Crimes Property Unit to handle computer crimes.
2. M.O.U. between law enforcement and corporate businesses.
3. Establish Regional Task-Force to investigate computer crime.

Discussion and Justification

Analysis of the selected strategies revealed a polarization for strategy number three. Those in favor of the strategy felt that loss of local control could be a strong issue. All agreed that a county or regional task-force approach has many benefits, including possible federal involvement which would access certain information and investigation techniques (wire tapping) not available to state and municipal agencies. They felt, however, that this approach would not necessarily be able to address all local problems.

There was also strong agreement that law enforcement and corporate management should establish a better understanding of each others concerns and expectations. This could possibly be established through further pursuing strategy number two, which could enhance relationships regardless of how decided to proceed with criminal investigations and prosecution.

Furthermore, to implement any long-range management plan for computer crimes without addressing all potential victims needs would be an oversight, containing a high degree of risk and potential liability for the city. Most panelists agreed that narcotics enforcement strategies practiced today should be followed, in that, local departments should have the capability of handling the minor violations in-house, leaving the regional task-force to handle the more complicated multi-jurisdictional computer-related cases.

Those who opposed strategy number four, felt that the success of a long-range development plan must include key stakeholders external from the police department, as this was not solely an internal problem. Business owners and potential victims would be discouraged from prosecuting due to the financial obligation to do so. This would be viewed as double taxation by victims and would have no support from the business community.

Strategy number one represented the least risk and would be the easiest to implement. It could be set up with the least disruption and with the shortest lag time. The required expenditures of resources would be manageable and signal the commitment of the city to solve its own problems. Some panelists commented that this was more of a reactive stance or business-as-usual approach, incapable of handling the more complicated cases.

Strategy number three would be able to better address the long term needs of the county, as it would include many of the stakeholders who could ultimately decide in that direction, provide additional external resources, and assist with viable internal options. Strategy number four received a lot of discussion, however the final consensus was that the financial cost of the study and potential unrealistic outcome due to stakeholders not being involved in the planning strategy made this approach the least feasible.

Upon careful consideration of the four remaining strategies the delphi panel decided that a mixture of the first three strategies had the greatest potential for success, and would address all future needs. This could best be accomplished by forming a task-force to further review strategies and develop timetables for implementation.

Implementation Plan

The implementation of a stakeholder task-force strategy would require close cooperation. The depth of participation would be an indication of how important external stakeholders viewed the issue. Each one of the participants must be convinced that a task-force would be advantageous to their individual interests and not a threat to their sovereignty. This type of reassurance could best be accomplished by the Chief of Police as part of his overall proposal for the task-force concept.

The following action steps are necessary to operationalize the task force.

Part I

- o Chief of Police communicates the vision of an organizational structure that will support a proactive stance toward computer-related criminal investigations.
- o Chief of Police announces the creation of a task-force to analyze the impact on the community from computer crime.
- o Senior management staff solicits interested members from internal stakeholders to serve on task-force. Time line - two months.

Part II

- o Task-force meets to discuss objectives and establish procedures and time lines. As a result of this study, a "white paper" would be submitted to the task-force.
- o Task- force discusses and identifies external stakeholders to the issue.
- o Contact and discussion with appropriate key external stakeholders to the issue.

- Task-force conducts interviews and surveys business community to identify magnitude of computer-related crime and concerns of those victimized.

Part III

- Task-force analyzes collected data to determine current and projected needs for managing computer crimes.
- Task-force prepares recommendations as to nature of problem and suggested strategies to resolve issue.
- Task-force presents recommendations to Chief of Police and senior management staff. Time line - four months.

Part IV

- Implementation of selected recommendations.
- Evaluation of implementation strategy and progress. Time line - six months.

NEGOTIATING ACCEPTANCE OF THE STRATEGY

The key components of the task-force strategy are the participation of the stakeholders in the developmental process, and the resulting stakeholders "ownership" of the task-force's recommendations. These ingredients are vital to the success of the strategy and are therefore non-negotiable in accomplishing the mission. When dealing with a highly subjective issue such as police effectiveness, it is essential that all parties have complete "buy-in" to the process or the process is likely to fail.

There are components of this strategy, however, which are of lesser importance and are negotiable for the sake of accomplishing the mission. The selection of the actual task-force members, for example, is far less critical to the overall process then the concept of having stakeholders participate. The City management and the City Council may have strong preference as to who should be selected to serve on the task-force. In many cases, an appointment to the task-force may be considered to be a political plum or payback for past favors. This presents then a great opportunity for compromise without risk of losing the real strength of the task-force process.

All principal stakeholders negotiating positions including the snaildarter have been identified as:

Stakeholder's Position

City Management - Placentia's city management is concerned with two primary issues: 1) maintaining quality service to the community and 2) providing more service with less revenue. The city management would hold firm on the issue of controlling the task force. There are very few aspects of the strategy that city management would want to leave to chance.

Business Community - The business owners are beginning to realize the many ways they can be victimized by high-tech crimes, and that criminal prosecution and publicity can act as a deterrent. Since many companies through the Chamber of Commerce are just beginning to explore their political power and influence, it would be reasonable to assume that they would be flexible on most issues concerning the task-force. The one notable exception to this, however, would come from their position that would demand a high level of investigation expertise from the city, but retain the ability to seek civil or other remedies should the crime jeopardize their business or reputation.

POST - The technical training needed for an investigator to conduct a thorough and competent investigation that is necessary for high-tech computer crimes will be a challenging issue for POST. POST has not been very flexible in providing basic computer skill training, let alone comprehensive investigation training.

They recently dropped the basic computer training from their training calendar, even though this was identified by many police agencies as necessary basic technical skills for today's police officer. POST will hold firm in this area for financial or philosophical reasons. As responsive as POST has been historically to state training needs, they will probably become more flexible as the demand for computer training increases.

Police Officers Association - The Placentia POA is the snaildarter of the task-force strategy. The POA often views itself as an adversary of city management and is therefore constantly on the lookout for a political advantage. This places the POA in a very unpredictable position. If the POA goes along with the process, it may be seen as aligning itself with the same city management that it fights against during other issues critical to the POA. However, the POA would still want to participate in the process to protect their interest.

California Police Chiefs - If law enforcement eventually entertains the thought of using regional resources to handle the complexity of computer crimes, it will require more flexibility on their part to release some local control to a regional task-force. Most larger agencies will probably be less flexible in this approach if they feel they have sufficient resources to handle their problems internally. The majority of police agencies would be very flexible in this approach, especially if asset seizures would offset many of the operating costs.

Sheriffs' Department - The Sheriff would have little interest in what approach Placentia uses to handle crime problems within its own boundary. However, if a regional approach was feasible, the Sheriff probably would not be very flexible in relinquishing control for political reasons. The Sheriffs' department currently has the only full time computer crime investigation unit in the county, which would fortify his position for power.

District Attorney - The District Attorney would be supportive of any advance professionalism of police services within Placentia. Like the Sheriffs' Department, they would provide technical assistance and prosecution when requested. The District Attorney would probably want to be an intricate part of any regionalization approach for professional and political reasons.

NEGOTIATING STRATEGY

The most desirable negotiating strategy is one in which all parties receive a mutual gain from participation in the process. This is especially difficult to achieve when dealing with the highly subjective ideals and the value-laden concepts surrounding the issue of police management. It is therefore critically important that negotiating leverage be obtained through a win-win scenario that emphasizes the common interests of the participants.

City Management - A rational information-based approach is most likely to influence city management. The police department is not in any position to use power as negotiating leverage with city management, and psychological influence seems to have little effect on bureaucrats. Anything that might upset the norm may be viewed as threatening to the existing power structure and is, therefore, undesirable.

Business Community - Placentia businesses are relatively new to the power and influence scene. They have become more active in Chamber of Commerce activity and Neighborhood/Business Watch Programs. Although their first priority is financial gain, they also are interested in protecting and preserving their business establishments and are unlikely to compromise. Consequently, they would most likely be responsive to a negotiating strategy which is a form of psychological influence as the primary negotiating leverage. If an appeal is made to their fiscal management concerns and they can be given assurance that the department's goal is the same as their goal, a mutual gain relationship can be established.

POST - Being associated with the education system, POST is accustomed to dealing with data and information. They also have many bosses to answer to who are influenced by politics. Being realistic, the city of Placentia alone has no leverage. It would take political influence brought to bear by police and city organizations that share the same concerns as the city of Placentia to provide the necessary leverage. These factors may indicate that POST would be more receptive to information-based rationality as negotiating leverage.

Police Officers Association - The Placentia POA is truly the snaildarter of the stakeholders. Their position on the issue is unclear which makes their behavior unpredictable. Because of their unique position in this process they are candidates for all three types of negotiating leverage. The first approach would be to attempt to influence them through rational leverage using the argument that their participation would benefit both the department and the city. If this proves unsuccessful, a psychological approach could be used stressing the importance of their participating as their duty to the community. If both strategies fail, they may be persuaded by power to participate.

California Police Chiefs - The California Police Chiefs would be most responsive to information-based rationality as a negotiating leverage. If an appeal is made to the rational side of their concerns and a mutual gain relationship is established, they be may convinced that our goals are all the same.

Sheriffs' Department - Allowing the Sheriffs' Department to coordinate the regional computer crime task-force would probably be the only way to gain their acceptance. The political power base to finance such an operation county wide could hinge on their involvement. They would negotiate strongly that the size of their agency, available resources and established contacts, make them the logical choice.

District Attorney Office - There is a strong chance of a power struggle developing for control of any regional approach between the District Attorney and Sheriffs' Department. The chiefs of police might have to use their influence to minimize issues that might arise between the two.

