

**THE FUTURE OF COMPUTER CRIME
AND
LAW ENFORCEMENT**

BY

**LYNN E. BUTTON
COMMAND COLLEGE CLASS XVI
PEACE OFFICER STANDARDS AND TRAINING (POST)**

**SACRAMENTO, CALIFORNIA
JUNE 1993**

TABLE OF CONTENTS

	Page
PART 1: Introduction	1
Technology	3
Information	8
Computer Technology and Law Enforcement	9
The Government's Role in Technological Advancement	9
The Criminal Element	10
The Family Shift	12
The Hacker	13
Law Enforcement's Involvement	14
Epitaph?	16
Summary	16
PART 2: Future Study	19
Introduction	19
Phase I	20
Phase II	22
Trends	22
Events	24
Phase III	25
Phase IV	37
Phase V - Scenarios	39
Exploratory	40

U.S. Supreme Court Rules in Favor of M.O.D.	40
Hospital Techno Death...Husband Arrested	41
Electronic Crime Wave...A Bust for Law Enforcement	42
Hypothetical	42
Computer Smut King Goes Free	42
Search and Seizure at the Forefront of Rambo Computer User	43
Computer Group Marches on Capitol	43
Modified Hypothetical	44
Chief's Computer Crime Unit: A Model for the State	44
Hacker Crackers Meet with Computer Group	45
This Rambo is not Sly	45
 Phase VI - Policy Impact	 46
 Policy One	 46
Policy Two	46
Policy Three	46
 Conclusion	 48
 PART 3 - Strategic Plan Development	 49
 Introduction	 49
Strategic Plan	50
Macro	50
Micro	51
WOTS UP Analysis	51
Threats	52
Opportunities	54
Capability of the Organization	55
Strengths	55
Weaknesses	56
Stakeholder Analysis	57
Chief of Police	58
City Council	58
POST	58
Media (Snail Darter)	59
District Attorney	59
Court Judges	59
Computer Vendors	60

Telecommunications Companies	60
Department of Justice/Attorney General	60
Chamber of Commerce	60
Private Security	61
Developing Alternative Strategies	61
Strategy One	62
Pros	63
Cons	63
Strategy Two	64
Pros	64
Cons	65
Strategy Three	66
Pros	66
Cons	66
Stakeholder Perceptions	67
Strategy One	67
Strategy Two	68
Strategy Three	69
Strategy Choice	70
Implementation Plan	70
PART 4: Transition Management Plan	74
Introduction	74
Critical Mass	75
Chief of Police	77
The Fresno City Council	78
Fresno County District Attorney	79
Telecommunications Companies	80
Chamber of Commerce	81
Transition Management Structure	82
Implementation Techniques and Methods	84
Communication of the Vision	84
Role Model	85
Responsibility Charting	85
Computer Crime Project Team	86
Goal-Setting and Time Management	86

Rewards	87
Feedback/Evaluation Mechanism	87
Summary	88
PART 5: Study Conclusion	89
APPENDIXES	97
BIBLIOGRAPHY	105

TABLES

1.	Trend Evaluation	25
2.	Event Evaluation	31
3.	Cross-Impact Evaluation	38
4.	Cross-Impact Analysis	47
5.	Commitment Chart	77

PART 1

Introduction

The media continues to report the exploits of individuals using a computer for unlawful activity. Consider the following:

A fifteen year-old hacker used an Amiga PC to access two minicomputers at Grumman Corporation. Grumman makes the Navy's F-14 Tomcat and the A-6 Attack Bomber, and works on various supersecret defense projects. The fifteen year-old accessed the system while it was performing maintenance. When apprehended, the boy was in possession of passwords and information on company employees.¹

A twelve year-old boy was arrested for breaking into TRW databases, confiscating credit card numbers, and posting them on a computer bulletin board.²

The Gulf War saw hackers break into the U. S. Department of Defense computers to tamper with sensitive military information. Hackers from the Netherlands were responsible.³

A man filed phony electronic refund claims with the IRS by using social security numbers from people who normally did not file claims. He was then able to obtain speedy refund loans from banks. His checks averaged \$3,000, totalling nearly \$1 million. Since the IRS began offering electronic tax filing in 1986, they have been victimized by phony electronic refund thefts. The 1992 year saw \$17.6 million in phony electronic fund claims.⁴

An alleged out-of-state computer hacker was arrested by San Diego Police. The hacker agreed to cooperate with the San Diego Police Department and the FBI in the investigation of an electronic network. As many as 1,000 hackers between fourteen and twenty-five years of age had shared information for at least four years. The hackers accessed major computer networks such as Telenet, Signet, and Sprintnet; gaining entry into the computers of national credit card and credit reporting agencies. One hacker learned how to break personal security codes for ATM's. The ring is believed to be based on the East Coast and over time has probably been responsible for the theft of large amounts of money. Mastercard reported \$381 million in credit card fraud in 1991, and Visa International lost \$259 million in 1989.⁵

A computer programmer called the Dark Avenger, who resides in Bulgaria, creates viruses which infect computer systems. One East Coast company lost \$1 million as a result of infection by one of his viruses.⁶

A hacker charged 11,733 telephone calls costing \$1,600 during August of 1992 to an emergency telephone located along a major freeway.⁷

Two of five arrested young hackers, belonging to the "Masters of Disaster or Masters of Deception" underground hackers organization, pled guilty to accessing computers from Bank of America, Southwestern Bell, Martin Marietta, TRW Information Services, and New York University, among others, selling information such as people's credit reports.⁸

Kevin Poulson, a twenty-seven year-old computer hacker in federal prison, was indicted on several charges of possessing a copy of secret U. S. Air Force orders on one of his computer tapes.⁹

Two teenagers broke into a computerized voice mail system, changed the greeting to lewd messages, and placed bomb threats and erased customer messages and orders. The cost to the company was \$2.4 million. Stated reason: the teens did not receive a free promotional poster from Computerworld.¹⁰

A subscriber to America Online, an online service for computer users for information and entertainment, posed as a thirteen year-old, and accessed pictures of what appeared to be juveniles engaged in sexual acts.¹¹

The FBI is investigating Ross Perot's presidential campaign on allegations that workers accessed security codes and broke into computer systems of companies that issued credit reports.¹²

Jeffrey Cushing's teenage son spent hours over a computer keyboard playing games and communicating with friends. All was fine until a Garden Grove telephone company greeted him with a lawsuit, accusing his son of hacking long-distance lines to the tune of \$80,000. Telephone fraud is responsible for losses of \$5 billion a year or more. Giving kids a computer and a modem is like giving them a loaded gun. Thrifty Tel Inc. of Garden Grove estimates losses of \$22,000 a month due to such activities.¹³

A fictional account depicting the infiltration of a virus into a large computer conglomerate was the subject of John Randall's book, The Tojo Virus.¹⁴

Obviously, the aforementioned occurrences clearly indicate that computers are currently used unlawfully by criminal violators. For the purposes of study, computer crime is defined as an activity involving a person using a computer device for the purpose of accessing, taking, vandalizing, destroying or manipulating data without the permission of the owner of the data and/or system. The question arises as to whether the subject of computer crime is suitable for futuristic research. Futuristic research seeks to identify a topical area based on evolving trends and events. Pundits may ask why this area is worthy of consideration for the future. Driving forces today will cause the proliferation of computer crime into the future, greatly eclipsing present occurrences. The manner in which computer crime is viewed today will not be the way it will be perceived in the future. The driving forces listed below will dramatize the transformation of computer crime from today to what it will become in the future.

This study is concerned with the broad application of computer crime. Computer crime can be delineated into specific types such as terrorism, pornography, theft of assets, vandalism through computer programs such as viruses, employee vandalism, theft of trade secrets and other sensitive data, and marketing of stolen commodities. Thus the scope of this study treats these offenses in a general fashion.

Technology

Technological advancement can cause major shifts in society. As an example, the farmer was considered to be one of the mainstays of U. S. history. One hundred years ago, 42.6 percent of Americans were farmers; whereas today less than 3 percent are farming. Technology and economics have improved productivity to the point that the

number of farms and farmers have been reduced. The use of chemicals, better seed, improved farming techniques and advancements in mechanization are the reasons for the change.¹⁵

The ever-changing field of computer technology is an issue which will affect all police agencies. There is a plethora of literature concerning the ever-changing high-tech society.

The 1990's will bring a worldwide spread of technological research and product development. Technological development will occur not only in the United States, but overseas in other countries--partnerships with businesses in other countries will be created for the purpose of developing technology. Such partnerships will lead to globalization of technological research.¹⁶

There is a wide range of technological advances planned for the future. For example, technological advances for the automobile include the following: (1) radar/sonar, collision avoidance [1994], (2) in-dash navigation system [1995], (3) complete heads-up windshield display [1995], (4) rear seat and door-mounted air bags [1996], and (5) in-car parking structure reservations [1998].¹⁷

For the home of the future, high-tech toilets, automatic window controls, and motorized security cameras are slated.¹⁸ Personal computers will have the ability to recognize human voices in the not-so-distant future.¹⁹ Telephones will be carried in the pocket which will allow one to identify their callers and the nature of the call from any location.²⁰

Two IBM physicists, Donald Eigler and Erhard Schweizer, were able to position individual atoms which can lead to fabrication of new materials.²¹

Technology will continue to allow for the office to be portable. Notebook computers, fax modems, portable printers, cellular phones, satellite linked pagers, etc., currently make this possible.²²

With a computer, modem and permission, anyone can dial a commercial network and research an on-line encyclopedia, look for a job, shop for grants, groceries, or clothes. It took seventy-five years for the telephone to become a common commodity. Today, this is not so. Fax machines were scarce a few years ago; today they are virtually everywhere. People currently can pay for meals or groceries with a debit card. Eventually, voting and househunting will be accomplished via computer--even airlines have telephones. Faxes and access ports will be available via laptop computers. A few years ago cellular phones and pager devices were a novelty. Today, people can be paged from nearly anywhere.²³

Edward Cornish, a noted futurist, stated that some of the important issues for the 90's will revolve around a shortage of energy.²⁴ Mr. Charles Taylor, of the Army Corporation of Engineers, supports the energy shortage theory and believes that there will be a new order of nations by 2010, as industrial nations will need energy. Thus, energy will become a valuable commodity and computer hackers will focus their attention on the confiscation of energy.²⁵

An information "superhighway" connected by fiber optic cable will join scientists, students, educators, business people, citizens and others. The superhighway will virtually

allow everyone the ability to communicate and access any number of information sources.²⁶

The past history of the Industrial Revolution is fraught with inventions which took several years before they were suitable for society's use. Today, a discovery may be available in from three to six months. One of the most memorable names in computer litany is Univac. The installation of the Univac computer at General Electric in 1954, designed to perform the payroll process, was met with doubt.²⁷

The emergence of computer technology over the past thirty-five years has been phenomenal. Change over the past decades from the Univac to the personal computer (PC) has been revolutionary.²⁸ Today, department stores such as Sears and Montgomery Ward are selling computer machines to households. It is estimated that during the late 1980's personal computers were in 20 percent of single-family homes. Eighty percent of the homes will have computers by the year 2000,²⁹ and Alvin Toffler's description of the "electronic cottage," which focused on the future of work being performed from the home, will come to fruition.³⁰ Homeowners will be able to shop, bank, communicate, and develop elaborate security measures for home and personal use. The potential exists for the resident to leave an electronic message with the police beat officer regarding vacations, meetings, suspicious activity, or crime tips. It is conceivable that some reports could be typed and sent electronically to the police station by the resident.

The effect of computer development was felt on the international level recently with the war in the Middle East. The "Electronic Warriors" and the dominance of the

electronic battlefield caused the impotence of Iraq, and the on-board computers of the aircraft provided the initial demise of the Iraqi forces.³¹ Mr. Frederick Mintz, of the Jet Propulsion Lab, was asked a question at a command college class regarding the amount of technology used in the Middle East War. He replied that only 60 percent of available technology was utilized.³²

Expert systems, artificial intelligence, neural networking, virtual reality, parallel processing, and robotics are some of the budding technologies which have the computer as their brain center. The advancement of these areas will provide all of society with quicker, cheaper, and more efficient ways of performing tasks. This technology is credited to the advancements of the computer and the microchip. The amount of transistors which can be placed on a chip surface is beyond comprehension. Intel, the chipmaker, has already developed the 486 chip which contains 1.2 million transistors and runs at 100 mHZ. This is monumental when compared to the first PC from IBM, which ran at only 4.77 mHZ. A new generation of super-computers can process 1 trillion floating operations per second.³³ By 1999 a \$350 workstation capable of 15 million instructions per second is envisioned.³⁴

The quotes which follow emphasize technological advancement and its competition with real-life activities:

High-resolution printers and scanners are being used by criminals to counterfeit checks and commit other acts of forgery. American Micro Systems Inc. discovered four counterfeit checks returned to the company from its bank, NationsBank in Atlanta, totaling \$1,300; but the loss to the company was actually much higher because it had to cancel its checking account and resubmit credit applications to all its customers. Chemical Banking Corp. Assistant VP of the Information Technology and Operations

Group Christopher Dowdell estimates that fraud using computer technology increases by almost 100 percent annually.³⁵

Electronic fund transfers are used by people as an alternative to physically taking money out of the country. This is accomplished by depositing money into a bank and then transferring the money electronically to domestic or foreign banks, financial institutions, or security accounts. Normally, money transferred by wire to Switzerland is pre-washed in a third country such as Panama, Luxemborg, or the Bahamas.³⁶

The extinction of physical money may soon arrive:

Electronic cash transactions, without the presence of physical money, is within reach. Eighty percent of Americans use credit cards and companies such as Visa and Mastercard handle tens of billions of transactions per year. A National Electronic Money Debit Card System would be possible. Money earned would be transferred to an electronic account and the owner would be able to purchase goods and commodities with the debit card. The system would be federally operated. Electronic security is a real concern due to frauds, electronic thefts, and breaches by hackers.³⁷

Information

Information will be a driving force in the upcoming decades; those who can create, process, and network will be the most successful.³⁸

The amount of information available to us will be astounding as machines and processing become faster, cheaper, and more accessible. Law enforcement, whether it be at the national, state, or local level, will also be able to access information from a variety of sources. Such advancements will create machines which will be able to equip officers with current and thorough information at a faster rate. Through the conception and implementation of centralized databases, information can be afforded to the police, particularly during extreme emergency situations where life is at stake. The drawback to this idea is twofold: first, "Big Brother" is watching you; and second, there is a question regarding the invasion of privacy. However, anyone who owns a PC today can access this

information. There are plenty of on-line databases that allow one to do just about anything without touching a manual.³⁹

Information databases can reveal the name of a person, the social security number, address, and spouse's name, among other data. All such data can be accessible from home by a knowledgeable PC user.

Computer networking will take privacy loss a step further. The history of people will be on a single database able to be accessed by all.⁴⁰ Terranet, a public/private venture in Ontario, Canada, placed 4.5 million land parcels onto a computer network for better public access. A politician claimed the easier access was an invasion of privacy. The information was available to the public via paper; however, the computer will make access easier and cheaper. The information, which can be accessed via computer, leads to a concern by some that sheer volume of information will lead to an electronic Three-Mile Island.⁴¹

Computer Technology and Law Enforcement

The growth of computer technology will unequivocally affect law enforcement. The effect will be explained from two perspectives; one perspective rests with government's ability to keep pace with the information/computer explosion, and the second perspective rests with the criminal element and their behavior.

The Government's Role in Technological Advancement

National, state and local governments have come to rely on computers. Today national, state and local economies are not fiscally sound and more demands are being placed on police administrators to produce more for less. Many politicians and citizen

activists are voicing concerns for the "most bang for the buck." Lack of resources has forced government to look for efficient and economic ways to accomplish tasks. Thus, computers are often justified and installed with the major purpose being the elimination of personnel costs, particularly since such costs consume 80-85 percent of general fund budgets. Consequently, entities are forced to shave dollars with automation as the answer.

The acquisition of technological equipment such as computers is often delayed by several factors. Possession of information implies accountability which often results in the phenomena of political amnesia. Politicians forget the agreements of well-laid plans and succumb to special interest pressure. In other words, when under the gun, cut everything!

Another dilemma is the purchasing process. Computer technology changes so fast that by the time government decides to purchase an item, the item is out of date. Even if the item were state of the art at the time, the purchasing process of equipment is difficult. The same problem holds true with software applications. Software vendors enhance their versions at a rapid pace, and some jurisdictions are not able to purchase an upgrade in a timely fashion.

The Criminal Element

The more formidable of the two perspectives affecting law enforcement involves the criminal element. The amount of money which is transferred over electronic data lines is staggering. Last year an estimated \$250 trillion was spent. Approximately .01 percent for cash, 1.5 percent for checks, and the remaining 98.5 percent of money

transmitted was sent via electronic fund transfer technology which consists of wire transfers, automated clearing houses, automated teller machines, point of sale, and telebanking. FEDWIRE, officially named the Federal Reserve Communications System, is a non-profit organization which has fourteen large-scale computers. In 1988, this system transferred \$150 trillion with an average transaction of \$2 million. Presently, it is estimated that 80 percent of daily financial exchanges occur via electronic fund transfers and computer-related crimes are costing American companies \$5 billion a year.⁴²

Should electronic theft be a concern? The average computer theft is between \$475,000 and \$560,000. It is no wonder that devious minds are attracted to this type of criminal activity. Compare this figure to an average of \$19,000 taken in a bank robbery.⁴³ A tremendous amount of time, effort, and publicity is spent capturing bank robbers and the electronic thief is being ignored. The sale of stolen goods, prostitution and pornography schemes, frauds, thefts, and vandalism (viruses) to our computer systems are costing the taxpayers dearly.