SECTION III

TRANSITION MANAGEMENT

PURPOSE

A strategic plan was developed and included negotiating strategies necessary for gaining stakeholder commitment. Actual implementation of a plan to manage computer crime investigations would require a transition management plan. Transition allows for identification of the critical parties who may in some way influence the plan. Furthermore, the degree of commitment of the "critical mass" may be accessed and adjusted, creating an environment conducive to change. A plan for transition management will bring life to the strategic plan and is contained in the following pages.

COMMITMENT STRATEGY

Critical to implementing the strategic plan is the process of "getting from here to there," or moving from the current state to the desired state. The success, or failure, of the change process depends on how well the transition process is managed.[15] A transition management plan must be designed for the unique environment of each individual organization. This section consists of three distinct but interdependent parts. First, those persons necessary to make the change begin are identified, their current commitment state is analyzed, and ways to build or change commitment are suggested. Next, the structure(s) necessary to manage the change effectively are identified. Finally, methods and tools to minimize the negative impact of change on the organization are suggested.

Among the stakeholders identified in the Strategic Plan were several "actors" that must commit to the plan to make change happen. These "actors" and additional stakeholders within the organization form a "critical mass" group. If the stakeholders in this critical mass support the plan it is likely to succeed, and if they oppose it, the plan is likely to fail. A consensus group consisting of three managers identified these critical mass actors, and agreed on the current commitment and needed commitment of the critical mass group. These critical mass actors are:

- o Chief of Police
- o City Manager
- o Adm. Div. Comdr.
- o PPOA President
- o Patrol Div. Comdr.

The level of current individual commitment and the commitment necessary to make the change occur are shown on the following Commitment Chart.

CRITICAL MASS COMMITMENT PLANNING CHART

Table 4

Key Players	Block Change	Let Change Happen	Help Change Happen	Make Change Happen
1. Chief of Police			X 0	
2. City Manager		X ——	—> 0	
3. Adm. Div. Comdr.			X ——	—> 0
4. PPOA President	X ——	—> 0		
5. Patrol Div. Comdr.		X ——	—> 0	

X = Current Commitment 0 = Needed Commitment

The following evaluation of current individual commitment include recommendations for approaching members of the critical mass to achieve the desired commitment level.

Placentia Chief of Police: The Chief must be convinced that the benefits of implementing the strategy will outweigh the expenditures in resources. To keep the Chief in the "help change happen" category, will require a united effort of management and supervisory personnel. They should stress that it would not only benefit the department but the community. The Chief must be willing to negotiate on the form and structure of the department in order to facilitate the implementation of the strategy.

Placentia City Manager: The City Manager's current position on the strategy coincides with that of the Chief due to a desire to support the Chief. If the Chief were to change commitment, the City Manager would follow suit, as he has no personal resistance to the strategy. The City Manager must be assured that the resources are available, that the city will benefit from the program, and that those involved as key stakeholders support the strategy. These assurances can be provided by the Chief.

Administrative Division Commander: The transition manager is the administrative division commander. He will have complete responsibility for "making the change happen," as the detective bureau is under his command which makes him the logical choice. This will include bringing together personnel and other resources. He will facilitate all required activities in order to realize the desired future, and furnish feedback to all concerned parties.

PPOA President: The Placentia Police Officers Association is the snaildarter of the task force strategy. The PPOA often views itself as an adversary of both city and police management and is constantly on the watch for political advantage. This makes PPOA behavior very unpredictable and a potential adversary. The PPOA President's political role is to scan all issues looking for political advantage and benefits for its general membership.

The PPOA generally would be highly skeptical of any change within the organization. However, they would want to be involved in any task force process to insure that the PPOA's best interest is served. The PPOA president's support is not vital to the process, however, his disapproval would be difficult to overcome. If the issue is deemed to be in the best interest of the PPOA they would probably assume a "let it happen" posture. This could easily change to "block change," if they somehow felt it was not in their better interest.

Patrol Division Commander: The Patrol Division Commander has the potential of blocking any transfer of resources that would be at the expense of his division. The department has a history of creating new positions and staffing it with personnel from the patrol division. In recent years the overall size of the agency has increased, and many new specialty positions have been created, however, the patrol strength remains at the same critical level that it was ten years ago.

The Patrol Division Commander must be convinced that any reorganization would not necessarily be at his divisions expense. Any long range planning without his involvement could potentially change his "let change happen" stance to one of "block change," if he felt his division's ability was going to be jeopardized by loss of additional manpower. He could easily be persuaded to "help change happen," if he had equal representation on future decision making affecting the department in this area.

TRANSITION MANAGEMENT STRUCTURE

The Administrative Division Commander was selected to manage this change. The chief of police has ultimate responsibility and authority. However, the time and energy required to make the transition will not allow the chief to oversee the change himself. Instead he will temporarily grant executive responsibility and authority to the transition manager. This structure would be the most effective because of the nature of change, the transition managers relationship to key individuals, and his enthusiasm for the project. The transition manager or "project manager" is in the best position to integrate the change and is willing to take the responsibility of implementation.

The project manager will facilitate all required policy formation involving the chief of police, city manager, and the employees. This will insure proper input and build a cohesive work group. He will chair the task-force made up of key stakeholders to assess current and future needs, and develop a long-range plan for managing computer crimes. The project manager will routinely provide feedback to all the critical mass and publish progress reports.

IMPLEMENTATION TECHNOLOGIES

It is generally understood that resistance is a part of most change. People become comfortable with what they know and fear what they don't know. The uncertainty is sure to produce anxiety. It is essential that methods and technologies are used to deal with the anxieties of change so that the desired future may be realized.[16]

Responsibility Charting

Responsibility charting will be done to help assess alternative behaviors for each party during the entire change process. This will clarify the behaviors that are required in order to affect the desired changes. Furthermore, this activity will promote team building since responsibility charting is a group effort. The process requires the anonymous consensus of the group for the required behavior of each party. The behaviors are plotted and include: (R) Responsibility (this indicates the designated individual has responsibility for a particular action); (A) Approval (the individual need only approve and has the power to veto); (S) Support (the individual must in some way support but does not have to agree); (I) Inform (the individual must be advised of intended action before it is taken). The Responsibility Chart is found in Appendix M.

The key to the transition process is communication and participation by those within the organization. The following management technologies have been selected for implementing the change.

Creating a Vision of the Future: In order to create a vision of the future, all those involved must be able to let go of the past. They may be given the opportunity to do that if the leadership communicates to everyone affected what the future will be like. If they can see it in their own minds, the change becomes less threatening. They will be confident that they can manage the future if they believe they know it.

Action Plans: Developing clear action plans that embody future goals will keep the proposed change on course and give the work group certain direction. Each step should include action plans and this activity should commence at the very beginning.

Team Building: The change will only be successful if those people involved are committed to the new method of performing work. This is especially true for those who will be doing the work. They must be involved in policy formation and action planning. This will be accomplished by open communication with shared authority and responsibility. The result will allow for flexibility and motivate the group to move ahead because they share in the outcomes.

Stakeholders Surveys: This is the device that is used to keep the transition manager in close contact with the stake holders. It also serves to promote communication in all directions. This may lead to affiliations between stakeholders which would not otherwise exist. Furthermore, problems may surface that were not anticipated and that need to be addressed.

Midpoint Scenario: The transition manager shall complete a midpoint scenario of what the half-way point will be like. This scenario will provide a useful measure and future guide for action. The scenario is used for a progress marker, and will help the work groups adapt as necessary.

Progress/Evaluation Reports: Written progress reports will be prepared at regular intervals. The reports will be used to give feedback to city manager and chief of police. The progress reports will also be shared with all department members and will evaluate and recognize the efforts of the task-force.

Celebrate Milestones: The project will plan to celebrate milestones of accomplishment. During the transition, several achievements will be recognized. The events will be preplanned and will serve to keep focus on the project while building enthusiasm.

SUMMARY

The purpose of transitional management is to give life to the strategic plan. That is a simple statement that represents a monumental task. The goal of transitional management is to create an environment that embraces change by minimizing the negative effects of the change. If done properly, the stakeholders will realize that their concerns have been addressed and the desired future will be realized.

SECTION III

TRANSITION MANAGEMENT

PURPOSE

A strategic plan was developed and included negotiating strategies necessary for gaining stakeholder commitment. Actual implementation of a plan to manage computer crime investigations would require a transition management plan. Transition allows for identification of the critical parties who may in some way influence the plan. Furthermore, the degree of commitment of the "critical mass" may be accessed and adjusted, creating an environment conducive to change. A plan for transition management will bring life to the strategic plan and is contained in the following pages.

COMMITMENT STRATEGY

Critical to implementing the strategic plan is the process of "getting from here to there," or moving from the current state to the desired state. The success, or failure, of the change process depends on how well the transition process is managed.[15] A transition management plan must be designed for the unique environment of each individual organization. This section consists of three distinct but interdependent parts. First, those persons necessary to make the change begin are identified, their current commitment state is analyzed, and ways to build or change commitment are suggested. Next, the structure(s) necessary to manage the change effectively are identified. Finally, methods and tools to minimize the negative impact of change on the organization are suggested.

Among the stakeholders identified in the Strategic Plan were several "actors" that must commit to the plan to make change happen. These "actors" and additional stakeholders within the organization form a "critical mass" group. If the stakeholders in this critical mass support the plan it is likely to succeed, and if they oppose it, the plan is likely to fail. A consensus group consisting of three managers identified these critical mass actors, and agreed on the current commitment and needed commitment of the critical mass group. These critical mass actors are:

- Chief of Police
- City Manager
- Adm. Div. Comdr.
- PPOA President
- Patrol Div. Comdr.

The level of current individual commitment and the commitment necessary to make the change occur are shown on the following Commitment Chart.

CRITICAL MASS COMMITMENT PLANNING CHART

Table 4

Key Players	Block Change	Let Change Happen	Help Change Happen	Make Change Happen
1. Chief of Police			X O	
2. City Manager		X —	—> O	
3. Adm. Div. Comdr.			X —	—> O
4. PPOA President	X —	—> O		
5. Patrol Div. Comdr.		X —	—> O	

X = Current Commitment O = Needed Commitment

The following evaluation of current individual commitment include recommendations for approaching members of the critical mass to achieve the desired commitment level.

<u>Placentia Chief of Police</u>: The Chief must be convinced that the benefits of implementing the strategy will outweigh the expenditures in resources. To keep the Chief in the "help change happen" category, will require a united effort of management and supervisory personnel. They should stress that it would not only benefit the department but the community. The Chief must be

willing to negotiate on the form and structure of the department in order to facilitate the implementation of the strategy.

Placentia City Manager: The City Manager's current position on the strategy coincides with that of the Chief due to a desire to support the Chief. If the Chief were to change commitment, the City Manager would follow suit, as he has no personal resistance to the strategy. The City Manager must be assured that the resources are available, that the city will benefit from the program, and that those involved as key stakeholders support the strategy. These assurances can be provided by the Chief.

Administrative Division Commander: The transition manager is the administrative division commander. He will have complete responsibility for "making the change happen," as the detective bureau is under his command which makes him the logical choice. This will include bringing together personnel and other resources. He will facilitate all required activities in order to realize the desired future, and furnish feedback to all concerned parties.

PPOA President: The Placentia Police Officers Association is the snaildarter of the task force strategy. The PPOA often views itself as an adversary of both city and police management and is constantly on the watch for political advantage. This makes PPOA behavior very unpredictable and a potential adversary. The PPOA President's political role is to scan all issues looking for political advantage and benefits for its general membership.

The PPOA generally would be highly skeptical of any change within the organization. However, they would want to be involved in any task force process to insure that the PPOA's best interest is served. The PPOA president's support is not vital to the process, however, his disapproval would be difficult to overcome. If the issue is deemed to be in the best interest of the PPOA they would probably assume a "let it happen" posture. This could easily change to "block change," if they somehow felt it was not in their better interest.

Patrol Division Commander: The Patrol Division Commander has the potential of blocking any transfer of resources that would be at the expense of his division. The department has a history of creating new positions and staffing it with personnel from the patrol division. In recent years the overall size of the agency has increased, and many new specialty positions have been created, however, the patrol strength remains at the same critical level that it was ten years ago.

The Patrol Division Commander must be convinced that any reorganization would not necessarily be at his divisions expense. Any long range planning without his involvement could potentially change his "let change happen" stance to one of "block change," if he felt his division's ability was going to be jeopardized by loss of additional manpower. He could easily be persuaded to "help change happen," if he had equal representation on future decision making affecting the department in this area.

TRANSITION MANAGEMENT STRUCTURE

The Administrative Division Commander was selected to manage this change. The chief of police has ultimate responsibility and authority. However, the time and energy required to make the transition will not allow the chief to oversee the change himself. Instead he will temporarily grant executive responsibility and authority to the transition manager. This structure would be the most effective because of the nature of change, the transition managers relationship to key individuals, and his enthusiasm for the project. The transition manager or "project manager" is in the best position to integrate the change and is willing to take the responsibility of implementation.

The project manager will facilitate all required policy formation involving the chief of police, city manager, and the employees. This will insure proper input and build a cohesive work group. He will chair the task-force made up of key stakeholders to assess current and future needs, and develop a long-range plan for managing computer crimes. The project manager will routinely provide feedback to all the critical mass and publish progress reports.

IMPLEMENTATION TECHNOLOGIES

It is generally understood that resistance is a part of most change. People become comfortable with what they know and fear what they don't know. The uncertainty is sure to produce anxiety. It is essential that methods and technologies are used to deal with the anxieties of change so that the desired future may be realized.[16]

Responsibility Charting

Responsibility charting will be done to help assess alternative behaviors for each party during the entire change process. This will clarify the behaviors that are required in order to affect the desired changes. Furthermore, this activity will promote team building since responsibility charting is a group effort. The process requires the anonymous consensus of the group for the required behavior of each party. The behaviors are plotted and include: (R) Responsibility (this indicates the designated individual has responsibility for a particular action); (A) Approval (the individual need only approve and has the power to veto); (S) Support (the individual must in some way support but does not have to agree); (I) Inform (the individual must be advised of intended action before it is taken). The Responsibility Chart is found in Appendix M.

The key to the transition process is communication and participation by those within the organization. The following management technologies have been selected for implementing the change.

Creating a Vision of the Future: In order to create a vision of the future, all those involved must be able to let go of the past. They may be given the opportunity to do that if the leadership communicates to everyone affected what the future will be like. If they can see it in their own minds, the change becomes less threatening. They will be confident that they can manage the future if they believe they know it.

Action Plans: Developing clear action plans that embody future goals will keep the proposed change on course and give the work group certain direction. Each step should include action plans and this activity should commence at the very beginning.

Team Building: The change will only be successful if those people involved are committed to the new method of performing work. This is especially true for those who will be doing the work. They must be involved in policy formation and action planning. This will be accomplished by open communication with shared authority and responsibility. The result will allow for flexibility and motivate the group to move ahead because they share in the outcomes.

Stakeholders Surveys: This is the device that is used to keep the transition manager in close contact with the stake holders. It also serves to promote communication in all directions. This may lead to affiliations between stakeholders which would not otherwise exist. Furthermore, problems may surface that were not anticipated and that need to be addressed.

Midpoint Scenario: The transition manager shall complete a midpoint scenario of what the half-way point will be like. This scenario will provide a useful measure and future guide for action. The scenario is used for a progress marker, and will help the work groups adapt as necessary.

Progress/Evaluation Reports: Written progress reports will be prepared at regular intervals. The reports will be used to give feedback to city manager and chief of police. The progress reports will also be shared with all department members and will evaluate and recognize the efforts of the task-force.

Celebrate Milestones: The project will plan to celebrate milestones of accomplishment. During the transition, several achievements will be recognized. The events will be preplanned and will serve to keep focus on the project while building enthusiasm.

SUMMARY

The purpose of transitional management is to give life to the strategic plan. That is a simple statement that represents a monumental task. The goal of transitional management is to create an environment that embraces change by minimizing the negative effects of the change. If done properly, the stakeholders will realize that their concerns have been addressed and the desired future will be realized.

PART IV

CONCLUSIONS - RECOMMENDATIONS

AND FUTURE IMPLICATIONS

The conclusion will be broken down into two separate sections: An answer to the issue and sub-issue questions with a summary of recommendations; and an identification of subjects for future study.

ANSWERS AND RECOMMENDATIONS

This paper dealt with the issue: **"What will be the status of the management of the investigation of computer crimes by the year 2001?"** To provide focus to the project, the study was further defined by the use of the following sub-issues:

- What will be the financial impact of investigation of computer crimes on the budget?
- What will be the need for specialist personnel?
- What will be the legal changes in investigation regarding federal vs. municipality responsibilities?

A major issue that must be taken into consideration is the trend toward privatization of police services, as it will have a significant impact on who will do the majority of the investigations of computer crimes. While some law enforcement executives view this trend with great concern, others see much benefit. A number of senior police officers speculate that the future police community will separate into three distinct strata -- public, private and corporate.[17] This stratification will continue to evolve from the present trend toward police privatization, especially in the area of computer crime.

Public police agencies will be victimized in the future by underfunding, understaffing, lack of proper equipment and inadequate training.[18] These conditions could encourage the trend toward privatization, thus minimizing public involvement in major corporate losses.

The growth of corporate policing has established what may be regarded as a quasi-criminal justice system in many major corporations. The expansion of this phenomenon is expected to continue well into the future. Corporate security investigators and auditors already conduct investigations regarding a wide range of financial crimes including credit card fraud, computer fraud, and embezzlement. In many cases, corporations, not the courts, decide the disposition of these crimes. Many times major corporate embezzlements involving hundreds of thousands of dollars result only in forced resignation of the defender, not prosecution in a court of law.

Corporations lack confidence in the ability of law enforcement to address these investigations in a manner that will protect sensitive corporate business interests. In recognition of these circumstances, the law enforcement community should seek to engage in closer and more effective working relationships in order to better understand each other's values, motivations, and roles.

Sub-issue 1: What will be the financial impact of investigation of computer crime on the budget? In order to determine this factor one must purview their community in order to determine the magnitude of potential victims. This could obviously vary depending on the balance of the community's business vs. residential make-up, and the size of the city. A community like the city of Placentia, a predominantly residential community with some light industry, would be less likely to be impacted than a city with a higher percentage of businesses, which are more apt to be victimized.

Being service oriented, the majority of law enforcement's budget concerns would be the necessity for more personnel to investigate computer crimes, as personnel generally account for eighty-five percent of the budgets. Computer hardware and software would have significant start up cost, but could be prorated over a period of years depending on the life of the product. These costs could also be affected by normal wear and by new technology. Hardware has seen significant drops in pricing over the past several years. Software, however, has continued to increase in cost.