Estimates suggest that computer criminals in the workplace may cost businesses up to \$3 billion per year.⁴⁴ Reported computer and telecommunications crime losses amount to \$555 million per year, with unreported losses estimated at \$5 billion annually.⁴⁵ In 1991, the FCC reported that nearly \$500 million in fraudulent calls are placed through corporate PBX's each year.⁴⁶

On August 23, 1993 Julie Tamaki and Michael Connelly reported in the Los Angeles Times that:

The combination of computer knowledge and magnetic strip encoding equipment contributes to costly fraud cases committed against the credit

card industry. Los Angeles is suffering widespread perpetration of computer and credit card crimes committed by offenders that include teenagers. The U. S. Secret Service Agency in Los Angeles makes credit card encoding arrests on an almost-weekly basis. Encoding fraud accounted for \$39 million in losses for Visa International in 1991, up from zero losses in 1989. Criminals obtain valid credit card numbers illegally then sell the numbers to those who in turn encode the magnetic strip on the back of their own credit cards. The solution to this crime involves comparing the computer-generated receipt with the number on the credit card.⁴⁷

The number of attempts to steal data via computers and telecommunications has tripled over the last five years. More than one-third of the 165 Fortune 1000 firms reported thefts or attempted thefts of corporate secrets.⁴⁸

An added dimension is the threat of terrorism and theft of national defense information, as was the case described in the book "The Cuckoos Egg." This book depicts Cliff Stoll's account of his discovering hackers from Germany who were bent on accessing secret military defense and nuclear weapons information from the computer banks at the Lawrence Livermore Laboratory.⁴⁹ There have been reported cases of hackers breaking into police departments, hospitals, colleges, schools, and other business and government institutions.

The Family Shift

Children today are exposed to and use electronic gadgets from telephones, VCR's, video cameras, and computers with a variety of applications such as Spell Check and Grammar Correction. Middle-class children are conducting business with microchip products which can be purchased from Sears, Wards, Macy's and other retail outlets. The family does not interact with household members. Interaction occurs between the children and their friends in bedrooms via computer modem. Thus, the biological family

has been supplanted with the electronic family. Today 72 percent of households have video recorders, 78 percent have microwaves, and nearly 50 percent have computers at home or have access at school, up from less than a third in 1984.⁵⁰

Sacramento, KXTV CBS Channel 10 recently aired, as their opening story, interactive video programs featuring computer pornography or hard-core software. People will have digital sex.⁵¹ If children are spending time in their bedroom they will have access to these types of programs.

The National Institute of Justice sponsored three studies on the topic of computer crime. One conclusion reported computer criminals obtaining their skills at a very early age, usually from school. The children usually start by copying software and move through a transition period up to credit card fraud. Their beliefs and information stem from contacts with other hackers.⁵²

The Hacker

The attitude of the hacker is one in which they believe information is for everyone to access. The question of privacy will surface in the future, having a bearing on information storage and access. Cyberpunks, who roam the techno underground, are computer cowboys in a world of bitstreams and databases inside computer networks. With the tap of a key, they claim they could effectively cripple the economy or shut down communications systems the world over. If that is true, then Cyberpunks hold the potential for becoming the most powerful counter-cultural force ever.⁵³

To compound matters, Mitch Kapor, founder of Lotus Development Corporation and Creator of Lotus 1-2-3, has founded an organization named Electronic Frontier

Foundation (EFF) to defend people charged with computer-related crimes. The group is concerned with protecting constitutional rights and fostering creativity within the computer industry. They believe penalties should be given to those for unauthorized access to computer systems. Part of EFF's intent is to ensure that ordinary people are free to access information.⁵⁴

Law Enforcement's Involvement

A drug dealer buys a computer and via an E-mail hookup, conducts his business of illicit drug marketing. The reason this is possible is twofold: (1) computer system hardware and software is affordable, and (2) computer literacy among criminals is increasing. Criminals are moving beyond cellular phones and digital pagers to computer systems.⁵⁵ The information presented previously identifies a member of the criminal society moving toward computer usage conducting his illicit trade. Law enforcement is the logical entity to address such abuse; however, its current position is tenuous at best. For example, computer crime is a more esoteric and unusual crime than burglary or assault. Many law enforcement officers do not understand it, and because it does not involve physical danger to anyone it is likely to get low priority treatment when it comes to investigations and prosecution.⁵⁶

James Daly, in his article on telephone toll fraud, stated that:

Telephone toll fraud is quietly and insidiously picking corporate America's pockets. In fact, unauthorized calling has gotten so bad that U. S. businesses will pay the bill to the tune of \$4 billion in 1992. A call/sell operation attracts drug dealers, organized crime and illegal aliens, and skilled hackers can originate calls through private branch exchanges (PBX) and prevent the calls from being tracked. Furthermore, law enforcement officials believe the problem is only going to get worse.⁵⁷

The state of California enacted California Penal Section 502 entitled, "Computer Crimes" which took effect January 1, 1990. It was the intent of the legislature to criminalize computer crime based on the proliferation of computer technology. Based on a 1990 survey, 18 percent of police and 12 percent of sheriffs and prosecutors had an individual unit that specialized in computer crime.⁵⁸

The section is comprehensive and seeks to protect "individuals, businesses and government agencies from tapping, interference, damage, and unauthorized access to lawfully created computer data and systems."⁵⁹

Penal Code Section 502.01 allows for the investigating government agency to seize the physical computer components and computer programs for violation of the computer crime statute.⁶⁰

Silicon Valley is located in Santa Clara County, home to many computer enterprises. An interview with Mark Haynes, Supervisor for the Economic Crimes Unit, Santa Clara District Attorney's Office, reported that computer crime is a growing commodity. The paper office will soon turn to a binary society or paperless society. Computer storage will be the container of data which will make it ripe for crime. Once money is extended to the debit card from traditional means, the criminal will have to adapt and pursue communications theft.⁶¹

Unfortunately, the criminal justice system is slow to act and law enforcement has trouble catching up with technology. The police are preoccupied with traditional crimes such as robbery and burglary. The public is also preoccupied with these types of crimes.

Thus, economic crimes, due to their low visibility, do not receive an immediate response.⁶²

Computer crime is serious in nature and law enforcement is behind the times; however, the police are expected to curtail this type of activity. The electronic thief steals state of the art equipment, hacking their way to riches. They have no budget process. Unfortunately, law enforcement has placed little emphasis on the computer criminal and must beg and purchase equipment with tight budgets.

Epitaph?

Computers form a common bond with all people, particularly when the vast majority will have access to them. In an interview with Isaac Asimov, he stated that computers will reduce brain-numbing work allowing more time for other activities and more toward learning. Interactive devices will emerge to occupy free time. This will enhance the learning atmosphere and people can learn because of the pleasure involved.⁶³

Summary

Several driving forces were examined during this chapter. It is the development of these driving forces which will alter the perception of computer crime in the future.

Technology is increasing at an exponential rate. More people will become dependent upon technology, as electronic components become more powerful and smaller in size. There will be increased opportunity for everyone to possess such devices. Information will be accessible by anyone, particularly since 80 percent of the homes by the year 2000 will have a computer. The migration to a debit card system and the

elimination of physical money will cause criminals to develop new technological talents. Historically, law and the criminal justice system have been slow to react to technology. The criminal element does not seem to possess this problem. Government has not kept abreast of technological advancement, admittedly due to fiscal constraints. The law enforcement community is very slow to respond to computer crime, often categorized as a white collar crime offense.

The change in the family is of grave concern, especially when parents, most of whom have not been exposed to computers, do not interact with their children because "junior is interacting with his electronic family." In the past, hackers infiltrated computer systems for the purpose of challenge, growth, and experimentation. The hacker of tomorrow will not have the same kind of "ethical" understanding of hacking and will have the potential to cripple any government or private organization.

Lastly, law enforcement's failure to reprioritize their efforts is indicative of their lack of foresight. This point is particularly evident when comparing the cost of a bank robbery to that of a computer crime.

All of the above described driving forces point to a potential turbulence for society. What makes this issue so important is the fact that the computer criminal of the past accessed computer systems via large machines located at businesses, universities, or another remote location. The difference is that in the future, virtually everyone will possess a computer. An unsophisticated barometer, yet astute observation, is that computers can be purchased nearly anywhere today, even at large department stores.

The prices are affordable and people can purchase computer systems via credit card accounts.

Society will eventually evolve into a "smart" culture, meaning that the environment will be controlled by computer technology. The computer criminal will subsequently adjust to a level of sophistication whereby future crimes will be committed through the use of a computer. This will be of concern to all in the future.

Someone will have to contend with computer wizards who cover their tracks without detection. Businesses may become bankrupt because computer pirates are stealing their assets. Will society keep pace with technological change and will governments or politicians allow law enforcement to do so? By the year 2000, law enforcement's Armageddon may very well be the collision of information, computer technology, and the computer criminal. Consider this quote from the book Sneakers, which was also a major motion picture:

The world runs on information--it's the one true international currency. This is pure power, the main vein to the universal juice, all of it.

Cosmo moved in close, speaking with great urgency. "The world isn't run by weapons anymore, Marty," he said. "Or oil, or even money. It's run by little ones and zeroes. Little bits of data. It's all just electrons." . . . it's about who controls the information.⁶⁴

PART 2

Future Study

Introduction

Law enforcement has seen enormous change during the past decades, with many factors causing or creating the change. Factors such as shifts in social values and structures; spontaneous war conflicts; socio-economic clashes between cultures; environmental movements and incidents; seemingly cyclical political shifts of power; and the advancements of technology, particularly that of computerization; are but a few trends which have caused us as a society to change. It is the area of computerization which seems to change faster than one can blink an eye.

Law enforcement must pay strict attention to new technological developments and keep pace with the chameleon-like change in computerization. Technology causes change and if there is a lack of attention to the change, hazardous situations can arise and law enforcement will have to answer to or for the hazard.

Changes in availability, size, speed, power, and ease of computer use are being thrust upon us in rapid succession. Society will make the transition and move forward with this new-found technology. If law enforcement does not keep pace, it may suffer the consequences from a criminal subculture which continues to use the very technologies available to commit criminal offenses. Thus is born the concern for law enforcement to ensure that society is protected from *all* criminal elements, regardless of how the criminal chooses to commit his crime. The criminal who uses a computer to perpetrate offenses has increased potential to be very destructive.

Scanning of periodicals, newspapers, books, bulletins, and interviews with persons knowledgeable about computer technology have led to the question of computer technology and crime. A process was used in organizing collected data for the research. Articles of the data were classified in the following categories: social, technological, environmental, economic and political (STEPP). The process allowed for identification of issues, trends and events. The researcher developed the issue and a police specialist from the Fresno Police Department, who is an expert in computer crime, discussed the sub-issues which relate to the issue.

Phase I

The issue and sub-issues concerned with the aforementioned are:

What impact will computer crimes have on a large law enforcement agency by the year 2002?

A futures wheel, a technique used to assist in the identification of issue and sub-issue impacts, was used to identify three sub-issues for future study (See Appendix A):

Will the responsibility for investigating computer crimes rest with law enforcement?

Shrinking revenues, budget cuts, and lack of computer expertise may be some of the reasons to question law enforcement's ability to investigate computer crimes. Conversely, there is a sense of duty to protect all citizens from the criminal elements, and law enforcement historically devotes resources to this task. Thus the large law enforcement agency may or may not be responsible for investigation of computer crimes.

What type of training and education will be needed by the investigating body?

Training and education will be a concern for any unit investigating computer crime. The complexity and diversity of computer crime offenses makes them different than traditional law enforcement criminal investigations. The need to educate and train investigators, first responders, and management on this type of crime will be necessary. Training personnel in the area of computer crime can impact any department's budget.

How will the investigating unit keep pace with technology?

The concern for the investigating agency will be whether their budget will allow for the updating and or upgrading of equipment and training. A large law enforcement department's budget can be impacted if new computer programs and computer systems are needed due to technological advancements.

Once the issue and sub-issues were identified, a panel of seven people were selected to participate in a nominal group technique process. This group was formed in order to identify trends and events which may impact the issues at hand. The group was composed of people from different areas within government and the community. Members of the group represented the following: a crime analysis unit supervisor, a large-city computer services programmer, a state-operated law enforcement section criminal investigator who possesses expertise in computer crime investigations, a police

manager in charge of investigation of white-collar crime and fraud, a police manager who is experienced in future trends and events forecasting, and a systems analyst in the private sector who has also taught computer courses at a major university (Appendix B).

The group was asked to identify trends which would impact the issues. A trend was identified as "a drift, inclination, or tendency that currently exists or could exist." The panel developed twenty-seven trends (Appendix C).

The panel was also asked to develop events which would have the probability of impacting the issues. An event was identified as "something that would happen or happened and may reoccur or could potentially happen at a specific time and/or place." The group identified twenty-five events (Appendix D).

Phase II

The panel reviewed each trend and was asked to identify the five most likely and important trends which related to the issues. Independent selection of the trends was critical in an effort to minimize the possibility of bias or persuasion to any one trend. The panelists were asked to submit the number of the trend and their rank order on individual cards and give them to the moderator. Scores were given to trends selected and the five most important trends were selected.

Trends

1. Availability of information. Information on individuals in massive databases, along with many other services going on-line, enables anyone with a computer to access

1. Availability of detailed facts for any type of purpose. Concomitant with this availability of information is the rapid growth of technology and ease of obtaining computers.
2. Level of security development and standards for computer systems. Security of computer information has not been a priority in many computer applications and settings. One need only consult the media to learn of the latest virus which has created havoc among computer users to see that security is infantile. There are also many different computer vendors and operating systems. This diversification leads to a lack of standards and lends itself to victimization.
3. Acceptance of shared ethics for computer use. Ethics are of little concern for computer users who tend to work their way into someone's computer system. There is little remorse or respect of privacy when the hacker community believes information is open to the public.
4. The use of electronic fund transfer. The ease of obtaining computers, the availability of information, and the lower cost of operating a business have caused the private sector to offer services from any remote location via computer technology. Use of the ATM card is an example of obtaining money from remote locations. If computers in the home become the norm, then electronic banking, shopping, computer-based instruction, and other conveniences heighten the attraction of criminal behavior.
5. Level of funding to investigate computer crime violations. This type of offense will need resources for investigation purposes along with ways to proactively

prevent criminal conduct. The investigation unit will need personnel trained in this area along with the equipment for detection and solvability.

The panel was asked to identify five events from the list they had developed which had a high probability of occurring. The process used in selecting the trends was also used to identify the five events, which appear as follows.

Events

1. Judge rules violation of the Fourth Amendment. A United States Supreme Court will rule that evidence used to convict a computer criminal was in violation of the fourth amendment's search and seizure statute.
2. Hacker sets-off major military movement. A computer hacker will crack the security code of a military base and send directives which cause mobilization of a military unit.
3. Sophisticated criminals form organization. A national effort on bulletin board networks will organize hackers from all parts of the country in retaliation to the pressure set forth by government bodies for criminal computer offenses.
4. Police contract computer crimes investigation. Many police agencies will contract computer crimes investigations to private firms.
5. Hospital patient dies. A computer hacker bypasses a security system of a major hospital and changes the data of a patient, who subsequently dies as a result of the tampering.

Phase III

The panelists were asked to forecast the trends and events. The trends were evaluated first and the group was asked, on an independent basis, to forecast where the trend was five years ago from today, where it will be five years from now and ten years from now. Regarding the future, the panelists were asked where each trend will be (explorative) and should be (normative). The table below depicts the panel median for the data requested.

Table 1

TREND EVALUATION

N = 7

Trend	5 Years Ago	Today	5 Years From Now	10 Years From Now
Availability of Info	25	100	300/150	400/200
Security Standards	90	100	120/200	200/400
Ethics of Computer Use	90	100	110/200	110/400
Electronic Fund Transfer	50	100	200/200	250/200
Funding for Investigating	10	100	110/200	200/400

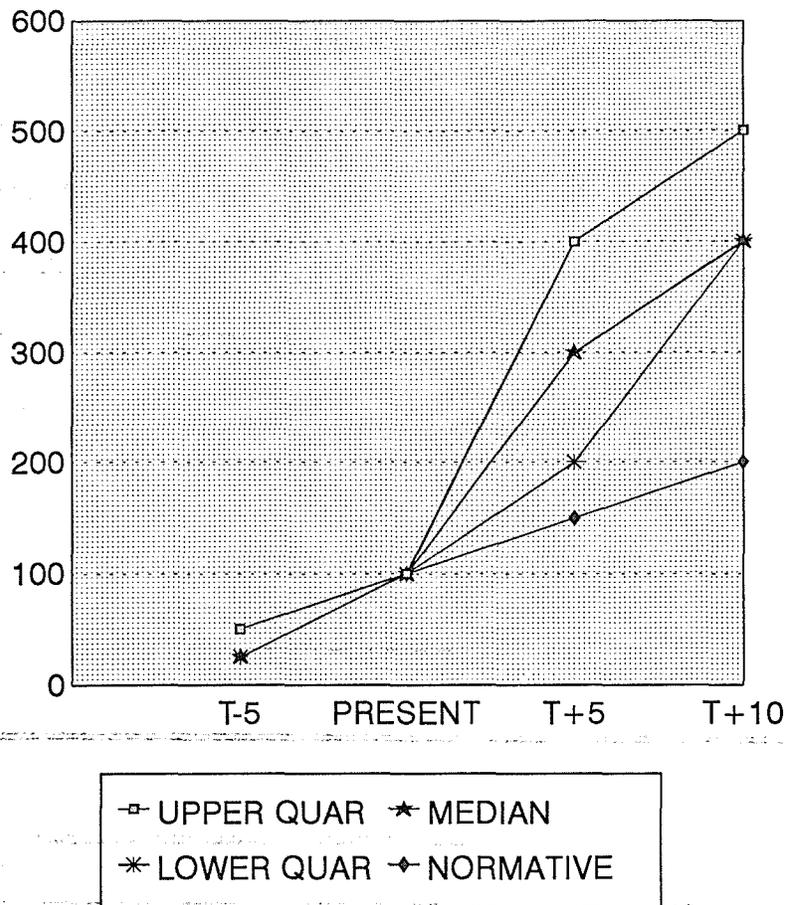
Will be/
Should be

Will be/
Should be

The following charts more clearly depict each trend, the interquartile upper and lower forecast points, the media or explorative point which illustrates where the panel believes the trend will be, and the normative point or where the trend should be.