In 1970 it took computer technology 10 years for it to become obsolete. In 1980 it only took three years. Today the time has been reduced to eighteen months. Next year it will only take just nine months.[19] This rapid acceleration in technology does not necessarily make equipment obsolete over night, however the newer technology allows the computer to work faster, store more information, and utilize newer software programs that expand the computer capability.

Of significant consideration is the length of time required to investigate computer crimes, as estimates range from four months to a year for many cases. The most critical aspects of determining the cost impact on the budget would be derived from traditional criteria such as calls for service relating to computer crime, necessary manpower for interdiction, proper equipment, and specialized training.

Sub-issue 2: What will be the need for specialized personnel? This is going to be controlled by the development of computer technology, which is accelerating at a faster pace than ever. Currently it takes a high level of training to investigate computer crimes. This required level of special technical training for computer crime investigators will eventually be reduced by more sophisticated equipment, which will reduce the technical aspect now necessary to investigate computer crimes.

Technology as we know it today will be passe ten years from now. Only twenty percent of a computer's capability are currently being used. New technology will open up the remaining eighty percent that is not being used due to computer illiteracy stemming from todays complicated software which vary from program to program.[20]

All the people that have been left out by not learning how to use computers will come of age with voice activated "spoken command" computers. The keyboard will become a thing of the past. This technology is here today and will be available to the public in some form in two years. Soon we will see "palm top" computers, with voice activated command cellular modems. The computers will fit on a belt, similar to our pagers of today, or in a pocket or purse. The information can be up loaded by cellular modems to a host computer.

Some futurists at Massachusetts Institute of Technology (MIT) believe that we will have developed "artificial intelligence" (implanted technology) around the years 2000-2010.[21] This will further minimize the need for extensive in house training, or the hiring of personnel solely for the technical background and computer skills they possess.

The need for specialized personnel will decrease as modern technology takes off like we have never experienced before. We will be handling high-tech problems with low tech solutions, as we will still be dealing with people.

Computer literacy will increase significantly when field officers routinely use computers to take initial reports, enter evidence collection information, enter or recall detailed floor plans, diagram crime and traffic accident scenes, and never leave the location of the incident.

Currently, however, the absence or minimal use of computers in many law enforcement and prosecutors' offices is both a symbol and a symptom of a critical problem for investigators and prosecutors.[22] It suggests how little computers are being considered by justice officials and underscores how far behind the criminals many departments have become.

A simple solution (though not necessarily easy to implement), is for law enforcement and prosecutors' agencies to install as many micro-computers in their agency as budgets will allow. An agency should realize many rewards from such a strategy. For one, existing personnel will likely become computer literate, which would improve their ability to handle computer-related crimes. The agency might even be appealing to a person with strong technical skills who could oversee the use of the computers and be an expert advisor to investigations of computer-related crime. As a third benefit, the agency would have access to the expanding collection of computer software aimed at managing criminal justice caseloads, training justice personnel, and analyzing justice information.

Sub-issue 3: What will be the legal changes in investigation regarding federal vs. municipal responsibility? At this time most states, including California, have enacted legislation regarding computer crimes. However, computer-related offenses are often interstate in nature, and involve investigators and prosecutors in several local jurisdictions and the federal government. Nearly all crimes involving telephone code abuse are interstate, as are some automatic teller networks. The United States Secret Service and the Federal Bureau of Investigation are charged with the investigation of most computer crimes that fall under federal statutes.

Negotiating the investigation and prosecution of multi-jurisdictional cases is difficult for several reasons. First, federal prosecution standards limit federal involvement in many computer-related offenses that come to the attention of local, state and county investigators. U.S. Attorneys decline to prosecute juveniles, which eliminates many "hacker" cases from their consideration, because the federal criminal justice system is not designed to handle juvenile matters. Cases involving adults are also declined if the dollar loss is not sufficient to meet federal prosecution standards.[23] The author believes that this dollar figure will continue to climb as reported computer crimes begin escalating, overloading the federal authorities. And that federal prosecutors will require a monetary loss of over a million dollars in order to prosecute cases in the future.

It would be naive to believe that federal legislation would be enacted that would mandate more federal responsibility for computer crime investigations. When one considers that virtually all businesses, regardless of size, utilize computers to some degree, a couple of sobering facts emerge. First, computer crime is within the capability of millions of people, much more than most of use realize. Second, most computer crime is, therefore, within the investigative jurisdiction of state and local agencies.

Computer crime is here to stay. Law enforcement is doing an admirable job in combatting it, considering all the legal and technical hurdles that must be overcome during an investigation and prosecution. Agencies cannot slacken in their commitment to develop expertise in computer-related investigations. The future of law enforcement depends heavily on a commitment to stay abreast of current and developing trends.

STRATEGY FOR THE FUTURE

Each city should consider a strategy based on its size, budget, and the nature of the community served when planning to address computer related crime. The following areas should be carefully studied and explored:

1. Make a commitment to be responsive to the victims of computer-related crime.
   a. From executive level (Chief of Police)

2. Determine the level of commitment that is feasible.
   a. Shared resources
   b. Functional Specialist
   c. Full-time assignment

3. Identify those in your organization who have an interest in computer-related crime. (Preferably who have economic crime investigation background).

4. Assure that the individual(s) receive adequate training.

5. Establish operating procedures and organizational reporting requirements.

6. Identify technical support resources.

7. Coordinate law enforcement and prosecution efforts.

8. Join state computer crime associations, such as High-Technology Crime Investigators.

9. Involve potential victims in planning strategy.

Because there are currently so few individuals capable of investigating and prosecuting computer-related crime, the need to pool resources will continue for a number of years. Education alone is not the answer to developing good computer crime investigators. As in most areas, computer fraud investigative instruction only lays the groundwork. The true education comes from participating in such investigations. Credibility comes from training and experience.

The research tends to indicate that California law enforcement can manage computer-related crime in the future, however it will place many new demands that will require a strong commitment. If we provide effective and creative guidance during the transition period we can meet the challenges of the coming century.

SUBJECTS FOR FUTURE STUDY

During the study, the researcher identified several issue areas that appear to be worthy of future study. Some of these are:

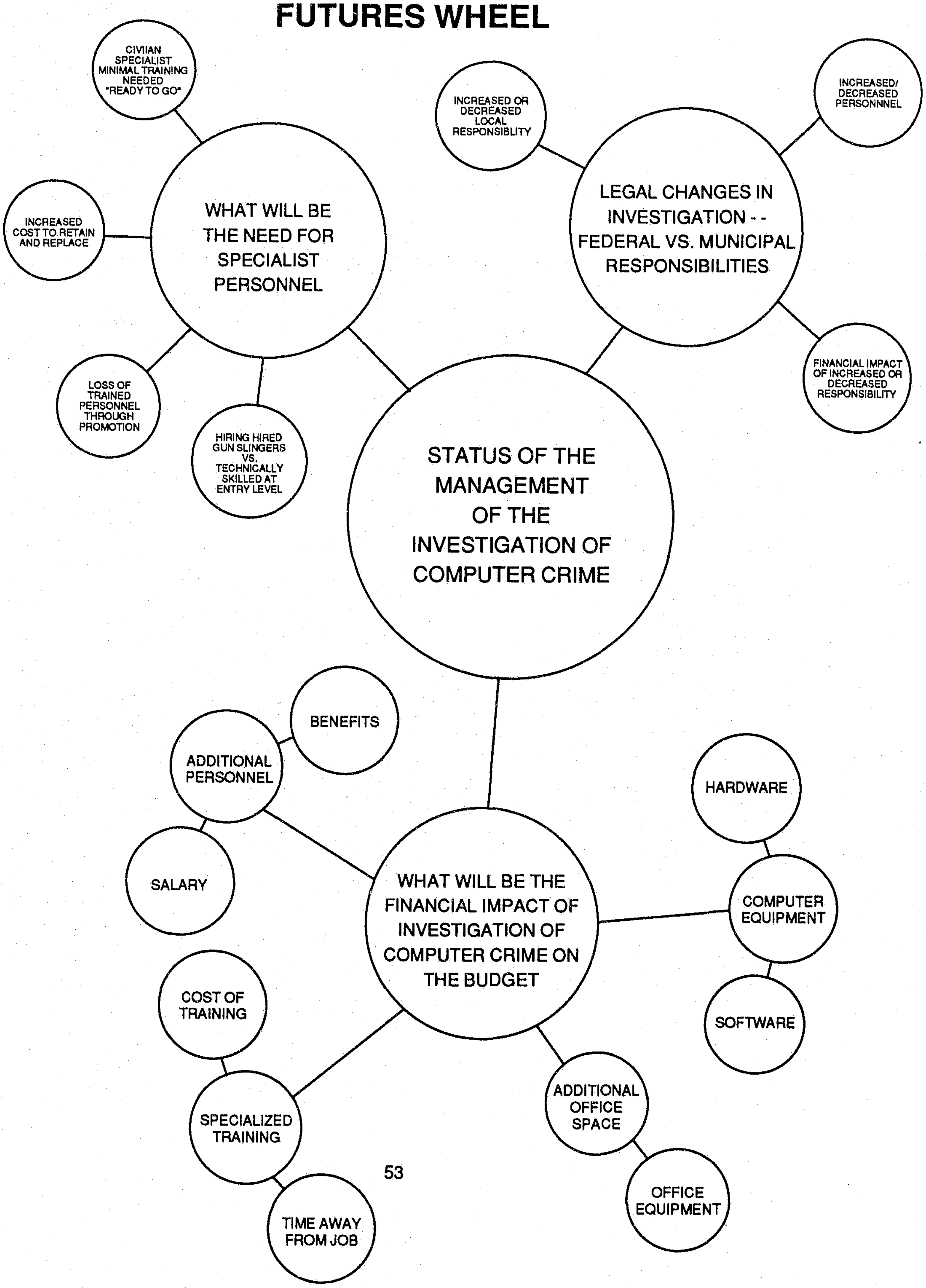
- The need for computer ethics being taught as a prerequisite for high school and college computer classes.

- How will a future "moneyless society" impact future computer crime.

APPENDIX

Appendix A

FUTURES WHEEL



CIVIAN SPECIALIST MINIMAL TRAINING NEEDED "READY TO GO"
INCREASED OR DECREASED LOCAL RESPONSIBLIITY
INCREASED/ DECREASED PERSONNNEL
INCREASED COST TO RETAIN AND REPLACE
WHAT WILL BE THE NEED FOR SPECIALIST PERSONNEL
LEGAL CHANGES IN INVESTIGATION - - FEDERAL VS. MUNICIPAL RESPONSIBILITIES
FINANCIAL IMPACT OF INCREASED OR DECREASED RESPONSIBILITY
LOSS OF TRAINED PERSONNEL THROUGH PROMOTION
HIRING HIRED GUN SLINGERS VS. TECHNICALLY SKILLED AT ENTRY LEVEL
STATUS OF THE MANAGEMENT OF THE INVESTIGATION OF COMPUTER CRIME
BENEFITS
ADDITIONAL PERSONNEL
HARDWARE
SALARY
WHAT WILL BE THE FINANCIAL IMPACT OF INVESTIGATION OF COMPUTER CRIME ON THE BUDGET
COMPUTER EQUIPMENT
COST OF TRAINING
SOFTWARE
SPECIALIZED TRAINING
ADDITIONAL OFFICE SPACE
TIME AWAY FROM JOB
OFFICE EQUIPMENT

Appendix B

BIBLIOGRAPHY

Anaheim Police Department Training Bulletin "Handling Computer Evidence and Computer Crimes." (June 1991).

Alexander, Michael. "Hacker Sentenced to Prison." Computerworld (April 1, 1991).

Branscomb, Ann. "Common Law for the Electronic Frontier." Scientific American (September 1991): pp. 154-164.

Clede, Bill. "Computer Crime Studied by National Center." Law and Order (May 1989): p. 10.

Colvin, Bill D. "Computer Crime Investigators: A New Training Field." F.B.I. Law Enforcement Bulletin (July 1979): pp. 9-12.

Conley, Catherine J., J. Thomas McEwen, "Computer Crime," NIJ Reports, January/February, 1990, Pg. 1-7.

Conser, James A. "The Future of Computer Crime." National Institute of Justice Computer Crime Conference, Washington D.C. (September 14-15, 1989).

Coutourie, Larry. "The Computer Criminal: An Investigative Assessment." F.B.I. Law Enforcement Bulletin (September 1989): pp. 19-22.

Fitzpatrick, Carlton W. "Overview of Computer Crime." The Police (March 1987): pp. 68-71.

Hanson, Gayle. "Computer Users Pack a Keypunch in a High-tech World of Crime." Insight on the News (April 15, 1991): pp. 8-17.

Hughes, William J. "Computer Crimes Isn't a Game." The Washington Post (July 15, 1986).

Jones, Chuck, et al. "Moving Toward the Future -- 2000." Department of Justice, Special Agent 2000 Committee.

Kusserow, Richard P. "An Inside Look at Federal Computer Crime." Security Management (May 1986).

Mangan, M.A. and Michael G. Shanahan "Public Law Enforcement/Private Security." FBI Law Enforcement Bulletin, Special Futures Issue (January 1990): pp. 18-27.

McCord, Rob and Elaine Wicker "Tomorrow's America - Law Enforcement's Coming Challenge." FBI Law Enforcement Bulletin, Special Futures Issue (January 1990): pp. 28-32.

McEwen, Thomas. "Computer Ethics." National Institute of Justice Reports (January/February 1991): pp. 8-11.

McEwen, Thomas J., et al., Dedicated Computer Crime Units, National Institute of Justice, Issues and Practices, June 1989, Pg. 62.

Morris, Richard. "The 31st Century Impact of Privatization on the Investigation of High-tech Crime." P.O.S.T. Command College Class II Project (1986).

Moulton, Roger M. "Computer Crime -- An Emerging Law Enforcement Priority." The Police Chief (May 1988): pp. 47-48.

Parker, Don B. "Computer Crime," Criminal Justice Resource Manual, Second Edition, (August 1989).

Parker, Patricia A. "Downloading Computer Crime." Police (August 1991): pp. 55-123.

"Private Police: Their Role of the Private Sector in Law Enforcement Grows." Wall Street Journal (October 15, 1991).

Sessions, William S. "Computer Crimes: An Escalating Crime Trend." F.B.I. Law Enforcement Bulletin (February 1991): pp. 12-15.

Swanson, C. R. and Leonard Territo "Computer Crime: Dimensions, Types, Causes, and Investigations." Journal of Police Science and Administration (September 1980): pp. 305-315.

Tafoya, William L. "A Delphi Forecast of the Future of Law Enforcement." Doctorate Dissertation (1986)

U. S. Department of Justice, "Basic Considerations in Investigating and Proving Computer-Related Federal Crimes." (1988).

Vranizan, Michelle, "Computers Programmed Into Entertaining Series." Orange County Register, Section F, April 6, 1992.

World, Jeffrey. "Computer Crime: The Undetected Disaster." Disaster Recovery Journal (January 1991).

Appendix C

PERSONS INTERVIEWED

Clay W. Hodson, Chief Investigator
President High Technology Crime Investigation Association
Riverside District Attorneys Office
4075 Main Street, Riverside, Ca 92501

Jill Kossow, National Account Executive
Apple Computer, Inc.
600 Corporate Pointe, Suite 1200,
Culver City, CA 90230

Ali R. Movasaghi, Systems Engineer,
International Business Machines Corporation (IBM)
355 S. Grand Ave., Los Angeles, CA 90071

Appendix D

May 17, 1991

Name
Title/Position
Address

Dear ___________,

Thank you very much for consenting to participate in my Independent Study Project (i.e., Master's thesis) Nominal Group Technique (NGT) exercise. As I mentioned to you, it is a form of "structured brain-storming" exercise with a relative strict protocol. The process will include both individual and collaborative work in a group setting.

We will be meeting on Wednesday, May 22, 1991, from 9:00 A.M. until around 1:00 P.M., at the Placentia Police Department, 401 East Chapman Avenue. I have attached directions and a map for your reference. All participants are invited to be my guest for lunch at the conclusion of the exercise.

Let me share some information about the issue we will address, and the purpose that we will use in our analysis.

The Issue

The primary issue is:

> What will be the status of management of the investigation of computer crime by 2001?
>
> For the purpose of defining this issue, a computer crime is defined as the taking or transferring of funds, information, or the illegal or unauthorized entry into a computer's data files.

My Sub-Issues are:

1. What will be the financial impact of investigation of computer crimes on budget?
2. What will be the need for specialist personnel?
3. What will be the legal changes in investigation regarding federal vs. municipality responsibilities?

The Process

We will be using the Nominal Group Technique, or NGT for part of our session, and a group survey method for the remainder of the time. Our goals will be:

1) to identify important trends and events which are related to, or may affect or impact, my issue/sub-issues; and

2) to forecast the shapes of the trends and probabilities of the event.

Definitions

Event - A single occurrence, that can be traced to a given point in time. (Several events occurring over time create a trend).

Example: New legislation is passed to increase the penalties for computer crimes.

Trend - Several similar events which take place over a relatively short period of time. They are indicators of possible change.

Please note that I fully expect the process to last (4) hours. I am depending on all participants to complete the full process. If, for any reason, you are unable to make a commitment to do so, please call as soon as possible (714 993-8168).

Again, thank you for your willingness to participate in this process.

See you on May 22nd!

Daryll Thomann, Captain

Appendix E

NOMINAL GROUP MEMBERS

1. First Interstate Bank, Vice President and Manager of Information Security

2. Rockwell International, Director of Computer Security

3. Los Angeles Police Department, Coordinator Computer Crime Unit

4. California Department of Justice, Bureau of Investigation Special Agent, Computer Crimes

5. TRW General Services Division, Space and Defense Sector, Manager Computer Security

6. Orange County Sheriffs' Department, Computer Crime Supervisor

7. Los Angeles District Attorney's Office, attorney assigned to Major Frauds Division (Computer Crimes)

Appendix F

TRENDS IDENTIFIED BY THE NOMINAL GROUP PANEL

1. Number of Computer Crimes Reported vs. Occurrences
2. Use of Computers in Criminal Activity
3. Technological Improvement (Access vs. Control)
4. Networking, Decentralization Susceptibility of Computers (Cheaper, Easier to Use/Penetrate)
5. Specialized Training For Law Enforcement
6. Uniform Application of Law (Jurisdiction to Jurisdiction)
7. System Connectivity (Ultimate Global Network - Jurisdiction)
8. Anonymity of Perpetrator
9. Resources/Commitment/Focus
10. Working/Sharing Relationship Between Law Enforcement and Civilian Counterpart
11. Level of Computer Literacy and Access/Use of Computers
12. Portability and Mobility for Criminals
13. Reliance on Computers by Business and Industry
14. Information Exchange by Criminal Element (Sharing Techniques)
15. Development of Expertise by Law Enforcement (Retention of Assignments)
16. Computer Ethics Relating to Computer Crime
17. Role of Professional Organizations (Developing Standards and Qualifications)
18. Empathy Towards Institutional Victims
19. Effects of Downsizing on the pool of Potential Perpetrators (Disgruntled Insiders)
20. Changing Internal Controls
21. Jurisdictional Questions
22. Systems Expertise/Systems Complexity
23. General Insensitivity and Understanding of Computer Crime
24. Loss/Recovery Passed to Consumers
25. Lag time Between Occurrence and Response