TREND ONE

AVAILABILITY OF INFORMATION

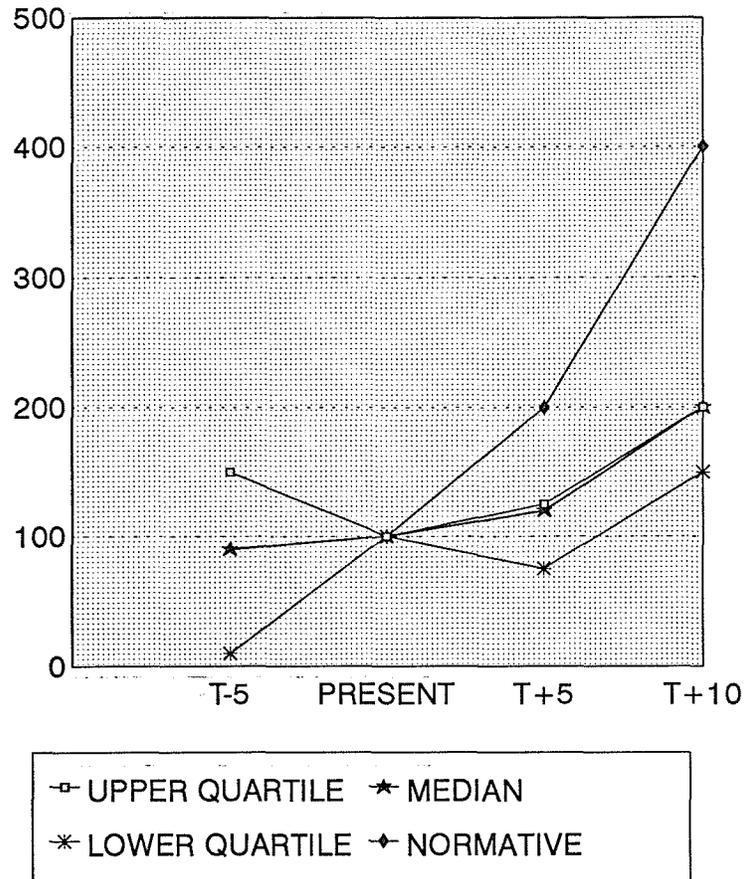


Trend One shows the panel's forecast as to the availability of information increasing from where it was five years ago to tripling five years from today. The median and lower quartile points were identical from T-5 to present. Interestingly, the panel felt that the information *should* be less available than where they believe it *will* be. The panel believed that there will be inadequate controls of information and that any person with access to a computer will be able to manipulate data for their own cause.

TREND TWO

SECURITY DEVELOPMENT AND STANDARDS

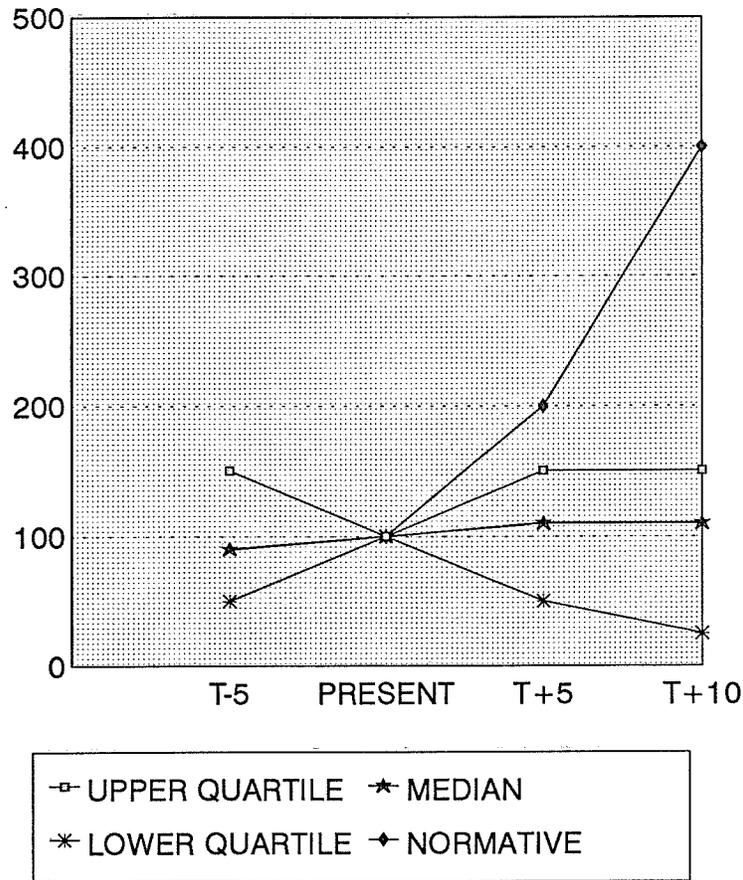
27



Trend Two shows that the panel believes security development and standards should be significantly higher ten years from today. There was a consensus that, in the exploratory or "most likely" future, today's level will only double in ten years.

TREND THREE

ETHICS OF COMPUTER USE

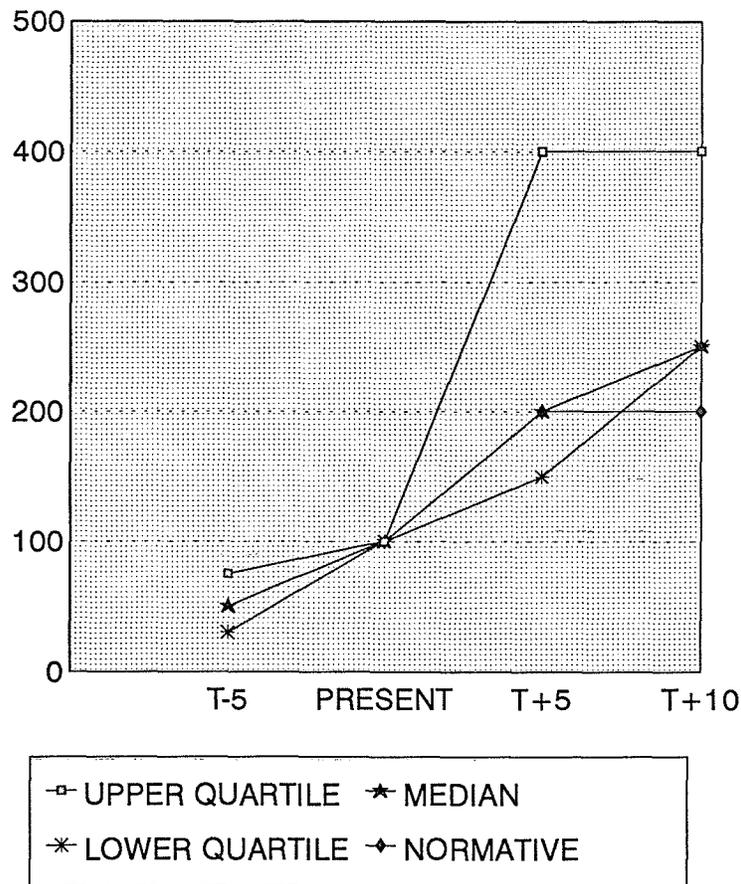


Trend Three shows that the panel believes the existence and concern for ethical standards in computer usage will increase only slightly over the next ten years. The panel believed that government will not respond soon enough to the need for ethical standards due to bureaucratic red tape and court challenges relating to privacy of information. It was their consensus that the concern for computer ethical standards should be four times greater than it is presently.

TREND FOUR

ELECTRONIC FUND TRANSFER

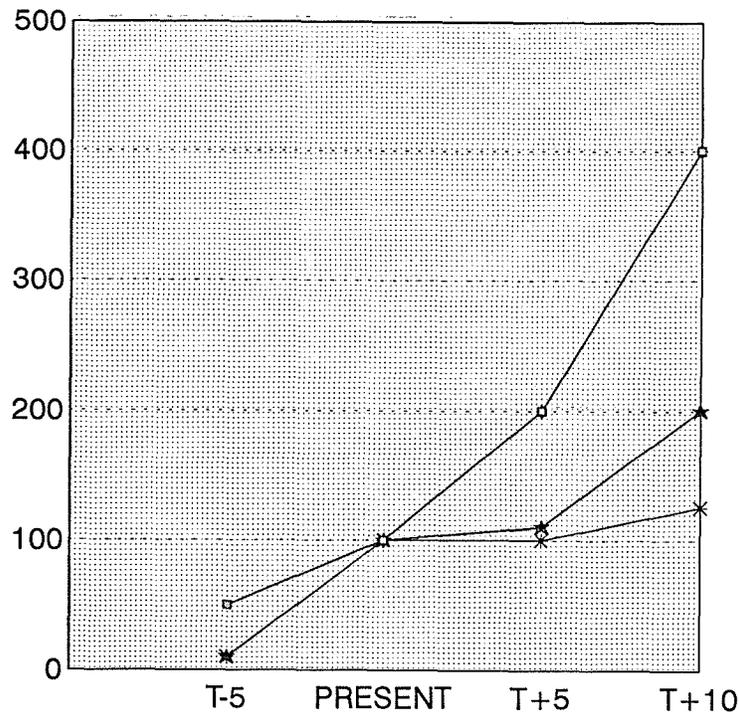
29



Trend Four shows the panel believing that the transfer of money via computer will continue on an upward swing and double from present to T5. There was no increase from T5 to T10 during the normative expression. The group, in its normative expression from T5 to T10, generally believes that government will not place a high priority on electronic crime matters. Therefore, they feel that there will be a greater opportunity for crime to flourish as growth of electronic transfers continues.

TREND FIVE

FUNDING TO INVESTIGATE COMPUTER CRIMES



□ UPPER QUARTILE ★ MEDIAN
* LOWER QUARTILE ◆ NORMATIVE

Trend Five shows the panel believing that funding for investigating computer crimes will be half in ten years of what it should be. The upper quartile and normative points from present to T+10 were identical. The lower quartile and median data were the same from T-5 to present. The panel believed that in ten years funding should be four times higher than the present, and consistently reiterated that government will be slow to consider crimes via computer as a high priority.

The panelists forecasted each event individually. The event evaluation forecast focused on the years to first probability of occurrence, probability of the event by five years and ten years from today, and whether there would be a negative or positive impact on the future, if the event actually occurred. There is a positive impact on Events Two and Five because the panel believed that it will take a significant occurrence to motivate change regarding government's computer crime attitude. The following event evaluation table indicates the median scores.

Table 2

EVENT EVALUATION

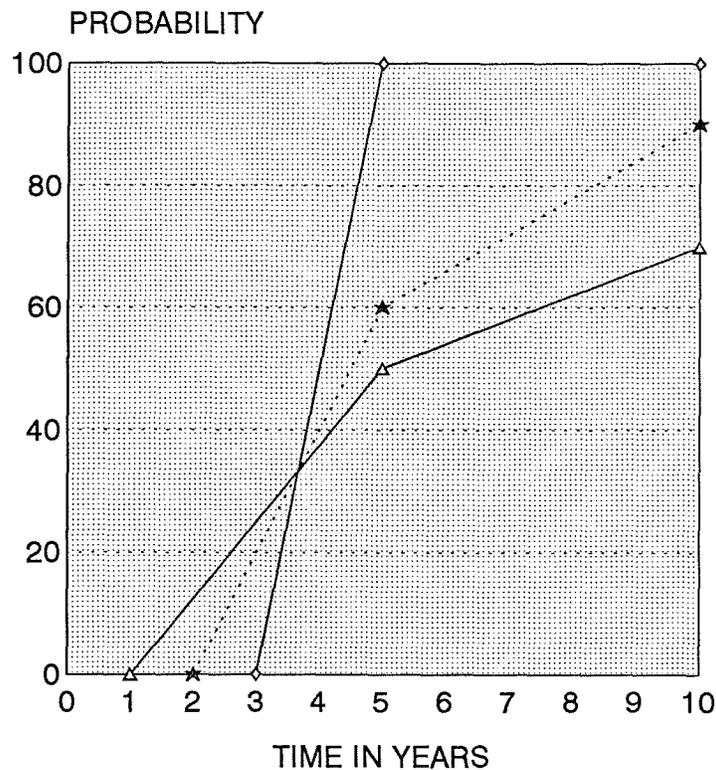
Event	Years > Than Zero	5 Years From Now	10 Years From Now	Pos	Neg
Judge rules Fourth Amendment	2	60	90	0	10
Hacker: Military Move	4	25	70	4	8
Hackers Organize	2	50	75	5	5
Police contract	2	50	75	5	5
Patient dies	1	50	80	4	5

The following charts depict each event. The interquartile range is shown along with the median.

EVENT ONE

JUDGE RULES ON 4TH AMENDMENT

32



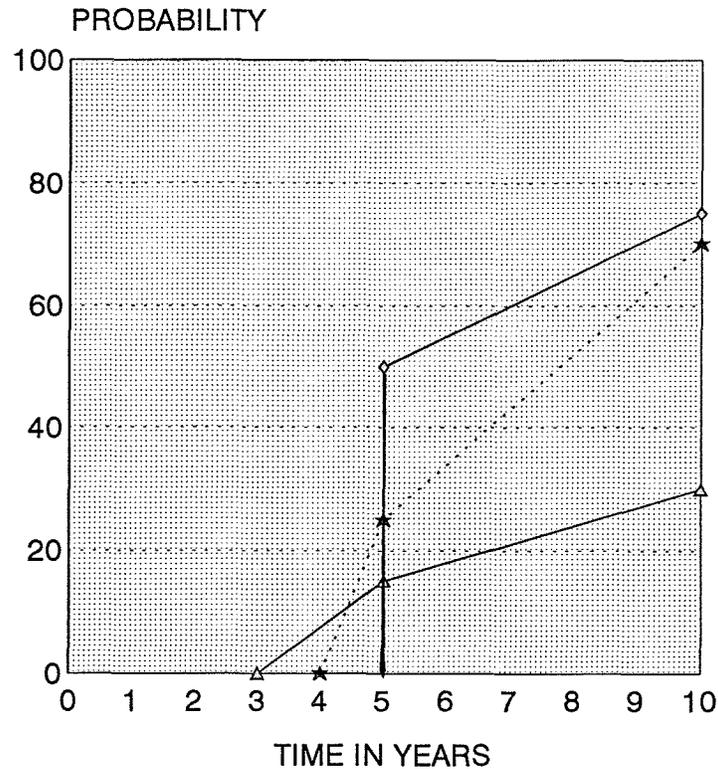
◇ UPPER QUARTILE * MEDIAN △ LOWER QUARTILE

Event One shows the panel believing that the event has a significant chance of occurring, particularly between years 2 and 5. The group believed this event would have a negative impact on the investigating body's ability to thoroughly investigate criminal violations. Added legal procedures, and procurement of search warrants are examples of activities which would hinder the process.

EVENT TWO

HACKER STARTS MILITARY MOVEMENT

33

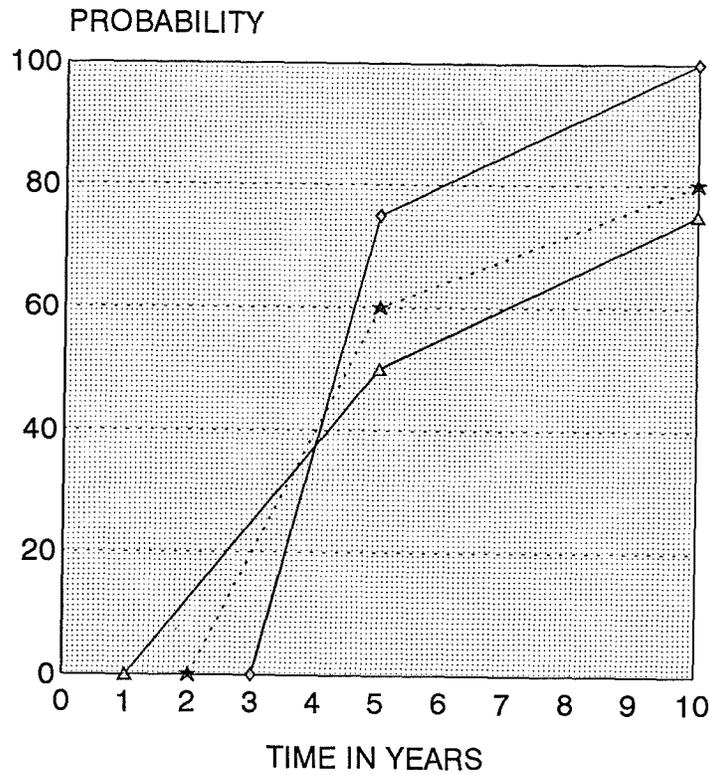


◇ UPPER QUARTILE * MEDIAN △ LOWER QUARTILE

Event Two shows the panel believing that the probability of a hacker starting a military movement has a high chance of occurring within the ten-year study period. There was twice the negative impact versus positive impact. The military represents government and is therefore often the target of dissident individuals or groups. The group felt that once law enforcement becomes involved in investigating computer crime, hackers will utilize their talents to impede the activities of any type of government institution.