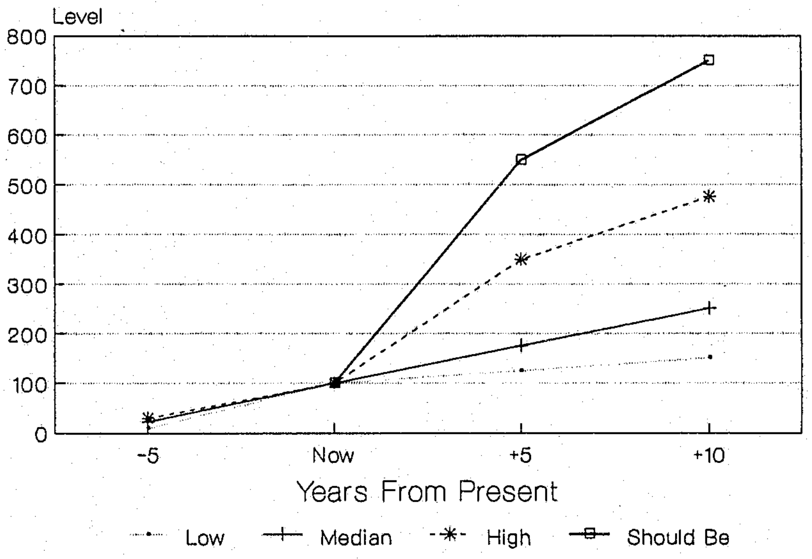
Appendix G

EVENTS IDENTIFIED BY NOMINAL GROUP PANEL

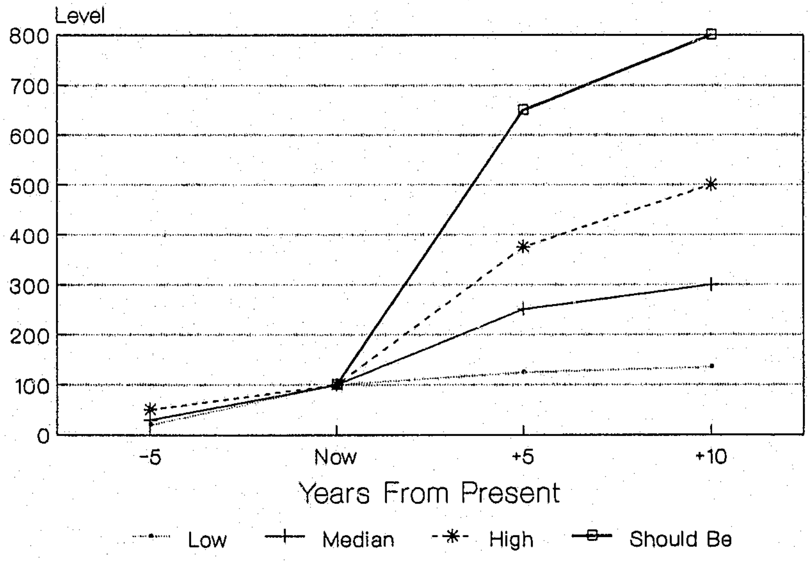
1. A Significant Event or Major Computer Catastrophe
2. Passage of Federal Statute For Enforcement/Regulation
3. Revenue Windfall (Federal/State Money for Computer Crime)
4. Technological Breakthrough
5. Private Sector Funding For Law Enforcement (Statute Mandating Funding as Part of Restitution)
6. Establishment of a Non-Profit Foundation For Computer Security (Private or Public Funding)
7. Establishment of a Centralized Investigation Agency/System
8. Education Board Establishes Ethics Course as a Prerequisite For Any Computer Course
9. Special Interest Initiative Regarding Freedom of Information Act (Protection For Accessing Information)
10. Formal Computer Syndicate Created (For Criminal Purposes)
11. Law Enforcement Actions Resulting in Bad Case Law
12. Facility Established For Cross Training Law Enforcement and Private Sector Security Specialists
13. Deployment of a National/Regional Computer Utility

Appendix H

Trend 1
Retention of Expertise

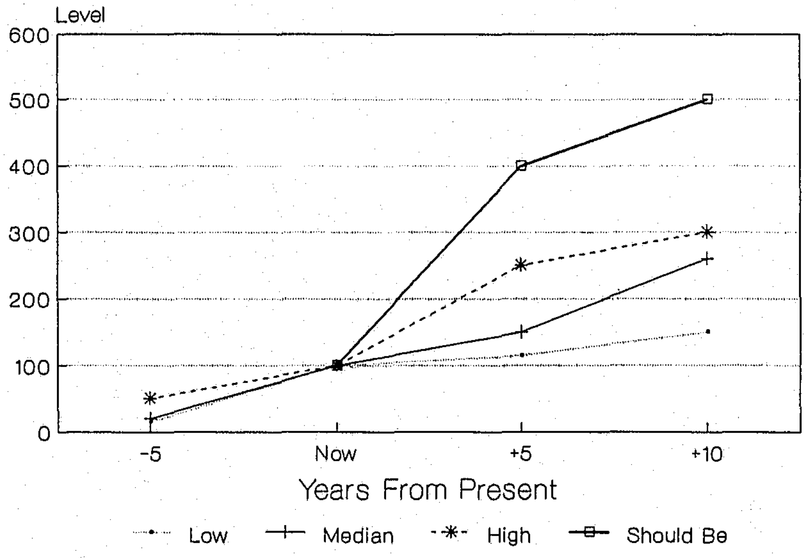


Trend 2
Level of Specialized Training

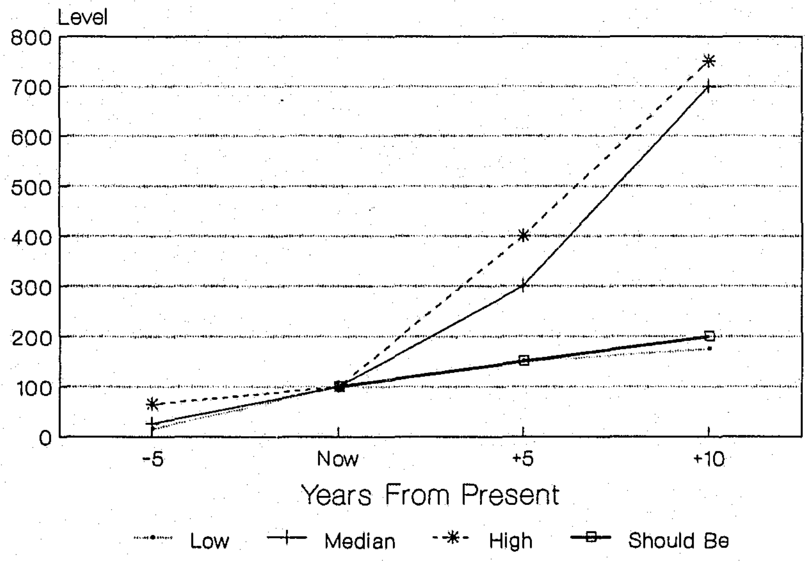


Appendix H (Continued)

Trend 3
Level of Allocation of Funds



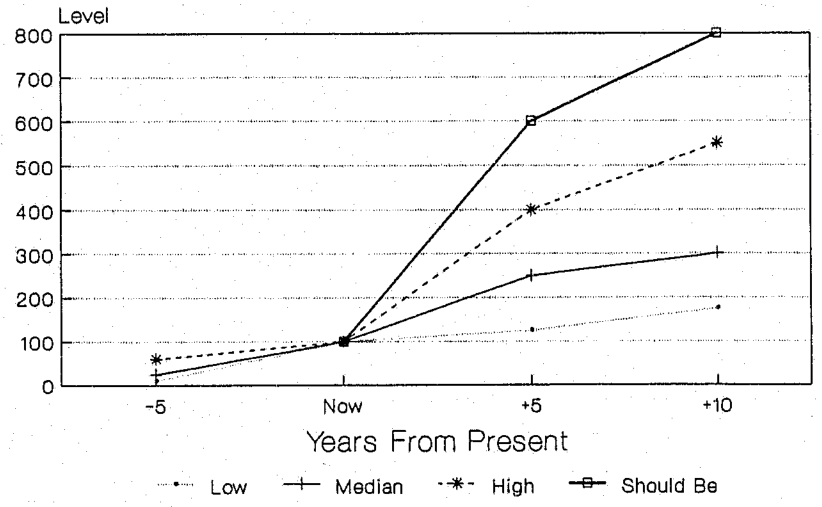
Trend 4
Use Of Computers By Criminals



Appendix H (Continued)

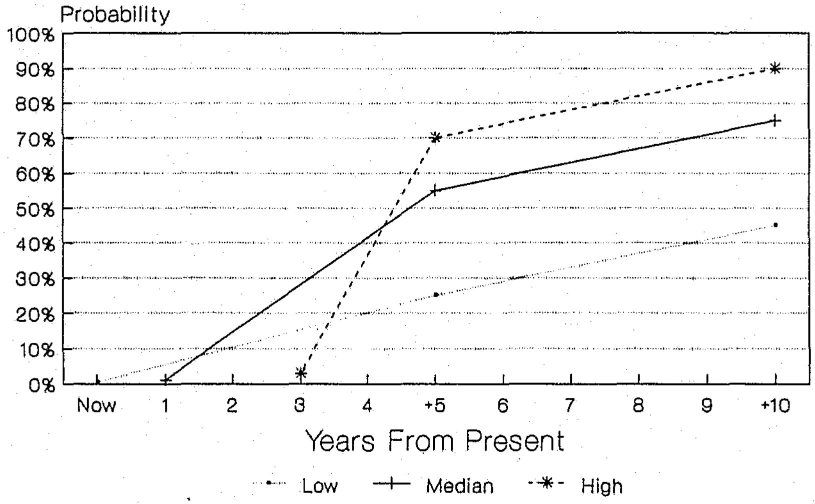
Trend 5

Working/Sharing Relationship With Private Sector

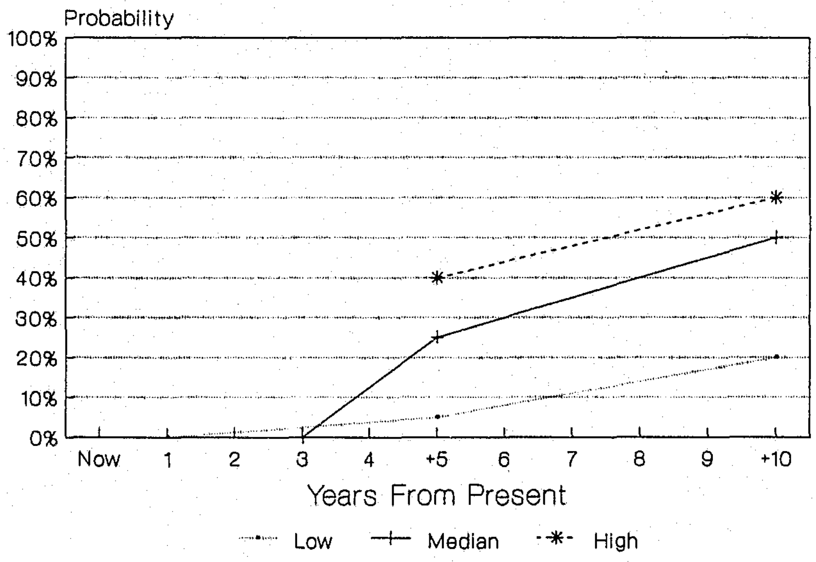


Appendix I

Event 1
Significant Event (Catastrophe)

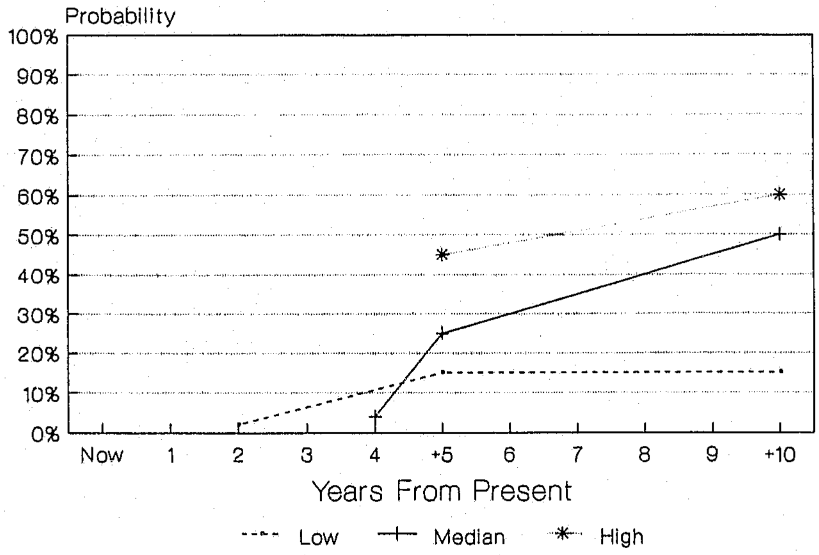


Event 2
Federal Statute For Enforcement

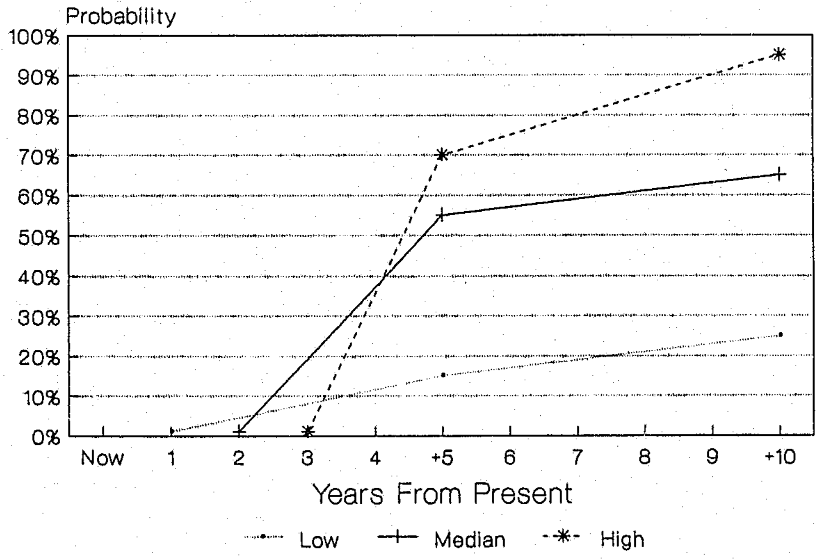


Appendix I (Continued)

Event 3
Centralized Investigation Agency



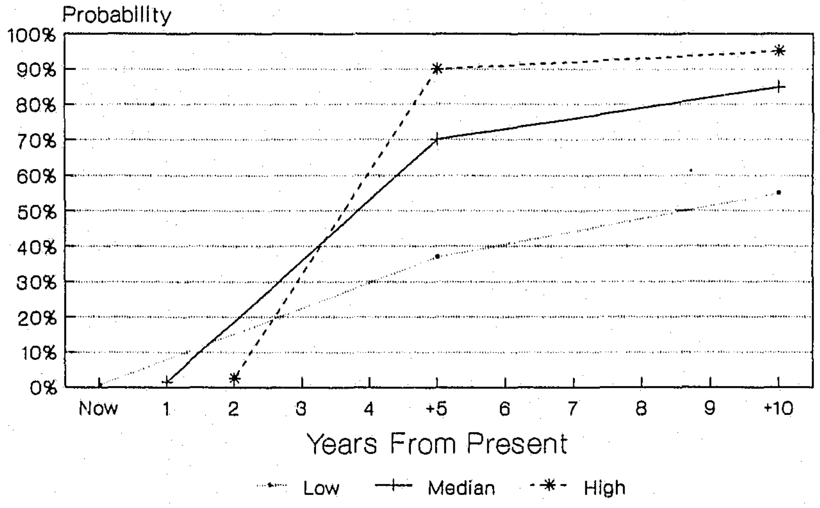
Event 4
Special Interest Initiative



Appendix I (Continued)

Event 5

Law Enforcement Action Results In "Bad Case" Law



Appendix J

STAKEHOLDERS

A. Police Officers Association

1) Will support a high-tech crime investigation unit; additional lateral transfer ability.

2) Will oppose developing new unit as they may feel it would be at the cost of patrol strength and and become a morale issue. May seek to challenge current promotional practices. (Snaildarter)

B. Chief of Police

1) Conceptually supportive of the issue; reviewing current and future investigative needs; however, must be convinced that gains exceed resource expenditures. Will want an effective monitoring system.

2) Supportive of new investigative unit for employee morale; more possibilities of lateral movement within organization.

C. Business Community

1) Mixed conditionally supportive. Small businesses will be concerned about degree of expertise and recoverability of losses.

2) Will not be supported by major corporations, as they would be resistant to change; suspicious of expertise. Would prefer to handle themselves.

D. City Manager

1) Will support program that will improve employee morale; increase efficient use of resources, and satisfy the city council.

2) May oppose the hiring of additional personnel and start-up costs of high-tech unit.

E. District Attorney

1) Conditionally supportive, increased investigations will require additional case load for court staff.

2) Supportive to improved management of computer crimes, and increased expertise; will make prosecution easier. Might struggle for political power with Sheriff if regional approach is eventually realized.

F. First Amendment Advocates

1) Would be opposed to any changes that would further restrict freedom of information.

2) Opposed to any action that would attempt to prosecute for copy right infringements.

G. Computer Hackers

1) Would not be supportive of any increased police proficiency relating to computer crime enforcement.

2) Would oppose any law enforcement action that would further restrict, control, or have the potential of curtailing their activity.

H. Sheriffs' Department

1) Would be neutral regarding Placentia establishing a computer crime unit to handle local cases.

2) Would support regional approach if convinced the need was there; would demand a high degree of control.

I. California Police Chiefs

1) Conditionally supportive; would like feasibility study of regional approach.

2) Would be supportive of additional training to increase their investigators' productivity.