EVENT THREE

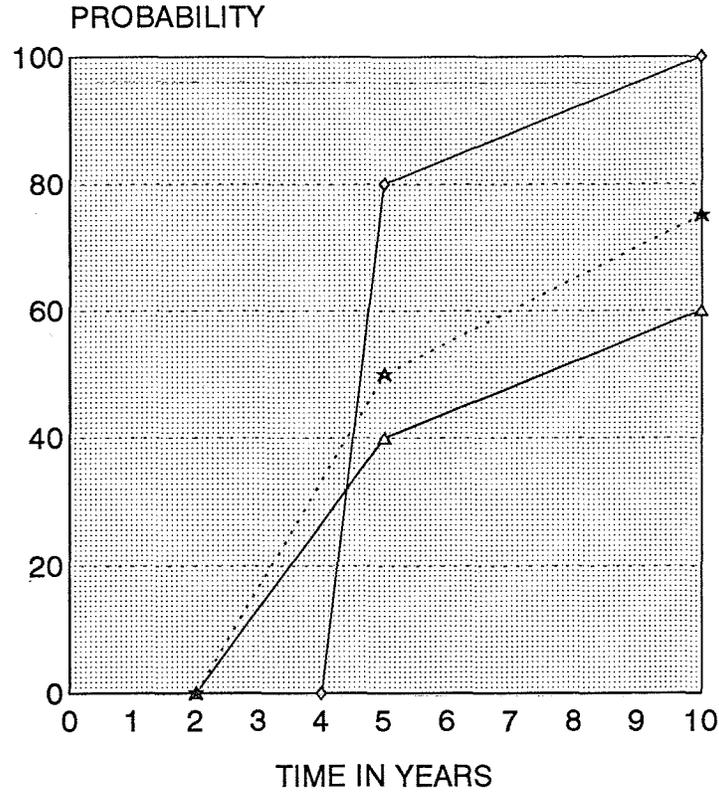
HACKERS UNITE



◇ UPPER QUARTILE * MEDIAN △ LOWER QUARTILE

Event Three shows the panel believing that if there is a significant push to crack down on computer crimes and hacking, there will be a high probability that hackers will unite. The group felt there was no positive benefit and a high negative impact.

EVENT FOUR
POLICE CONTRACT COMPUTER CRIME UNIT WITH PRIVATE SECTOR

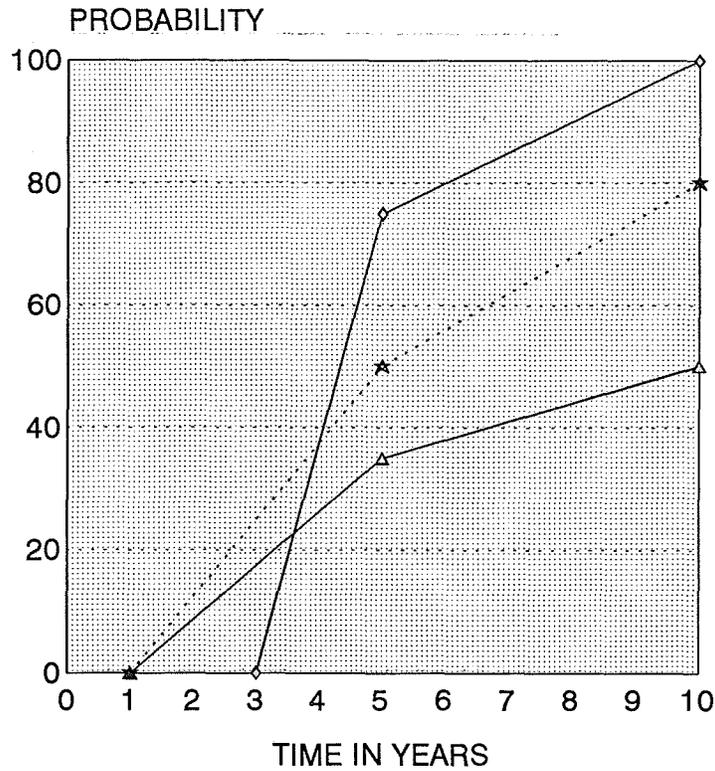


◇ UPPER QUARTILE ★ MEDIAN △ LOWER QUARTILE

Event Four shows the panel believing that law enforcement has a high probability of contracting the investigation of computer crimes between five and ten years. The positive and negative impacts were equal.

EVENT FIVE

HOSPITAL PATIENT DIES FROM HACKER



◇ UPPER QUARTILE * MEDIAN △ LOWER QUARTILE

Event Five shows the panel believing the probability of a patient dying from a hacker tampering with their medical chart to be high. The median illustrates a probability of 50 percent in five years increasing to 80 percent in ten years. There was a positive impact associated with this event because the panel felt that it would take an event such as this to make people aware of the magnitude of this type of behavior. The negative impact was at the mid range.

Phase IV

A cross-impact analysis evaluation was done to determine what impact the occurrence of each event would have on the forecasted probability of the other events and to see how the occurrence of each event would affect the forecasted level of each trend. This writer and another police lieutenant completed the process. Each worked independently of the other and surprisingly, the outcome was very similar with very minor differences. The differences were based on interpretation of how an event would impact the other events and trends and the number of years before the trend or event would occur. The table below illustrates the results of the cross-impact evaluation.

Table 3
CROSS-IMPACT EVALUATION

<u>Maximum Impact (% change +/-)</u> <u>Years to Maximum</u>											
	E1	E2	E3	E4	E5	T1	T2	T3	T4	T5	ACTORS
E1	X	$\frac{+30}{4}$	$\frac{+10}{2}$	$\frac{+40}{5}$	$\frac{+30}{4}$	$\frac{-10}{3}$	$\frac{+30}{2}$	$\frac{-30}{2}$	$\frac{-10}{2}$	$\frac{-30}{3}$	E1 9
E2	$\frac{-30}{5}$	X	$\frac{-30}{5}$	$\frac{-10}{4}$	$\frac{-0}{0}$	$\frac{-50}{2}$	$\frac{+40}{3}$	$\frac{+30}{3}$	$\frac{+10}{2}$	$\frac{+30}{3}$	E2 8
E3	$\frac{+40}{3}$	$\frac{+10}{6}$	X	$\frac{+20}{3}$	$\frac{+20}{4}$	$\frac{+30}{3}$	$\frac{+20}{3}$	$\frac{+10}{4}$	$\frac{-5}{4}$	$\frac{+30}{2}$	E3 9
E4	$\frac{+20}{4}$	$\frac{-0}{0}$	$\frac{+40}{2}$	X	$\frac{+10}{5}$	$\frac{0}{0}$	$\frac{+20}{4}$	$\frac{+25}{3}$	$\frac{+30}{3}$	$\frac{-20}{2}$	E4 7
E5	$\frac{-30}{5}$	$\frac{-5}{5}$	$\frac{-5}{6}$	$\frac{-30}{3}$	X	$\frac{-20}{4}$	$\frac{+40}{2}$	$\frac{+30}{3}$	$\frac{-15}{3}$	$\frac{+30}{3}$	E5 9
Reactors	4		3	4	4	3	4	5	5	5	5
	<u>Events</u>					<u>Trends</u>					
	1. Judge rules violation of Fourth Amendment 2. Hacker set-off major military move 3. Hackers unite 4. Police contract computer crimes 5. Hospital patient dies					1. Massive availability of information 2. Security development and standards 3. Ethics of computer use 4. Electronic fund transfer 5. Fund to investigation of computer crimes					

After reviewing the information in the cross-impact table, it was determined that the events significantly impacted the events and trends. Events One, Three, and Five impacted each of the other trends and events. Trends Two, Three, Four, and Five reacted to each of the events.

Event One impacted the trends and events because a search and seizure ruling can create investigation process problems by requiring search warrants for telephone lines

and individual system users. Hackers would be ambivalent with the law change. On one hand they would enjoy the additional protection from police intrusion; however, they would not appreciate being told that they would have to respect the privacy of others from an ethical standpoint. The restrictions placed on police can motivate a movement to allow the private sector to assume the investigative responsibility for computer crime.

Event Three impacted the trends and events based upon the belief that as hackers form a unified front and organize resources, they will be able to apply special interest influence on government. They would also be in a position to organize legal and subversive efforts in an effort to mitigate law enforcement actions. Such organized effort could lead to their initiating court challenges on such issues as application of ethical requirements and standards. Their unity may provide the impetus for government allocation of resources to combat illicit efforts.

The fifth event, a hospital patient dies, also impacted the other events and trends. Again, the impacts were mostly on the negative side. The positive influences were on Trends Two, Three and Five. If a hospital patient were to die from the tampering of a computer criminal, then, as in most cases when a tragic event brings forth overwhelming awareness and concern, resources and interest from government for ethics, security, and finally funding for the investigative process would occur.

Phase V - Scenarios

A scenario is defined as a narrative description of a potential course of trends or events which might lead to a future state. Three scenarios will follow as a means of looking ahead to the future. The scenarios to follow will incorporate the aforementioned

trends and events into a story. After the story has been told, policies and strategies can be explored and developed in order to affect the course of trends or events.

The types of scenarios are exploratory, hypothetical, and hypothetical which was modified with a policy change. The exploratory scenario will interweave the already identified five issue-related trends and events which have been occurring and will more than likely continue to occur without disruption. The hypothetical scenario will display the same trends and events identified in the cross-impact analysis matrix which had a 30 percent probability level. This format is referred to as the "turbulent future." The modified hypothetical scenario will change the previous hypothetical scenario by adding an implementation policy. The addition of the policy to the hypothetical scenario will illustrate how the turbulent future can be affected.

Exploratory

"U. S. Supreme Court Rules in Favor of M.O.D." The United States Supreme Court issued a ruling today which set law enforcement back in its ability to investigate computer hackers. The Masters of Data (MOD) organization, formally Masters of Destruction, challenged a government case in which a seventeen year-old computer enthusiast infiltrated a U. S. Navy shipyard in Alameda County, activating an early warning detection alarm. The hacker was able to simulate a multi-missile attack on Alameda and San Francisco. Military defense mechanisms engaged in countering the "missiles" by arming the base anti-missile electronic defense system.

Federal investigators, monitoring the MOD Computer Bulletin Board, learned of the identity of the perpetrator and seized his computer system. The federal authorities

did not have a search warrant, citing national security as its basis for recovering the computer system and arresting the youth.

The government, in citing its case, emphasized the lack of ethics by computer enthusiasts, especially by the radical underground group Masters of Destruction. The Masters of Destruction, wanting to change their ruthless image, changed their name and direction as a result of introduced government legislation which considered computer-based information as private.

"Hospital Techno Death . . . Husband Arrested." A thirty-six year-old mother of three died at Valley Medical Center Hospital of barbiturate poisoning. The woman was connected to a sophisticated monitoring system which provided current information regarding patient status, administering medication and nutrients to the body as needed. A reading of the decedent's chart indicated she received a dosage of barbiturates to which she was allergic.

Hospital officials would not comment on the death, citing the lack of security as the reason for the penetration into their computer system. In recent months the hospital had tried to increase its computer system security. Manufacturers of computer components and systems and software companies were contacted. Each reiterated the lack of standards of laissez faire in promoting their products.

A breakthrough in the case centered on Transamerica Database providing information on a database inquiry which was registered to a specific telephone number. The inquiry appeared on the medical history of the deceased, enabling police to trace the phone number to the deceased's home. The husband was subsequently contacted,

leading to his ultimate confession. Later, he cited marital difficulties, indicating his wife was planning to leave him and the children. When asked why he accessed the National Database, the husband stated that he could not remember a medicinal compound he knew his wife was allergic to. The database allowed him to access his wife's records without detection--or so he thought.

"Electronic Crime Wave . . . A Bust for Law Enforcement." Local officials, feeling the heat from taxpayers to cut their budgets, decided to contract with private firms to investigate thefts involving computers. Law enforcement officials were somewhat ambivalent regarding this new development. Police officials have repeatedly requested modern computer equipment for the purpose of investigating the surge in thefts of funds via computer. Additionally, they cited their lack of technological experience as a drawback to investigating such offenses. Officials also mentioned the possibility of the federal government eliminating the need for tangible money by issuing a debit card to each person, assigned to their social security number.

Hypothetical

"Computer Smut King Goes Free." The United States Supreme Court reversed the decision of a 23 year-old computer pornography distributor who was involved in the shooting of a suspected gang member. The decision was based on an unlawful search and seizure by a computer investigation firm. Local law enforcement, not having the expertise to investigate the offense, received the go-ahead from City officials to contract with the firm. The firm, consisting of retired police officers with investigative experience, apprehended the suspect after monitoring an underground computer bulletin board. The

court ruled that the firm was an extension of the police effort, acting as their agents and susceptible to the constitutional guarantees of search and seizure. Law enforcement officials continue to stress the need for government-created ethical standards. Some headway was seen by law enforcement when two years after the homicide, legislation was enacted to establish security efforts and standards for computer users.

"Search and Seizure at the Forefront of Rambo Computer User." A computer hacker who caused the activation of a sophisticated military defense system was freed from custody when the judge ruled that the police did not follow proper search and seizure protocol in accordance with the U. S. Constitution. The case has caused local government officials to contract with private firms specializing in computer crime investigation. "Law enforcement has been slow to react to this problem," was the theme presented by the government officials. Law enforcement officials cited lack of funding, concern for ethics associated with computer usage and standards, too many vendors and operating systems, and security measures as the reason for their inability to fully and successfully investigate computer crime offenses. Law enforcement officials were also somewhat ambivalent regarding the decision due to the fact that they felt slighted by the lack of funding and support. However, they were relieved that the crimes will at best be investigated.

"Computer Group Marches on Capitol". A united group of computer enthusiasts called "Keep Data Free" marched on the Capitol in Sacramento, protesting their right to privacy and their dissent upon being referred to as "hackers." The group has contended that information transferred over electronic lines is open for public review, regardless of

its ending destination. The group was ecstatic when the Federal Court of Appeals overturned the arrest of a 17 year-old boy who had altered credit history from a national data collection service. In the case, officers investigating the offense had been operating for one year when the case was uncovered; however, they did not obtain a search warrant for the arrest and seizure of the youth's computer system. The judge had received pressure from computer enthusiasts to ensure law enforcement complies with constitutional guarantees.

Modified Hypothetical

Policy: The Chief of Police makes computer crime a priority.

"Chief's Computer Crime Unit: A Model for the State."

The Chief of Police of a large Central Valley police agency recently enhanced and formed a separate computer criminal investigation unit. The Chief advised that criminals of today are becoming more sophisticated and resorting to computers to commit traditional crimes. The announcement came after one of his investigators uncovered an "electronic contract hit" for a patient at a local hospital. The patient, recently involved in a shooting by a suspected gang member, was earmarked for death. A computer hacker had been hired to bypass the hospital security system for the purpose of altering the patient's computer-based medical monitoring unit. Investigators waited for the hacker to bypass the security system, at which point they diverted him to a remote location. The hacker's phone line was traced and he was arrested without incident. Computer equipment and records were confiscated by police. The mother of the patient was very grateful for the police department's efforts. The Chief was quoted as stating that

computer crime can be impacted if resources were dedicated to the problem. He further stated that computer crime appears to be the wave of the future and called upon all of law enforcement to join together to develop networks throughout the nation. The Chief also said that he has been contacted by at least two major computer manufacturers who have offered to assist his department with equipment and training.

"Hacker Crackers Meet with Computer Group". The Chief of Police of a large central valley police agency has been instrumental in pioneering the investigation of computer crime. The Chief recently implemented a computer crime unit consisting of two officers and two civilian computer operators whose sole function is to investigate crimes involving computers. The unit, which calls itself "Hacker Crackers," met with a group called "Keep Data Free" to explain their intentions. The Chief of Police was emphatic that the unit work with groups and businesses in the community stem the tide of computer crime. The Chief reminded all that the rapid growth and miniaturization of computer components, expansion of Vice President Gore's high-tech fiber optic super highway, and computer-controlled living and business environments have created a need to keep pace with technology. The Chief cited the Supreme Court's overturning of a Federal Court of Appeals decision regarding a 17 year-old youth convicted of changing the personal history of a police officer as a major indication that the movement being initiated is worthwhile. The business community responded favorably, providing all of the needed computer hardware and software for the unit.

"This Rambo is Not Sly". A computer hacker who initiated the beginnings of a major military defense operation was stopped dead in his tracks when members of the

Central Valley Police Agencies Computer Crime Unit were able to show the court that the arrest and seizure of the defendant was deemed proper. The unit, formed by the Chief of Police as a measure against the growth of computer crimes, received special training and assistance from the Federal Government's Federal Law Enforcement Training Center. The unit, supported by local businesses, is comprised of a partnership effort between police and local computer operators. The computer crime unit is the first of its kind and was instrumental in thwarting the "Rambo" hacker.

Phase VI - Policy Impact

Three policies were identified to address the undesirable future from the hypothetical scenario. The policies were developed by the researcher and the police assigned to crimes against property for the Fresno Police Department. The policies, if enacted, should impact the exploratory and hypothetical scenarios. Hopefully, the implementation of these policies would temper an undesirable future. Policy One was used in the modified hypothetical scenario.

Policy One

The Chief of Police decides to treat computer crime as a high-priority concern.

Policy Two

The Chief of Police supports legislation aimed at developing ethical standards for computer users and for enhancing security for government computer systems.

Policy Three

The Chief of Police makes training of all personnel in the use of computers a priority and enters into a partnership with the business community regarding computer

crimes.

The policies were compared with the trends and events which had the most impacts identified in the hypothetical scenario and a cross-impact analysis was completed.

The results of the analysis are featured in the table below.

Table 4

CROSS-IMPACT ANALYSIS

Maximum Impact (% Change +/-)											
Policy	E1	E3	E5	P1	P2	P3	T2	T3	T4	T5	Act
P1	0	0	+30	XX	+40	+50	+5	+5	+5	+30	7
P2	+10	+10	+20	+30	XX	0	+60	+60	+50	+20	8
P3	+30	+10	+25	+40	0	XX	+10	+10	+25	+40	8
Reactors	2	2	3	2	1	1	3	3	3	3	

E1 Judge rules violate 4th amendment
 E3 Hackers unite
 E5 Hospital patient dies
 T2 Security standards for computers
 T3 Ethics of computer use
 T4 Electronic fund transfer
 T5 Funding to investigate computer crime unit

P1 Computer crime a priority
 P2 Support legislation for ethics
 P3 Emphasis on computer training

The three policies impacted each of the trends in a positive fashion due to the fact that there is a recognition and awareness that computer crime is of concern and that law enforcement recognizes the need to prioritize its resources. The policies impact the

trends in a positive manner because of the support for increased ethics and training of law enforcement personnel on computer crime. Recognition of computer crime as a priority concern can lead to support for security and standards and that electronic fund transfers may become the target for computer criminals this recognition can lead to keen awareness and strategies to thwart thefts and prevent injury or death.

Conclusion

This research has shown that computer crime, if allowed to go unchecked, can create many problems for society and law enforcement. The trends and events identified by the panel as having the most actors and reactors cannot be viewed as all-inclusive. The other trends and events not selected for inclusion in the hypothetical scenario may in fact happen. None of the data is to be ignored as it will require further study.

The exploratory and hypothetical scenarios indicate the impact on society should computer crime not be proactively pursued. The modified hypothetical scenario illustrates what can be done through the implementation of a policy. The three policies developed have a direct bearing on the issues and can impact an undesirable future.

PART 3

Strategic Plan Development

Introduction

The issue examined during the futures forecasting was what impact computer crimes will have on a large law enforcement agency by the year 2002. Trends and events which may occur were identified during this process. The trends and events which focused on the issue indicated that the use of computers will continue to increase during the next ten years. Data bases of information, diverse in nature, will eventually be available to anyone with a computer. Additionally, there will be an increase in the movement of money through electronic means. Ethics concerning computer usage will not improve much from today's principles while security standards for computer systems will improve.

The three scenarios in the previous chapter displayed what can happen with the trends and events. The exploratory example allowed the trends and events to unfold without any type of intervention. The hypothetical scenario represented trends impacting other identified trends and events in the turbulent future. The third scenario exemplified the impact of a policy in the hypothetical scenario. The exploratory scenario will be used as the basis for developing the strategic plan. The major focus will be to develop a plan over the life of the study period in order to reach a desired and attainable future.

The exploratory scenario showed how criminals using computers cause severe consequences and hinder investigations, particularly those targeting the computer criminal element. The rulings from the court can also impede or expedite an

investigation based on their decisions. Thus, the impact can have far-reaching and negative consequences. A significant question to answer is who will investigate a crime committed by someone using a computer as the tool to complete the offense, and what will be the end result of the investigation?

Alternative strategies to address the problem will be identified, using the Fresno Police Department as the model department for combating the issue.

Strategic Plan

Any plan contains certain elements which lead to the implementation of a strategy and achievement of objectives. This plan will include a mission statement which serves as a basic guide for energy output and commitment by the organization; an analysis of the environment and capability of the organization; identification of individuals or groups who can impact the issue and strategy along with their assumptions; and lastly, the development of more than one strategy to combat the issue. One strategy will be selected and studied for implementation.

The mission of the Fresno Police Department will be displayed as the macro mission and a micro mission will identify the emphasis on addressing computer crime.

Macro

Fresno Police Department Mission Statement

The Fresno Police Department is dedicated to providing professional, ethical, and innovative service. With our emphasis on integrity, consistency, and pride, we are never satisfied with service short of excellence.

Our organization is sensitive and responsive to the needs of our diverse community, recognizing and accepting our responsibility to provide a safe environment for the citizens of Fresno!¹

Micro

Unlawful activity, regardless of its origin, will diminish the quality of life in the community. All Department members are committed to making Fresno a safe place to live through the apprehension of those who threaten community members. The criminal element will commit highly technical crimes through the use of the computer. Police personnel will be prepared to aggressively curtail this type of deviant behavior.

WOTS UP Analysis

Analysis of trends and events which will assist in the accomplishment of the mission, as well as analysis of those which will hinder the mission, will be performed in this segment. The technique used for this analysis is labelled WOTS UP. The technique encompasses an evaluation of the external environment for both opportunities and threats and the internal organization's strengths and weaknesses. The opportunity section includes trends and events which can help the mission succeed. The threats section seeks to identify trends and events that can limit the ability of the mission to succeed. The organization strengths are examined to determine what is routinely occurring in meeting the mission. The organization's weaknesses are also examined to determine which activities minimize the mission. The scanning of information process, STEEP, as used in issue and sub-issue identification, plus a legal category was used for data compilation. The writer developed the criteria based on extensive familiarity with the topic, STEEP information, and discussion with a police specialist involved in investigating computer crimes.

Threats

1. The use of and complexity of computer "viruses" will increase dramatically.
(Social-Economic)
2. A political activist for a "Save the Earth" affiliate organization causes two trains carrying toxic agricultural chemicals to collide by switching tracks via computer. (Environmental-Social-Political-Economic)
3. A prison inmate uses a computer in a prison computer lab to transfer money from a major credit card company to a Swiss bank account. (Social-Economic)
4. Police personnel who investigate computer crimes become the target of computer hackers by disrupting their credit ratings. The access to national databases will make this activity relatively easy to accomplish. (Social-Economic)
5. Courts rule that a search warrant must be obtained before the contents of any computer system can be examined, thereby complicating the investigation process. (Social-Legal)
6. Lack of revenue causes a law enforcement computer crime investigation unit to be reduced. (Economic-Political)
7. The deregulation of the telephone system continues to hamper law enforcement by requiring them to produce a warrant for every telephone carrier service company involved in a computer hacking case. The breakup

- of the AT & T monopoly created many different telephone service providers. (Social-Political-Legal)
8. A disgruntled and recently fired employee of a major department store tampered with computer payment records, causing creditors to stop shipment of retail goods. (Social-Economic)
 9. The criminal statute in California delineating computer crimes (P.C. 502) is vaguely understood by prosecuting attorneys. The statute requires a specific intent for violation. (Legal-Political-Social)
 10. Computers today are so small and inexpensive that any person can obtain a device with a modem. Local department stores make it easy to purchase computers on credit plans. (Technology-Economic)
 11. The ACLU files suit on behalf of computer users for resisting restrictions on the use of their computers because of an ethical standard mandate. (Social-Legal- Political)
 12. The criminal stereotype of a highly sophisticated male hacking into a computer system will evolve to the criminal today (burglar, robber, thief) using a computer to commit crimes. (Social-Technology)
 13. Technology today and in the future will make it extremely easy to commit crimes from any remote corner of the world. A computer, modem, and telephone line is all that is needed. (Social-Technology)

Opportunities

1. Over 80 percent of households will have micro-computers in the home and the public will be computer literate. (Social-Technology)
2. Legislation is introduced to expand the current criminal code section to include any use of a computer for unlawful gain as a general intent to commit an offense. (Social-Legal)
3. A letter of support is sent to the Department of Justice in care of the Attorney General to recommend an asset seizure statute be drafted to allow the seizure of assets of any computer enthusiast who uses a computer to obtain resources through the use of a computer system. This would be modeled after the narcotic asset seizure statute. (Legal-Political- Economic)
4. Judge rules that the Fourth Amendment is not in violation when searching the computer files of a suspected computer criminal. (Social-Legal)
5. The miniaturization of and exponential advancements of computer components allows agencies to obtain devices from computer vendors. (Technology-Economic)
6. The community has become aware of the seriousness of the computer criminal and supports the efforts of the police in investigating this offense. (Social-Political-Economic)
7. Several computer companies involved in hardware and software offer law enforcement agencies free training and government discounts on equipment due to the rise in use of computers by criminals. (Social-Economic)

8. Large computer database information services such as Prodigy and CompuServe assist government agencies in adopting ethics and standards concerning the use of computers. (Social)
9. Businesses throughout the nation are forming an alliance to combat computer pirates from stealing their assets. (Economic-Social)

Capability of the Organization

This section will refer to an assessment of the organization's ability to currently accomplish the mission as it relates to the issue.

Strengths. The organization's strengths will be briefly delineated.

1. The Chief of Police has been in charge of the organization for nearly two years and understands the importance of computers and technology. The Chief of Police has emphasized to staff the need to become familiar with computers.
2. The majority of management in the organization consisting of executive, middle, and first-line supervisors possess college degrees; for middle and executive management, completion of the FBI National Academy and/or the Command College is the norm.
3. Several staff officers are currently aware of the power of computers resulting in an emphasis to automate as many tasks as possible.
4. The Police Department enjoys a good relationship with the community and therefore has favorable support.

5. The Department has formulated various programs to serve the community. These programs include Neighborhood Watch, crime prevention, Combat Auto Theft, Police Activity League (PAL), and Drug Awareness Recognition Education (DARE). There is a strong desire to provide education to the community to help diminish the possibility of victimization. Such programs emphasize a commitment to prevention and intervention strategies as well as apprehension.
6. The Department employs a police specialist recognized throughout the nation as being particularly knowledgeable in the area of computer crime. He has also been able to acquire some equipment for such investigations.
7. The Department is committed to providing personnel with mandatory and essential training to increase job or task efficiency. Officers receive advanced officer training annually, beyond POST requirements.

Weaknesses. The weaknesses of the organization appear below:

1. The City's economic picture is bleak with seemingly endless budget problems. The City has not committed adequate resources to the Department and tax revenue is not keeping pace with the general fund costs.
2. The police specialist with expertise in computer crimes is three years from retirement. Movement from this assignment may cause him to retreat to the private sector, and there is a lack of commitment to train a replacement.

3. It is very difficult to obtain equipment for combatting computer crime. The City's financial policy severely restricts the purchase of equipment. The nemesis of city government is that once a physical object is purchased, the anticipated lifespan of the object is several years; and, in some cases, decades. Unfortunately, computer technology changes rapidly.
4. There is no major understanding of the magnitude of the computer crime problem by Department personnel.
5. The relationship with the District Attorney regarding computer crimes or economic crimes is not compatible. This is partly due to the lack of resources in the D.A.'s office as well as their lack of expertise in these areas.
6. Investigations into computer crimes are technical in nature, requiring a large amount of time to obtain evidence for court prosecution.
7. There is no clear understanding of what constitutes a computer crime. The lack of understanding is engendered by its spiraling growth and the business community not reporting damages caused by computer criminals.
8. Many computer crimes are not reported due to a lack of faith with the criminal justice system, and the fear of decreased business and customer loss.

Stakeholder Analysis

The identification of an individual or group of individuals capable of impacting the issue is very important to the strategic plan. Such people can influence the outcome

positively or negatively based on their understanding and commitment to the issue, solution, or strategy to the issue. For this purpose, stakeholders have been identified and the assumptions they hold regarding the issue will be discussed. A snail darter was also identified. A snail darter is an unanticipated stakeholder who can radically impact the strategy. A stakeholder can be either internal or external to the organization. The writer and a police specialist compiled the list of stakeholders and their assumptions. The list was presented to the modified delphi for their input.

Chief of Police

1. Recognizes technology is increasing and is aware that criminals are utilizing computer technology to commit crimes.
2. Realizes budget dollars are limited and may have difficulty providing resources to combat computer crimes.
3. Would support legislative efforts to combat the problem of computer crimes.

City Council

1. Will express concern for the issue of computer crimes and high tech offenses; however, they will not understand its implications.
2. Would assist in legislation to support changes in the legal system to investigate computer offenses.

POST

1. Would be very interested and aware of the significance of computer crime.

2. Would perceive the legislature as the government body which would require POST to impose training standards statewide for investigating computer crimes.
3. Would see a mandate for training as an opportunity to justify budget requests, particularly in today's mode of reducing State agency budgets due to the serious economic picture.

Media (Snail Darter)

1. The media is a staunch defender of search and seizure and could hinder what they perceive as government intrusion into an individual's computer system.
- B. If a human interest story concerning an arrested individual peaks media interest, much energy may be devoted to "over report" the actual case. The theme of, "big brother is watching you" may be cause for concern.

District Attorney

1. Would not welcome another new type of crime to try in court due to personnel shortages.
2. Would not have the technical expertise or understanding to try such cases.

Court Judges

1. Does not have the technical expertise regarding computer crimes.
2. Would rely on Penal Code Section 502 as the section referencing computer crimes. If the use of a computer did not fit this section, the case would not be heard.

Computer Vendors (Hardware and Software)

1. Marketing of computer products will be the primary concern, and they initially will not be overly concerned with computer crimes.
2. Will see an opportunity to make money for new and different security devices if standards are adopted.
3. May provide assistance to law enforcement as a "good faith" gesture for controlling unlawful use of computers.

Telecommunications Companies

1. Would resist regulation of phone companies and would require a search warrant for each carrier involved in a computer crime.
2. Would assist and support law enforcement in training investigators.

Department of Justice/Attorney General

1. Has a very good understanding of the current criminal statute and would support legislation changes to aid investigations.
2. The Department of Justice would need additional resources to do more in the area of computer crimes, particularly if it becomes a priority.

Chamber of Commerce

1. Would welcome assistance from police to investigate computer-related crimes.
2. Would resist publishing loss of revenue statements to the media for fear of loss of credibility with the public.

3. Unless convinced otherwise, may not believe law enforcement has the expertise or resources to investigate computer crimes.

Private Security

1. Would see computer crimes investigations as an opportunity to generate income.
2. Would aggressively pursue individuals who have expertise in computer technology and the investigation of computer offenses.

The stakeholders and their assumptions were analyzed as to their degree of validity, either certain or uncertain, and whether the stakeholders believed the assumptions were important or unimportant. A strategic assumption map was used for the process (Appendix E). All of the stakeholders had at least one assumption in the certain and very important quadrant except for the media which was also identified as the snail darter. The media can negatively impact the issue and strategy if they perceive the issue of the Fourth Amendment as a cause for support. They can also become embroiled in a human interest story which can lead to negative press, particularly if the victim was wrongly accused, lost a business or income, or if government was portrayed as the villain in its investigation.

Developing Alternative Strategies

The addressing of a problem and accomplishment of the mission requires a solution. The exploratory scenario represented consequential results if computer crime is not addressed. The driving forces mentioned in the introduction, plus the identified trends and events, will have a negative impact on society in the future. The scenario, if

allowed to continue, presents a bleak picture for law enforcement. If law enforcement does not assume a proactive stance, then confidence in their ability to protect the community will diminish and others may assume their responsibility. For this reason enhanced training and development of expertise regarding computers and their different systems is important. Government must be able and ready to support this endeavor through funding or partnerships with the community. For this reason alternative strategies need to be developed. The reason for developing different approaches is to explore as many ideas as possible to discern which approach is best or which combination of an approach is most practical. A modified policy delphi process was used and eight members from the police department created eight ideas for impacting computer crime (Appendix F). Each strategy was evaluated with a discussion of the pros and cons of each suggestion. Three strategies were then chosen due to their feasibility of implementation. The choices were difficult, as six of the eight strategies identified were determined to be desirable by the group.

Strategy One

The focus of the first strategy was for the Department to push for state legislation which would allow law enforcement agencies to seize assets accumulated by a computer criminal. The seizure of assets is modeled after the Narcotic Asset Forfeiture Statute, which is enforced today. The strategy would require the City Council to actively endorse the concept and contact state legislators for their support. The Chief of Police and the affiliate chief's organizations, of which he is a member, would be supportive; particularly in the area of political persuasion.

Pros

1. The enactment of such forfeiture legislation would generate revenue for the police department, also supplying them with confiscated equipment for future criminal investigations.
2. A disincentive would be evident to the perpetrator as there would be a risk of asset loss as a result of the illegal activity.
3. Funding would be generated to train police officers in the investigation of such offenses.
4. Forfeiture specialization within the organization could be viewed as an enterprise whereby the confiscated assets would finance the investigation.

Cons

1. An initial budget allocation for the computer crimes unit would be required.
2. Additional training of personnel in the application and procedures of the law would be needed.
3. More personnel for the forfeiture process would be required.
4. Changes in legislation can be a very time-consuming process.
5. An increased caseload for an already overburdened court system would result.
6. The possibility that the press may report a person under investigation can be an unfavorable circumstance which may impact the legislation.

7. Legitimate users of computers would see this concept as a restriction of the use of their systems and may balk at its implementation.

Strategy Two

Strategy Two focuses on the formulation of a dedicated and specialized prosecution, investigation, and judicial team. Each criminal justice agency would be required to allocate resources for the investigation through final adjudication of the case. A quality commitment from each agency involved would be essential.