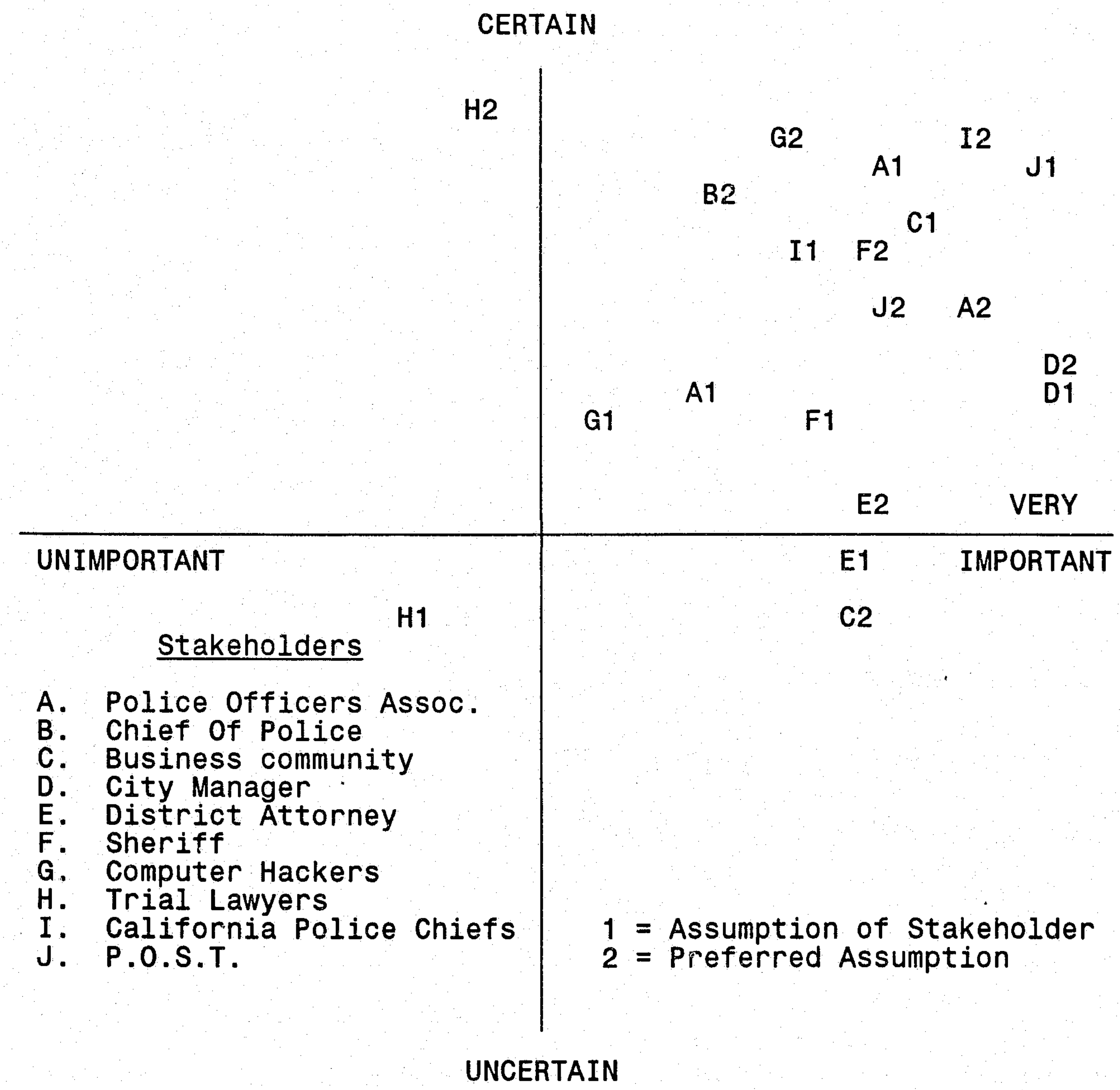
J. POST

1) Conditionally supportive of providing technical training classes; if need shown and supported by top executive law enforcement officers.

2) May hesitate to show support as need for training may not initially be identified, and start-up costs expensive.

Appendix K

ASSUMPTION MAPPING



<u>Stakeholders</u>

A. Police Officers Assoc.
B. Chief Of Police
C. Business community
D. City Manager
E. District Attorney
F. Sheriff
G. Computer Hackers
H. Trial Lawyers
I. California Police Chiefs
J. P.O.S.T.

1 = Assumption of Stakeholder
2 = Preferred Assumption

Appendix L

ALTERNATIVE STRATEGY EVALUATIONS

1. Restructure Crimes Property Unit to Handle Computer Crimes
The department would implement new position(s) to handle cases within current investigation unit.

Pros:
- o Local control of local problems
- o Establishment of closer ties with local business
- o More access to investigators for assistance with other internal priorities

Cons:
- o Less available resources for major cases
- o Would not be able to address major corporate losses
- o Start up costs, training needs, retention of expertise

2. M.O.U. Between Law Enforcement and Corporate Businesses
The Placentia Police Department would establish a memorandum of understanding with corporate businesses. The purpose would be to better understand each others capabilities and to clarify each others role regarding computer-related crime.

Pros:
- o Establish a spirit of cooperation and understanding
- o Will foster corporate support for the department
- o Mitigate some of the opinions held by law enforcement regarding privatization of police services

Cons:
- o May be resistant by some members of both sides
- o Would reveal weaknesses in current law enforcement investigation capabilities

3. Establish Regional Task Force to Investigate Computer Crime
Pooling of resources by interested municipal law enforcement agencies, Sheriffs' Department, District Attorney, and possibly federal agencies.

Pros:
- o Cost affective
- o More proficient
- o Build confidence of business community
- o Improve professional image of involved agencies

Cons:
- o Power struggle for control
- o Would require time and money to equip and train
- o Political climate is constantly changing; consequently, so will support and financial commitment.

4. Contractual Services For Computer-Related Crime

Contract with private security companies specializing in computer-related crime investigations. Victims and city to share cost of investigations.

Pros:

- o Would lessen financial impact on local government
- o Would allow more police deployment on high profile, violent crimes.

Cons:

- o May be resisted by POA members of the department
- o Overcoming those comfortable with existing culture
- o Billing those who already pay taxes for police services

Appendix M

Table 5
RESPONSIBILITY (RASI) CHART

ACTORS DECISIONS or ACTS*	Chief of Police	Steering Comm. Chair	PPD Managers Spoke-person	City Manager	PPOA group Chair
Formulate police	R	I	S	I	
Choose taskforce committee chair	R	I	S	A	
Select taskforce	A	R	I		S
Assess organization and culture	A	R	S		
Identify internal and external resources	A	R	I		S
Design computer crime investigation unit	A	R	I	I	S
Identify computer crime investigation participants	S	A	R		
Maintain contact with stakeholders	A	R	S		S
Begin computer crime investigation unit	A	R	S	I	S
Monitor program and community reaction	A	R	S	I	
Periodic reports to Chief	S	R	I		I

* Legend

R = RESPONSIBILITY for action (but not necessarily authority)
A = APPROVAL (must approve, has power to veto the action)
S = SUPPORT (has to provide resources, but does not have to agree to the action)
I = INFORM (must be informed before action, but cannot veto)
Blank = Irrelevant to that particular action

Appendix N

ENDNOTES

1. Robert F. Littlejohn, "Teaming Up to Fight Computer Crime," Security Management, July 1990, Pg. 37.

2. William L. Tafoya, "A Delphi Forecast of the Future of Law Enforcement," Doctorate Dissertation, 1986, Pg. 321.

3. Bill Clede, "Computer Crime Studied by National Center," Law and Order, May 1989, Pg. 10.

4. Robert F. Littlejohn, "Teaming Up to Fight Computer Crime," Security Management, July 1990, Pg. 37.

5. Donn B. Parker, "Computer Crime," Criminal Justice Resources Manual, Second Edition, 1989, Pg. 7.

6. Chuck Jones, et al., Special Agent 2000, "Moving Toward the Future," California Department of Justice, 1990, Pg. 44.

7. Gayle Hanson, "Computer Users Pack a Keypunch in a High-tech World of Crime," Insight on the News - The Lineup on Computer Crime, April 15, 1991, Pg. 11.

8. Robert F. Littlejohn, "Teaming Up to Fight Computer Crime," Security Management, July 1990, Pg. 37.

9. Catherine H. Conley, J. Thomas McEwin, "Computer Crime," NIJ Reports, January/February 1990, Pg. 3.

10. Catherine H. Conley, J. Thomas McEwen, "Computer Crime," NIJ Reports, January/February, 1990, Pg. 7.

11. J. Thomas McEwen, "Dedicated Computer Crime Units," National Institute of Justice, Issues and Practices, June 1989, Pg. 11.

12. James A. Conser, "The Future of Computer Crime," National Institute of Justice Computer Crime Conference, Washington D.C., September 14-15, 1989, Pg. 9.

13. Thomas C. Esensten, POST Command College notes (July 24, 1991), POST

14. Thomas C. Esensten, POST Command College notes (July 24, 1991), POST

15. Richard Beckhard and Reuben T. Harris, Organizational Transitions, Managing, Complex Change, second edition, Addison-Wesley, NY, 1987, Pg. 71.

16. Richard Beckhard and Reuben T. Harris, Organizational Transitions, Managing, Complex Change, second edition, Addison-Wesley, NY, 1987, Pg. 71.

17. Terence J. Mangan, Michael G. Shanahan, "Public Law Enforcement/Private Security, A New Partnership," FBI Law Enforcement Bulletin, Special Futures Issue, January 1990, Pg. 26.

18. Terence J. Mangan, Michael G. Shanahan, "Public Law Enforcement/Private Security, A New Partnership," FBI Law Enforcement Bulletin, Special Futures Issue, January 1990, Pg. 26.

19. Jill Kossow, Apple Computer Inc.

20. Jill Kossow, Apple Computer Inc.

21. Jill Kossow, Apple Computer Inc.

22. Catherine H. Conly, "Organization for Computer Crime Investigation and Prosecution," National Institute of Justice, Issues and Practices, July 1989, Pg. 45.

23. Catherine H. Conley, "Organization for Computer Crime Investigation and Prosecution," National Institute of Justice, Issues and Practices, July 1989, Pg. 39.