Pros

1. Cases would receive quicker and more efficient investigation and adjudication due to specialization in a highly technical area.
2. Cases would be cost-effective since the resources are shared and each involved branch of the criminal justice system would possess the same knowledge.
3. The resources, by being combined, would eliminate jurisdictional problems.
4. Resources, working together, would reduce the chance of duplicated effort.
5. More cases would be investigated by this unit as they can be assigned to the same court and will not have to be rotated to any available court.
6. A renewed confidence could be established within the community.
Consolidation and coordination of efforts are being advocated in communities today due to shrinking revenues.
7. It would be easier for a combined group of specialists to stay current with training and new technologies.

Cons

1. The method can be expensive, particularly if the specialists leap to the private sector based on increased pay and benefits. Also, government will need to allocate money to equipment and commit to keeping pace with technological advancements.
2. Jurisdictional conflicts can arise, particularly with out of state agencies involved in the case. The issue of who controls the case could lead to friction.
3. The priority of cases to be solved can lead to potential misgivings if one jurisdiction perceives they are not obtaining the best "bang for the buck."
4. Individual units within each criminal justice agency may need to be retained and/or maintained due to conflicts or disagreements regarding the operation.
5. Due to their inexperience, it would take some time before the prosecution and judicial arms were competent to proceed with a case.
6. The educational level of the prosecution and judicial team members is not at the same level as the police investigator. Time will have to be given in order to raise the competence of these units.

Strategy Three

Strategy Three focuses on the changing of the law to specify that the use of a computer is sufficient to establish general intent for the crime. The penalty should also be commensurate with the crime. For example, it is known that the crime of burglary is accomplished when a dwelling is entered with the intent to commit grand theft, petit theft, or another type of felony. If the law is revised and a computer is used as part of the strategy for obtaining entry into a dwelling to commit theft or another felony, the use of the computer would satisfy the general intent for burglary. Thus a criminal violator can be held responsible for violating the computer crimes statute and for the crime of burglary.

Pros

1. The prosecution of crimes would significantly improve and simplify the investigation.
2. The role and understanding of the prosecutor would be clarified.
3. The second part of this approach includes a penalty for the crime which may lead to a decrease in crimes committed.

Cons

1. Unless the penalty is explained adequately, the crime can be diluted. An average theft of money via computer is enormously higher than theft of money in a burglary.
2. Legal change is slow to implement.

3. Investigation of computer crimes is time-consuming in a time of shrinking resources.
4. The cost of training officers to investigate the different computer systems and environments would be very expensive.
5. If legislation is passed, law enforcement will need to investigate computer crimes due to its criminal nature. The private sector would become very concerned, especially if there are not adequate resources and the police do not have the needed expertise.

Stakeholder Perceptions

The selection of a strategy for implementation cannot be accomplished unless the perceptions of the stakeholders are taken into account. The stakeholders can impact the outcome of any strategy if their holdings are not considered. The Stakeholder Perception Chart (Appendix G) identifies the three strategies and whether the stakeholders support, oppose, or are indifferent. An analysis of the stakeholders' perceptions will follow.

Strategy One

Support for this strategy stretched to over half of the stakeholders. The Chief of Police and City Council would be strong advocates for the proposal especially since there is a potential to obtain other revenues during poor economic times. POST would also support this strategy as they would no doubt receive reports from Chiefs and Sheriffs throughout the state supporting the proposal. The District Attorney and court judges would support the proposal if they saw potential for receiving revenues from the seizures.

The Attorney General/Department of Justice would lend support because they, too, would receive support for legislation requests from Chief and Sheriff organizations. They would also vie for a statewide lead agency role. The legislation could be the impetus needed to add resources to an already existing computer crime unit. The computer vendors, affected minimally, would be indifferent unless they were to receive pressure from the media or other groups to develop standards and security measures for computer products. The media may initially support the concept until a controversial story arises. They could then take a negative reporting approach, causing the public and any opposing special interest group to change or revoke the legislation. The media may also raise constitutional questions regarding the Fourth Amendment of search and seizure. Telecommunications companies may express opposition as they could become embroiled in each litigation case, spending precious resources in providing documentation and complying with search warrants. The private security companies may oppose the idea if they lose their chances of obtaining additional income.

Strategy Two

Support for this strategy reaches across the board to all stakeholders, with the exception of private security. Again, private security may view the strategy as a reduction of their ability to solely investigate crime and generate revenue. However, they may also realize that they can contract with a company to provide this service and supply the investigation team with information they have generated. One advantage that private security would recognize is that they are not bound by the legal edict of entrapment, since government is the only structure which must comply with this sanction. The other

stakeholders would agree that specialized knowledge is needed in this highly technical field and that a group of experts from each segment of the criminal justice area would be able to adjudicate these cases more efficiently and effectively. The consolidation of effort would be both appealing and consistent with today's demands for consolidation of services, particularly to the City Council and Board of Supervisors.

The media would probably change their assumption if they were the target of a computer hacker who edited their story before disclosure to the public or disrupted their broadcast or printing of a subsequent edition.

Strategy Three

Support for this strategy is somewhat mixed. The Chief of Police, POST, DOJ/Attorney General, and the business community would support this effort because it clearly delineates the application of intent to any criminal statute through the use of a computer. Also attractive to these stakeholders would be the assessment of a penalty for a conviction. The provision would help relieve the misunderstanding and complications associated with investigating white-collar crimes. White-collar crimes are difficult to prosecute, require endless reams of documentation, and also require specialized knowledge by all members involved in the criminal justice system. The District Attorney and court judges would support the concept of clarifying the law and may oppose an added workload without additional resources. The media, computer vendors, and telecommunications companies would be indifferent to this approach as it does not impact them directly. Private security may balk at this idea if they perceive their chances

of additional revenue as negligible. This concern would diminish if they could provide the results of their investigation to the investigating body.

Strategy Choice

Each of these strategies should be implemented, as each one compliments the other. Unfortunately, implementation of each strategy would require much energy. Today's climate in both politics and fiscal management point to using public tax dollars in the most efficient and effective manner. For this reason the second alternative should definitely be implemented. The recognition of a special team designed to address the issue of computer crime has most of the stakeholders' support and addresses today's current trend of consolidation of government services.

Implementation Plan

The Chief of Police would assume the lead on the strategy as personnel under him have significant experience with the investigation of computer crimes. Also, the Chief of Police is responsible to the community for protecting them from the criminal elements. Therefore, it is in his best interest to assume initial control of the strategy. The Chief of Police would need to appoint the lieutenant in charge of the Property Crimes unit as the project manager. Typically, the staff officer assigned this function is responsible for computer crime or white collar crime. The Chief of Police must first meet with the District Attorney and Presiding Judge to come to a common understanding of the seriousness of such offenses along with the ramifications if no action is taken. Consequences need to be graphically illustrated through explanation of trends and

events. A commitment to the concept must be reached. The appeal of a joint investigation-prosecution-adjudication team is politically appealing.

An important factor in the Chief of Police's approach to the District Attorney and Presiding Judge is the need to locate funding for this endeavor. Two areas of funding can be sought. The first area of funding would be application to the state and federal government for a grant project. Grant proposals which involve co-ventures by different jurisdictions are more apt to receive approval than individual grant applications. Also to be explored would be the possibility of grants from the private sector. Assistance from the business community stakeholders would be needed. The other source of funding would be for the Chief of Police to direct asset seizure monies from narcotic asset forfeiture cases to the project. The application for outside funding would alleviate the fears of the District Attorney and Presiding Judge. After the essential meeting with the District Attorney and presiding judge, a meeting with the stakeholders should occur. Their support must be enlisted and an explanation of the current situation and future scenarios should cause them to lend support to the concept. Letters of support for inclusion in the grant proposals would be obtained for augmentation of receiving grant money. Hopefully, a meeting of the stakeholders, particularly the media, will ease potential negative reactions.

A presentation before the City Council and Board of Supervisors would be necessary. Education concerning the computer crime problem will garner their support for the transition of the strategy.

Consideration should be given to forming an executive steering committee of stakeholders to involve them in the concept. The committee can be invaluable in supplying information as to developments in the area of technology shifts and crime threats, and they can also be asked for their input and their opinion as to which direction the specialized unit can embark.

A commitment of resources from each criminal justice agency would need to be obtained. At the very least, one police investigator, one district attorney, one judge, and one clerical position are needed. Computers and office equipment would also be required. The plan may need to be initially incremental with the clerical position, district attorney, and police investigator working together on cases. As funding becomes more readily available, a third component, the judge, could be assigned.

Training of all parties would be essential. The Federal Law Enforcement Training Center in Glynco has an excellent training course for computer crimes and it is open to law enforcement personnel. Arrangements could be made for each member of the specialized unit to attend this training as soon as possible. There may also be the possibility for the Training Center to travel to Fresno to train the team. The Department of Justice has a very good reputation for their knowledge of computer crimes and they, too, could be asked to assist in the training of the team. There are other individual units throughout the state specializing in computer crime investigations that could be considered as a resource for education.

There are computer crime investigator organizations at both the state and federal level. Membership in these organizations would be essential for the operation and education of this unit.

Cases would be tracked with a calculation of length of time used to investigate and length of time used to prosecute to final disposition in the court. Quarterly meetings with the affected agencies and stakeholders would determine the impact of the strategy. One important statistic to record would be the amount of money each criminal has stolen from a citizen or business or the cost of damage resulting from computer tampering.

This strategy, if implemented, could significantly impact the previously stated mission.

PART 4

Transition Management Plan

Introduction

The focus of this research effort was to indicate the impact computer crimes will have on a large law enforcement agency by the year 2002.

Advances in technology, particularly in the area of computers, have provided society with a medium of communication, increased task production, and more access to information gathering. The computer has moved from the research laboratory to business and to the home. People are purchasing portable desktop computers for their homes and they have access to diverse varieties of programs, services, and information. Such technology is linking homes with service and business institutions and it is this link which could unfortunately allow unauthorized entries into systems.

It is the criminal use which is of concern to law enforcement and the community. Such concern has been expressed by several, yet law enforcement still lacks the skills to successfully impact this type of crime.

A strategic plan was developed with the purpose of identifying alternative strategies to impact the issue. The mission statement included the need for the agency to focus its energy on crimes of a high technological nature. A policy statement was prepared, recognizing the need to consider computer crime a priority for the police agency. Organizations and individuals who could influence the outcome of the strategies were identified. The three alternative strategies were:

1. Emphasis on the need for state legislation which would allow law enforcement agencies to seize assets obtained by computer criminals. Such legislation, likened to the Narcotic Asset Forfeiture Statute, would require support from city and state officials as well as law enforcement agency heads.

2. Identification of the need for a specialized unit spread across the criminal justice system to identify, investigate, and prosecute computer criminals.

3. The modification of existing law by specifying that the use of a computer for the purpose of unlawful gain or for destruction is sufficient to establish criminal intent.

The three preceding strategies were evaluated as to their strengths, weaknesses, and level of support by the stakeholders. The second strategy was subsequently selected as the method of choice. It was basically felt that the problem of the computer criminal could provide far-reaching and immediate damage. Also, the criminal justice system seems to function more efficiently when a shared concern allows for the participation of law enforcement, prosecution, and judiciary bodies.

The purpose of this chapter is to delineate a transition management plan for the selected strategy. The transition takes into account the "critical mass," the type of management structure necessary to manage the transition, and technologies and methods used to augment the change.

Critical Mass

Critical mass refers to key people who can influence change, and it is common knowledge that the disruption of one's comfort zone can lead to resistance to change. A key element in minimizing this change is to identify groups or individuals who can cause

the change to occur as smoothly and expeditiously as possible; conversely identifying those who can cause the change to fail. The writer, a police lieutenant, and a specialist in the area of computer crime collaborated on the identification of the critical mass. The critical mass players for the issue at hand are:

1. Fresno Chief of Police
2. Fresno City Council
3. Fresno District Attorney
4. Telecommunication companies
5. Chamber of Commerce

A commitment chart was used to determine the commitment of the critical mass members. This technique evaluates the current position of the critical mass member, whether for or against, and where the member needs to be for the change to occur. This can assist in relocating the member to a desired state. Once the desired state is determined, approaches designed to enable members to reach the desired state can be identified and implemented.

Table 5

COMMITMENT CHART

Actors Critical Mass	Block Change	Let Change Happen	Help Change Happen	Make Change Happen
Chief		X		O
Council		X	O	
District Atty.	X		O	
Telecomm.	X	O		
Chamber of Commerce		X	O	

X = Current

O = Desired

Chief of Police

The Police Chief recognizes that the community looks to him to keep them safe from harm, both physically and psychologically. He also realizes that the support of the community is needed to accomplish the mission of the agency. If he is not proactive, drastic results may occur for which he could be held responsible. In the area of concern, such drastic results could be someone's death due to a computer being hacked and electronic impulses or charts changed, or a person's assets being eliminated resulting in bankruptcy or suicide. Such a situation could be compounded by the evolving trend whereby dependence of electronic data information and services by businesses and homes will be the norm. The Chief will want change to occur and must be one of the "cheerleaders" to help this happen.

The transition manager must keep the Chief apprised of changes in technology and encourage him to speak before businesses and criminal justice groups to acknowledge the catastrophic results of computer crime, particularly from an economic standpoint. The Chief must be the primary Department representative to the Fresno City Council through the City Manager's office, and must present his vision of what needs to be accomplished, selling the need to establish the computer crime investigation unit. The Chief must then ensure the project is completed. He must have a thorough understanding of the impact of computer crime and be able to articulate the consequences of the exploratory scenario. The transition manager must ensure that the Chief has adequate information. Thus, the Chief must move from a "let change happen" mode to one of "make the change happen." He must empower the transition manager with the latitude to develop the liaison with the other criminal justice agencies involved with the concept. He will also need to garner the support of the Chamber of Commerce, computer industry, and private security.

The Fresno City Council

The Fresno City Council realizes that they control the economic picture for the City of Fresno. Budgets are limited; however, they must be educated as to the seriousness of computer crime. They represent the citizens and the business community; therefore, they realize they can ill afford negative press, particularly in today's "hate the government" mood swing. The Council would be more receptive to allocating resources if they saw or observed a combined effort among different criminal justice agencies. The

Council is in a "let change happen" mode, and must move to one of "helping the change happen."

The transition manager must prepare and educate the Council as to the seriousness of the problem, emphasizing that their constituents may lose a substantial amount of funding if the project does not come to fruition. The transition manager must also engage the City Council in joint sessions with the Fresno County Board of Supervisors, assisting them in understanding the problem and sharing the responsibility. The transition manager would also need to pursue grant funding from the state or federal government for budget support and focus on the regional concept of attacking the problem. The City Council would be instrumental in this pursuit by passing local legislation in support of the unit, contacting district, state, and federal representatives for support.

Fresno County District Attorney

The Fresno County District Attorney's office is suffering from the same budget constraints as other government agencies. The County of Fresno is in the midst of a difficult economic period and its resources are limited. Thus, the District Attorney may attempt to block change due to personnel shortages and an already overburdened work force. The District Attorney does not have the technical expertise to investigate computer offenses and would therefore be reluctant to pursue a complaint in court. However, as computer crime becomes more newsworthy, the District Attorney will be expected to prosecute offenders.

The District Attorney is an integral element of the planned strategy and must be involved in the change process. He must move from a "let change happen" to "helping the change happen" mode.

The transition manager must coordinate his efforts with the District Attorney liaison and ensure that communication is paramount and that education of the technicalities of the crime occurs. The transition manager must assist in training the prosecution attorneys on the technological aspects of computer crime. Frequent meetings and an adoption of a joint venture are key to transition. The transition manager must also enlist the support of the District Attorney by applying for grant monies to assist in the funding of this project.

Telecommunications Companies

The main medium computer criminals use to infiltrate a computer system is phone lines via a telecommunications modem. Several telecommunications carriers have flourished due to government deregulation of the telecommunication monopoly held by AT & T. Consequently, a computer criminal who commits a crime across state lines can be shifted through several different carrier providers. For purposes of investigation, a search warrant must be obtained from each carrier for prosecution. Telecommunications companies are caught in a dilemma---they want to cooperate with law enforcement in apprehending the offenders, particularly if their customers incur phone debts out of their control. However, they are also aware of the search and seizure aspect and must pay heed to the release of sensitive information. Their reluctance to being sued civilly could cause them to block the change.

The telecommunication companies need to "let change happen" and assist law enforcement in the education process. They must also realize that their fear of search and seizure may become the focal point of a wrongful death or loss of property suit by allowing free access for criminal hackers to victimize individuals.

The transition manager must actively cooperate with the telecommunication companies, asking them to be involved with the joint task force. They must be encouraged to train the assigned criminal justice participants. The transition manager will want to consider the telecommunication companies as a viable source of economic stimulus. Meetings with company executives and local staff would assist in this endeavor, particularly if the concept were viewed as a consolidated investigative effort.

Chamber of Commerce

Today's economic picture is bleak, and businesses can ill afford substantial overhead. The average "hit" of a computer crime is \$470,000 to \$540,000. There are few businesses able to stay solvent for long, should such a depletion of resources occur. Smaller businesses could fall prey to computer hackers as well, dissolving more quickly as assets are lost. Consequently, the business community would welcome law enforcement's efforts to curb this crime. Today's shrinking government resources do not instill the necessary confidence the business community should have in law enforcement's ability to investigate computer crimes. Businesses would be apprehensive about reporting losses to the public, for fear of a loss of faith by the community. Such losses would no doubt be sensationalized and law enforcement would be pressured to apprehend the offenders. The Chamber of Commerce could want change to occur, encouraging law enforcement to

pursue its investigative efforts. The strategy of a combined and united effort would motivate the Chamber of Commerce representing the business community to embrace law enforcement. Thus the Chamber of Commerce would be in a "let change happen" mode and would need to "help the change happen."

The transition manager must request the business community's assistance in the effort of establishing the computer crime investigation unit. The business community has a voice in the political arena, and the transition manager must coordinate the efforts of the unit to reach the City Council, Board of Supervisors, and state and federal politicians. They must be educated as to the seriousness of this crime, the lack of security, and the need to develop safeguards to employees who may attempt to disrupt the business climate through malicious acts, theft of funds, or intentional destruction. The transition manager should include representatives from the business community on a steering committee along with members of the telecommunication companies and other critical mass individuals. The committee purpose would be education, updating, and coordination of progress.

Transition Management Structure

The Chief of Police, although the lead person for this project, does not have the technical expertise required. He must appoint a transition manager to facilitate the effective establishment of the computer crime investigation unit. The transition manager must work with the District Attorney's office and judicial unit to accomplish the set goal. The Chief of Police must lend his support to the project through the media. He must be willing to share this responsibility with those in charge of the other two government

criminal justice agencies to encourage a joint approach to the project. The transition manager must have a solid technical base in understanding computers, and must possess good organizational skills, particularly with the two other criminal justice agencies. The transition manager must have very good interpersonal skills and be able to amicably interact with the lead members from the District Attorney's Office and the judicial representative. The transition manager must be able to share in the development of the program and coordinate its implementation. He must have the ability to interrelate with the City Council, Board of Supervisors, and business community as an educator and information provider. Commensurate with the desired ability to interrelate with those outside of the police agency, is the necessity to inform the members of the internal organization of transition progress.

The Chief of Police would appoint a lieutenant to this position, expecting to be kept abreast of the progress of the project and planning of the transition. The Chief of Police would recognize that the transition manager must be given the authority and responsibility to ensure the plan is enacted, especially with the other agency counterparts.

The transition manager must share responsibility with the representatives from the other criminal justice agencies. The transition manager would absorb the lead role on this committee since he has the technical expertise regarding computer crime. This shared committee approach would be expanded eventually to include members from the telecommunications companies and members from the business community.

Implementation Techniques and Methods

Change can be enigmatic if there is no manner or method to ease its inception. People are always affected when change is imminent; and if a comfort zone is disturbed, the change meets with resistance. The role of the transition manager is designed to take these factors into account and move the desired future state to reality. It is critical that the change be planned and organized and that information be given to all internal and external parties affected. The transition manager, in concert with the critical mass and others, can accommodate the change through time.

The key to change is to emphasize its positive attributes and diminish any negative energy which would hamper its success. For this reason, different techniques and methods are used to heighten awareness and create a smooth transition. The methods and techniques to be used for this change would be the following:

Communication of the Vision

The desired future state must be clear and understandable and the vision must be understood by all affected parties. A clear image of what the change will accomplish is provided and all involved parties will have the same knowledge of what the future will entail. The Chief of Police is responsible for assembling the vision statement and must enlist the transition manager in its final development.

The transition manager must communicate the vision to all parties and it should be written and understood by all. The manager should also meet personally with all affected parties to verbally communicate the points of the vision and eliminate confusion

as to interpretation of the written document. The personal contact, whether it be by individual or group meetings, can also invoke instant feedback.

Role Model

Nothing detracts from a project or idea faster than negative energy. The transition manager must display an enthusiastic attitude, emphasizing positive movement. Any display of negative comments or feelings must be dealt with immediately. This can be accomplished by frequent meetings where information is exchanged, involvement of affected parties in decision-making, and celebration of small successes. Neglect in this area can cause discontent or frustration, hampering progress.

Responsibility Charting

The fact that three criminal justice agencies are involved in this project suggests that responsibilities need to be clear-cut so as to avoid duplication of effort and ensure accountability. The implementation team, consisting of the transition manager and representatives from the District Attorney's Office and Judicial Office, need to generate a list of tasks which will lead to the occurrence of change. Once tasks are assigned, it is the members' responsibility to ensure success of the tasks. It is incumbent upon the transition manager to coordinate this effort and ensure, through weekly meetings, that progress is being made on each task. This would also allow for adjustments in task accomplishment. The responsibility chart clarifies roles of transition team members as to who has responsibility, authority, provides support, or is informed of decisions. (Appendix H).

Computer Crime Project Team

The three law enforcement agencies must educate themselves and work in tandem in order for the project to come to fruition. After area responsibilities have been determined and the transition manager and implementation members are more comfortable with each other, the implementation team should be expanded to include the business community and telecommunications companies. Selection of the business community members and telecommunications representatives should be made by the Chief of Police, the transition manager, the District Attorney's office, and judiciary. The support of the additions to the transition team in the political process will be needed to overcome budget resistance from the City Council and Board of Supervisors. They can also augment the project with their involvement in training of the team members and assist in the procurement of state of the art equipment. The team should meet monthly to discuss progress. Lastly, use of their political clout could minimize budget resistance.

Goal-Setting and Time Management

A vision sets forth a desired result where one wants to be in the future. Once a desire is communicated, a plan and goals are soon to follow. The energy created by the vision must be reached in an organized and timely fashion. Frustration is eliminated by allowing all parties to understand the needs and the direction required to reach the desired result. The transition manager will need to coordinate the activities of the project and assure that goals are established.

Time can be a critical element during the transition state. Individuals can become frustrated if they lose sight of the goals and spend their time performing tasks not related

to the transition. Today's climate suggests that more work is being done by less people and when people are given more work than time, tasks will be missed, unfinished or poorly performed. The transition manager must keep the focus on the transition and specify time lines to help keep the pace of change. These steps will let everyone know the direction of change and the time in which it should be accomplished.

Rewards

Successes should be celebrated: everyone enjoys being told that they have done a good job. People are generally motivated when they are recognized for their efforts. The transition manager must ensure that individuals or groups receive recognition for their accomplishments. This can be done by formally acknowledging accomplishments in meetings, Council and Board of Supervisors proclamations, social outings for the implementation team, and something as simple as praising performance at the time of the accomplishment. These experiences promote positive energy and tend to reduce friction and frustration.

Feedback/Evaluation Mechanism

The transition manager must prepare a monthly report for the Chief of Police describing the progress of the transition. A copy of the report should be sent to the Chief Prosecuting Attorney and head judicial justice. Transition team members must participate in the development of the monthly report. The transition manager will need to conduct quarterly progress meetings with the police department, prosecution, and judiciary and provide an update of progress to date and delineate the anticipated progress for the next three months.

Summary

Change can occur smoothly or can be erratic and destined for failure. Successful change is always the desired state. Once a vision has been created and a decision has been made to pursue the vision, a plan is developed to implement the change. The appointment of a transition manager is a step to ensure the change is reached. Change is inevitable and people fear the change, resisting its implementation when comfort zones are disturbed or when there is no clear communication. The transition manager can allay such fears with an organized plan for the change and through the use of interpersonal and management skills.

Computer crime invades privacy, is costly to the community, and can lead to tragic occurrences. The establishment of a computer crime investigation unit can help alleviate these concerns. The transition of this change will lead to a smooth implementation of the unit and can mean success for the shareholders, critical mass, investigators and the public they serve. A critical consideration for the implementation of this plan is the length of time needed for the unit to be functional. Change does not occur overnight, and this transition period is no exception. It may be several years before the unit is established and able to impact events or trends. Also, the occurrence of an event and significant change in a trend can cause the plan to be modified both in brevity of time or prolongation. It is fundamentally important, however, that the plan eventually be implemented.

PART 5

Study Conclusion

The study sought to address the issue and sub-issues of the impact of computer crime on a large law enforcement agency. Specifically, the issue is:

- What impact will computer crimes have on a large law enforcement agency by the year 2002?

The sub-issues are:

- Will the responsibility for investigating computer crimes rest with law enforcement?
- What type of training and education will be needed by the investigating body?
- How will the investigating unit keep pace with technology?

A variety of techniques were used to address the issues. Scanning of newspapers, trade journals, periodicals, library research, group techniques focusing on input data collection, and analysis were employed for study purposes. Based on the information of the study, the issues and sub-issues were addressed.

Issue:

What impact will computer crimes have on a large law enforcement agency by the year 2002?

The computer criminal of tomorrow will deviate from the common stereotype of today. Computers will be owned by a vast majority of the populace, and as society

becomes more computer dependent, criminals will adapt. Law enforcement is not treating the crime of computer abuse with any degree of priority. The trends and events point to catastrophe, and the driving forces mentioned in the introduction are changing society. The criminal is employing the use of technological devices in his or her "trade." The strategic plan identified a manner to address the exploratory scenario through the involvement of three components of the criminal justice system.

Sub-Issue:

Will the responsibility for investigating computer crimes rest with law enforcement?

The selected strategy clearly indicates law enforcement along with the prosecution and judiciary as being responsible for investigating the crime. The transition management plan explained the manner in which the strategy could be implemented. If government does not wish to support the law enforcement agency and decides to privatize the investigation of computer crimes, then the law enforcement agency would be relieved of the responsibility. Unfortunately, economic-based decisions play a very large role in government's decision to perform functions--sometimes leading to the demise of the community.

Sub-Issue:

What type of training and education will be needed by the investigating body?

The investigating body will need technical training on the use of computers, evidence collection, different operation systems and advancements in technology. The strategic plan identified this area as a weakness and under the implementation plan

suggested agencies which could assist in this endeavor. Also, an aggressive educational program is needed for the community, criminal justice organization, and government units.

Sub-Issue:

How will the investigating unit keep pace with technology?

Technology is increasing at an exponential rate. Desktop personal computers were introduced during the late 1970's and early 1980's. Since then, technology has undergone a complete metamorphosis and the future will be no exception. The economic picture for government is of grave concern today and unless there is a change for the better, it will continue to worsen. For this reason, technological advancements may not be accessible to the investigation unit. The strategic plan offered suggestions such as grant funding, partnerships with the business community, and the possibility of contracting the investigation component to the private sector as methods of resolving the problem. It is paramount that the investigation unit be supplied with state-of-the-art equipment to be effective.

The study is not all-inclusive and can change based on the occurrence of the trends and/or events. There are areas which need further study. An example is the need to identify funding sources to augment government. Development of standards for computer vendors and the impact of this crime on the rest of the criminal justice system also needs further study. Also, privatization of computer crime investigations may warrant future research.

Alas, the computer crime of today will be different tomorrow. The writer believes that with a proactive outlook, law enforcement will be able to cope with change and impact tomorrow's future.

Notes to Pages 1-18

Part 1. INTRODUCTION

- ¹ "Robert Morris, Jr.," Scuttlebut: MIS Week (October 9, 1989): 50.
- ² "They Start So Young Nowadays," Scuttlebut: MIS Weed (May 7, 1990): 46.
- ³ "Hackers at War", Media Report Data Nation (January 1, 1992): 21.
- ⁴ French, Desiree, "Scams Flourish in Electronic Filing System," USA Today (June 15, 1992): 3B.
- ⁵ Bee News Services, "Hackers Credit Card Scam Found," Fresno Bee (April 18, 1992): A1.
- ⁶ Associated Press, "Computer Avenger Lurks in Bulgaria," Fresno Bee (January 30, 1992): A12.
- ⁷ Associated Press, "Freeway Phone Gets \$1,600 Bill," Fresno Bee, (October 24, 1992): A3.
- ⁸ New York Times, "Two Computer Hackers Plead Guilty," Fresno Bee (December 5, 1992): A10.
- ⁹ Clark, Don, "Hacker Re-Indicted," San Francisco Chronicle (December 8, 1992): C3.
- ¹⁰ Media Report, "Phrack Attack," Datamation (December 15, 1990): 29.
- ¹¹ Schwartz, John, "Sex Crimes on Your Screen?" Newsweek (Dec. 23, 1991): 66.
- ¹² Dallas Morning News, "FBI Investigates Charges of Computer Hacking by Perot Campaign," Fresno Bee (January 2, 1993): A7.
- ¹³ Saavedra, Tony, "Firms Hit by Young Hackers Take a Toll on Family Finances," Fresno Bee (February 19, 1993): A3.
- ¹⁴ Randall, John D., The Tojo Virus (New York: Kensington Publishing Corp., 1991).
- ¹⁵ Vobejda, Barbara, "Technology Whittles Down Number of Farmers," Fresno Bee (June 14, 1992): E1.
- ¹⁶ "When Technology Goes Global," Fresno Bee (January 27, 1992): B6.

¹⁷ Fall Motoring Special Advertising Section, "Phones, CD's, Luxury Touches Make Cars More Like Home," Fresno Bee (October 17, 1991): 8.

¹⁸ "Gadgets Ahead of Their Time," San Francisco Examiner (Feb. 2, 1992): E-4.

¹⁹ Corcoran, Cate, "Voice Recognition Moving Down To PC's," Infoworld (Nov. 11, 1992): 33.

²⁰ Vernaci, Richard L., "Phones Getting Smarter," San Francisco Examiner (Dec. 29, 1991): E-12.

²¹ CEO Info, "IBM Scientists First to Build Structures One Atom At a Time," Government Technology (February 1991): 25.

²² Lininger, Skye, "Mobile Office is Reality of '90's," Los Angeles Times (Dec. 7, 1992): C-14.

²³ Hanson, Wayne, "Say Hello to the National Computer Network," Government Technology (March 1992): 48.

²⁴ Cornish, Edward, "Issues of the 90's," 1990 World Future Society (Bethesda, MD: 1990), 10.

²⁵ Taylor, Charles, Presentation at the Command College Graduation for Class 15 (San Marcos, CA: Jan. 15, 1993).

²⁶ "Outlook '92 and Beyond: Recent Forecasts from the Futurist Magazine," World Future Society, (1991): 2.

²⁷ Caldwell, Bruce, "Where Have All the Clerks Gone?" Information Week (April 8, 1991): 15.

²⁸ Pressman, Roger S. and S. Russell Herron, Software Shock (New York: Dorsey House Publishing, 1991), 76.

²⁹ Hanna, Donald G., Police Executive Leadership (Champaign, Ill.: Stipes Publishing Co., 1990), 4.

³⁰ Toffler, Alvin, The Third Wave (New York: William Morrow & Company, 1980), 211-223.

³¹ "Blinders for Iraq's Defenses," Newsweek (Jan. 28, 1991):37.

³² Mintz, Frederick, Lecture for Command College Class 16, June 26, 1991.

³³ Paul, Fredric, "Dialing for Data," PC Computing (November 1988): 196-208.

³⁴ Ibid.

³⁵ LaPolla, Stephanie, "High Tech-s Dark Side: Fraud, Forgery, Check Swindles; Scanners, Printers are Accomplices in Crime," PC Week vol. 9 (July 20, 1990): 23.

³⁶ Webster, Barbara and Michael S. McCampbell, "International Money Laundering: Research and Investigation Join Forces," National Institute of Justice (September 1992): 4-5.

³⁷ Warwick, David R., "The Cash-Free Society," The Futurist (November-December 1992): 19-22.

³⁸ Budwey, James N., "Information Industry in Transition," Internet (February 1992): 2.

³⁹ Paul, Fredric, "Dialing For Data", PC Computing (November 1988), 196-208.

⁴⁰ Stephens, Gene, "High-Tech Crime Fighting," The Futurist (July-August 1990): 20-25.

⁴¹ Riley, Tom, "Privacy Concerns: A Symptom of Mistrust?" Government Technology (Nov. 1992): 21.

⁴² Notes and Handouts, "Criminal Investigation in an Automated Environment," Federal Law Enforcement Training Center (Glynco, VA.: Dec. 3-14, 1990).

⁴³ Ibid.

⁴⁴ Coutourie, Larry, "The Computer Criminal: An Investigative Assessment," FBI Law Enforcement Bulletin (Sept. 1989):19-22.

⁴⁵ Watson, Neil, "Can Today's Hacker Laws Work?" Communications Week (Sept. 18, 1989): 32.

⁴⁶ Top of the Week, "Phone Fraud: Somebody's Got to Pay," Information Week (May 6, 1991): 12-13.

⁴⁷ Tamaki, Julie, and Michael Connelly, "Computer Skills Aid '90's Credit Card Scam," Los Angeles Times (Aug 23, 1992): B1-42.

⁴⁸ Media Report, "Watch Your Data," DataNation (December 1, 1991): 23.

⁴⁹ Stoll, Clifford, The Cuckoo's Egg (New York: Doubleday, 1989).

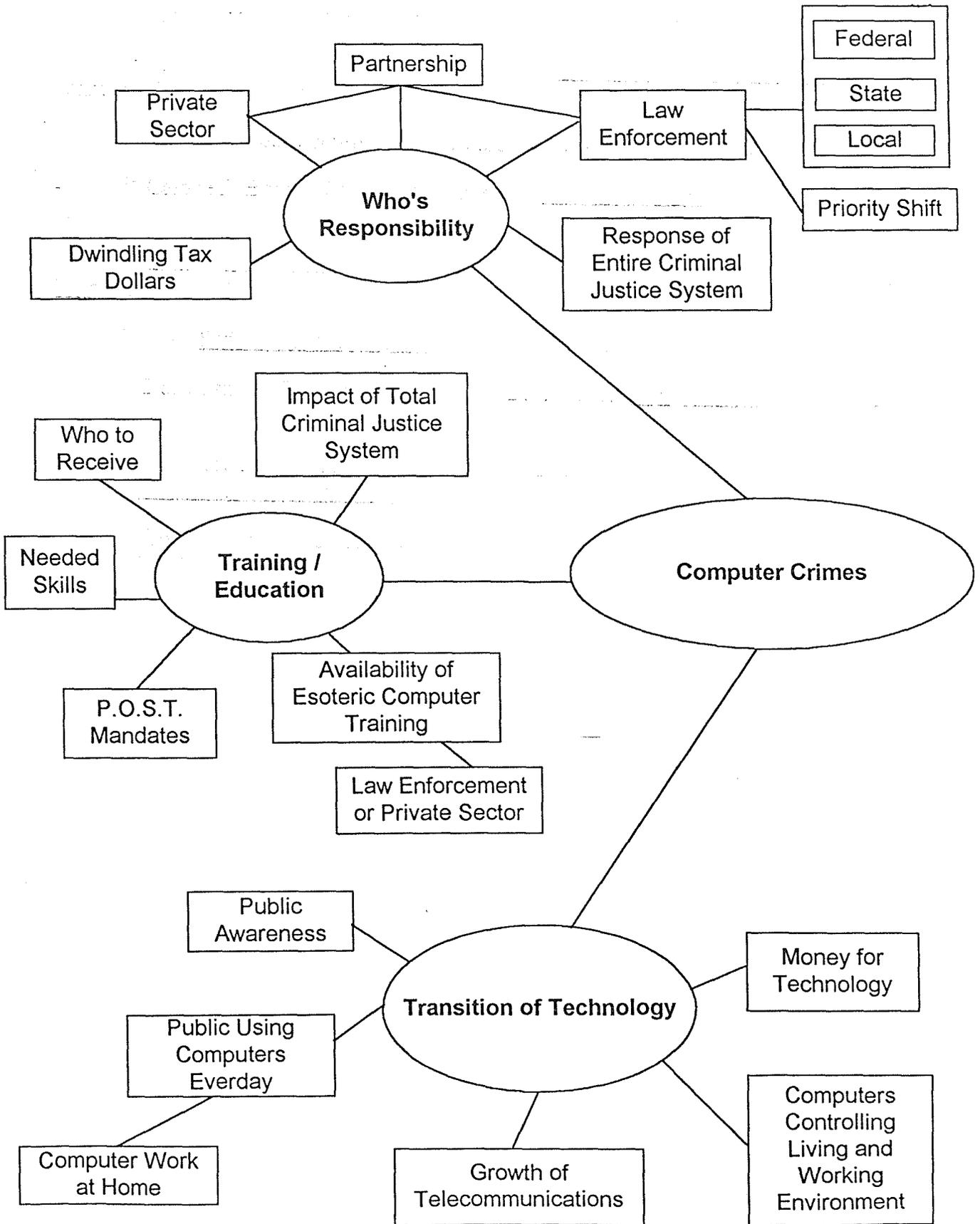
⁵⁰ Vobejda, Barbara, "How Electronic Gadgetry is Changing Childhood," San Francisco Chronicle (July 30, 1991): D3.

- ⁵¹ 11:00 p.m. News, CBS Channel KXTV 10, Sacramento, CA. March 4, 1993.
- ⁵² McEwen, J. Thomas, "Computer Ethics," National Institute of Justice Reports (January-February 1991): 8-11.
- ⁵³ Rayl, A. J. S., "Secrets of the Cyberculture," Omni (Nov. 1992): 59-67.
- ⁵⁴ Caldwell, Bruce, "Outlaws or Pioneers," Information Week (July 16, 1990): 12-13.
- ⁵⁵ Zimmerman, Michael R., "Drug Dealers Find Haven in On-Line Services," PC Week (March 4, 1991): 43.
- ⁵⁶ NA, Software Industry Bulletin vol. 8 (Nov. 9, 1992): 3.
- ⁵⁷ Daly, James, "Toll Fraud Biting Into Businesses," Computerworld vol. 26 (Dec. 7, 1992): 71.
- ⁵⁸ Webster, Barbara A. and J. Thomas McEwen, "Assessing Criminal Justice Needs," National Institute of Justice (August 1992): 4-5.
- ⁵⁹ Gould's Penal Code Handbook, California Penal Code Section 502 (Altamonte Springs, FL: Gould Publications), pp. 125-126.
- ⁶⁰ Ibid.
- ⁶¹ Mark Haynes, Interview with author, March 23, 1993.
- ⁶² Ibid.
- ⁶³ Coursey, David, "Asimov: Future Computers Will Make Work Fun," MIS Week (Nov. 6, 1989): 44.
- ⁶⁴ Lasker, Lawrence, and Walter F. Parkes, Sneakers (New York: Signet, 1992), 198.

Notes to Pages 49-73

Part 3. STRATEGIC PLAN DEVELOPMENT

- ¹ Mission Statement, Fresno Police Department, 1992.



Appendix B
NGT PANEL

98

- Mr. Conrad Nerdahl, Police Community Service Officer assigned to Crime Analysis, Fresno Police Department
- Mr. Ken Diliberto, Computer Technician - City of Fresno Information Systems Division
- Mr. John Clark, Investigator - California Department of Motor Vehicles
- Mr. Roger Enmark, Police Lieutenant - Crimes Against Property
- Mr. Tom Frost, Police Lieutenant - Area Commander
- Mr. Henry Monreal, Police Investigator - White Collar Crime Unit
- Mr. Steve Shultz, Fiserv Corporation, Computer Consultant and Part-Time Lecturer for computer course at California State University, Fresno

1. Paperless society.
2. Computer in home.
3. Computer controlled equipment networked on a global basis.
4. Telecommuting from any location.
5. Massive availability of information.
6. In-house investigation by private sector.
7. Reporting of computer crime to law enforcement.
8. Bi-directional invasion of privacy via video conferences.
9. Computerized classrooms.
10. Computer crime investigation organizations.
11. Security development and standards for computer systems.
12. Funding to investigate computer crime violations.
13. BBS networks.
14. Qualifications of personnel who access computer information systems.
15. Electronic fund transfer: home banking, retail sale, etc.
16. Number of people incarcerated for computer crimes.
17. Contracting for data processing services.
18. Artificial intelligence.
19. Downsizing to PC's.
20. Specialized units.
21. Civil disobedience through computer.
22. Home automation.
23. Electronic mail.
24. Court decisions: case law
25. Ethics of computer use.
26. Virus.
27. Virtual reality.

Appendix D
NGT EVENTS

100

1. Deviant individuals associated with computer gangs.
2. City water supply disabled by hacker.
3. Political assassination of candidate dumped on BBS.
4. Police contract computer crime investigations to private sector.
5. State of California files bankruptcy.
6. Hacker transfers dormant funds from savings account.
7. Hacker breaks ICBM security code.
8. Hospital patient dies from computer hacker.
9. Police stunned through computer hacker disabling MDT's.
10. Judge rules police violate fourth amendment rights for investigation of computer crimes.
11. Major bank collapses due to electronic funds theft.
12. City Council determines police will not investigate computer crimes.
13. Programmer transfers funds to own bank account.
14. Family devastated by hacker after altering personal information.
15. Foreign power causes nationwide communications failure.
16. Hostile takeover of large corporation through manipulation of company assets.
17. Legislation establishes DOJ computer crime unit.
18. Hacker alters NCIC database.
19. Wall Street brought to knees by hacker.
20. State prison inmate sets himself free.
21. Hacker sets-off major military movement.
22. 16,000 Californians lose drivers license before a virus is detected.
23. Food recall forced after hacker changes General Mills data information system.
24. IRS employee victim of hacker.
25. Sophisticated criminals form organization to thwart computer crime investigators.

Appendix E

ASSUMPTION MAPPING

		Certain			
			1A	1B	
			3A	9A	9B 11A
		5A 5B		6B	10B
			7B	8A	
			1C	3C	10A
		2B		10C	
7A	2A		3B	6A	
	4B		4A	8B	
			7C	11B	
		Uncertain			

Stakeholders

- | | |
|----------------------|--------------------------------------|
| 1. Chief of Police | 7. Computer Vendors |
| 2. City Council | 8. Telecommunications Companies |
| 3. P.O.S.T. | 9. Dept. of Justice/Attorney General |
| 4. Media | 10. Business Community |
| 5. District Attorney | 11. Private Security |
| 6. Court Judges | |

Appendix F
MODIFIED POLICY DELPHI

Mr. Frank Clark - Police Specialist	Computer Crime Unit - Fresno Police Dept.
Mr. Hal Hansen - Police Specialist	Personnel and Training Unit - Fresno Police Dept.
Mr. Conrad Nerdahl -Community Services Officer	Crime Analysis - Fresno Police Dept.
Mr. Mike Guthrie - Lieutenant	Internal Affairs - Fresno Police Dept.
Mr. Roger Enmark - Lieutenant	Crimes Against Property - Fresno Police Dept.
Mr. Tom Frost - Lieutenant	Area Commander - Fresno Police Dept.
Mr. Pat Rhames - Captain	Field Operations - Fresno Police Dept.
Mr. Richard Desmond - Sergeant	White Collar Fraud Unit - Fresno Police Dept.

Appendix G

STAKEHOLDER PERCEPTIONS

Strategy 1 State Legislature Asset Seizures	1	2	3	4	5	6	7	8	9	10	11
	S	S	S	O	O	S	I	O	S	S	O
Strategy 2 Special Team	S	S	S	S	S	S	S	S	S	S	O
Strategy 3 Change Intent Law and Penalty	S	SI	S	I	SI	SI	I	I	S	S	O

1. Chief of Police
2. City Council
3. P.O.S.T.
4. Media Oppose Controversy
5. District Attorney
6. Court Judges
7. Computer Vendors
8. Telecommunication Companies
9. DOJ/AG
10. Business Community
11. Private Security

Support Oppose Indifferent

Appendix H

RESPONSIBILITY CHART

R = Responsibility (not necessarily authority)

A = Approval (right to veto)

S = Support (put resources toward)

I = Inform (to be consulted)

- = Irrelevant to this item

Actors

Decision	Chief of Police	Project Manager	Prosecution Attorney	Judiciary	City Manager
Type of Training	A	R	A	A	I
Cost/Benefit	A	R	I	I	I
Evaluation	A	R	I	I	I
Equipment Acquisition	A	R	I	I	A/S
Personnel Commitment	A	R	A	A	A

BIBLIOGRAPHY

Books

- Bequai, August. Technocrimes. Massachusetts: Lexington Books, 1987.
- Hafner, Katie and John Markoff. Cyberpunk. New York: Simon and Schuster, 1991.
- Hanna, Donald G. Police Executive Leadership. Champaign, Ill.: Stipes Publishing Co., 1990.
- Lasker, Lawrence, and Walter F. Parkes. Sneakers. New York: Signet Published by the Penguin Group, 1992.
- Naizbitt, John. Megatrends. New York: Warner Books, 1982.
- Pressman, Roger S. and S. Russell Herron. Software Shock. New York: Dorset House Publishing, 1991.
- Randall, John D. The Togo Virus. Kensington Publishing Corp., 1991.
- Sanders, Donald. Computers Today. New York: McGraw Hill, 1988.
- Sterling, Bruce. The Hacker Crackdown. New York: Bantam Books, 1992.
- Stoll, Clifford. The Cuckoo's Egg. New York: Doubleday, 1989.
- Toffler, Alvin. Powershift. New York: Bantam Books, 1990.
- Toffler, Alvin. The Third Wave. New York: William Morrow and Company, 1980.

Journals

- Buchok, James. "\$5M Suit Filed Over Database Copying Claim." Computing Canada (November 9, 1992): 1.
- Budwey, James N. "Information Industry in Transition." Internet (February 1992): 2.
- Caldwell, Bruce. "Outlaws or Pioneers." Information Week (July 16, 1990): 12-13.
- Caldwell, Bruce. "Where Have All the Clerks Gone?" Information Week (April 8, 1991):34.

- Chin, Andrea. "The Coming Bottleneck." *Information Week* (April 22, 1991): 66.
- CEO Info, "IBM Scientists First to Build Structures One Atom at a Time." *Government Technology* (February 1991): 25.
- Corcoran, Cate. "Voice Recognition Moving Down to PC's." *Infoworld* (November 11, 1992): 33.
- Cornish, Edward. "Issues of the 90's." World Futures Society, Bethesda, MD.
- Coursey, David. "Asinov: Future Computers Will Make Work Fun." *MIS Week* (November 6, 1989): 44.
- Coutourie, Larry. "The Computer Criminal: An Investigative Assessment." *FBI Law Enforcement Bulletin* (September 1989): 19-22.
- Daly, James. "Toll Fraud Biting into Businesses." *Computerworld* (Dec. 7, 1992): 71.
- Eliot, Lance B. *AI Expert* (January 1992): 11-13.
- Executive Summary. "Chips." *Information Week* (Feb. 18, 1991): 10.
- Hanson, Wayne. "Say Hello to the National Computer Network." *Government Technology* (March, 1993): 48.
- LaPolla, Stephanie. "High Tech's Dark Side: Fraud, Forgery, Check Swindles; Scanners, Printers are Accomplices in Crime." *PC Week* (July 20, 1992): 23.
- Leibs, Scott. "Judgement Day." *Information Week* (May 7, 1990): 57.
- Mahabharat, C. T. "India: Security Imaging System." *Newsbytes* (Jan. 11, 1993).
- Media Report. "Phrack Attack." *Datamation* (Dec. 15, 1990): 29.
- Media Report Section. "Go Wireless, With No Strings Attached." *Datamation* (March 1, 1991): 19.
- Media Report. "Watch Your Data." *Datamation* (Dec. 1, 1991): 23.
- Media Report. "Hackers At War." *Datamation* (Jan. 1, 1992): 21.
- Newsweek. "Blinders for Iraq's Defenses." *Newsweek* (Jan. 28, 1991): 17.

- Orrick, Phyllis. "Mac Crime Wave Hits Big Apple: Bandits Leave Police Perplexed." *MacWeek* (Jan. 25, 1992): 34.
- "Outlook '92 and Beyond: Recent Forecasts from the Futurist Magazine." *World Future Society*, 1991.
- Paul, Fredric. "Dialing for Data." *PC Computing* (Nov. 1988): 196-208.
- Polilli, Steve. "The High-Tech Court of the Future." *Governing* (Sept. 1992): 18-19.
- Port, Otis. "Now, Big Brother Can Listen from a Hung-Up Phone." *Business Week* (Sept. 7, 1992): 93.
- Rayl, A. J. S. "Secrets of the Cyberculture." *Omni* (Nov. 1992): 59-67.
- Richter, M. J. "Sharing Information." *Governing* (Feb. 1991): 37-54.
- Riley, Tom. "Privacy Concerns: A Symptom of Mistrust?" *Government Technology* (Nov. 1992): 21.
- Schwartz, John. "Sex Crimes on Your Screen?" *Newsweek* (Dec. 23, 1991): 66.
- Scuttlebut. "No Robert Morris, Jr." *MIS Week* (Oct. 9, 1989): 50.
- Scuttlebut. "They Start So Young Nowadays." *MIS Week* (May 7, 1990): 46.
- Sessions, William. "Computer Crimes: An Escalating Crime Trend." *FBI Law Enforcement Bulletin* (Feb. 1991): 12-15.
- Sherizen, Sanford. "Security Weakness Makes Data Vulnerable." *Software Magazine* (Nov. 15, 1992): 66.
- Software Industry Bulletin*. "Software Piracy Now a Felony." Vol. 8 (Nov. 9, 1992): 3.
- Stephens, Gene. "High-Tech Crime Fighting." *The Futurist* (July-August 1990): 2.
- Taft, Darryl K. "Intel Says New Supercomputers Can Handle Up to 300 GFLOPS." *Government Computer News* (Dec. 23, 1991): 27.
- Toffler, Alvin and Heidi Toffler. "The Future of Law Enforcement: Dangerous and Different." *FBI Law Enforcement Bulletin* (Jan. 1990): 14.
- Top of the Week. "Phone Fraud: Somebody's Got to Pay." *Information Week* (May 6, 1991): 12-13.

Warwick, David R. "The Cash-Free Society." *The Futurist* (November-December 1992): 19-22.

Watson, Neil. "Can Today's Hacker Laws Work?" *Communication Week* (Sept. 18, 1989): 32.

Zimmerman, Michael R. "Drug Dealers Find Haven in On-Line Services." *PC Week* (March 4, 1991): 43.

Newspapers

Associated Press. "Freeway Phone Gets \$1,600 Bill." *The Fresno Bee*, 24 October 1991, A3.

Associated Press. "Computer Avenger Lurks in Bulgaria." *The Fresno Bee*, 30 January 1993, A12.

Bee News Services. "Hackers Credit-Card Scam Found." *The Fresno Bee*, 18 April 1992, A1.

Clark, Don. "Hacker Re-Indicted." *San Francisco Chronicle*, 8 Dec. 1992, C3.

Dallas Morning News. "FBI Investigates Changes of Computer Hacking by Perot Campaign." *The Fresno Bee*, 2 January 1992, A7.

Fall Motoring Special Advertising Section. "Phones, CD's, Luxury Touches Make Cars More Like Home." *The Fresno Bee*, 17 October 1991, 8.

French, Desiree. "Scams Flourish in Electronic Filing System." *USA Today*, 15 June 1992, 3B.

Fresno Bee. "Computer Masters Ancient Chess Puzzle." 29 October 1991, A7.

Fresno Bee. "When Technology Goes Global." 27 January 1992, B6.

Lininger, Skye. "Mobile Office is Reality of '90's." *Los Angeles Times*, 7 December 1992, C14.

Los Angeles Times. "Computer Skills Aid '90's Credit Card Scam." 23 August 1992, B1.

New York Times. "Two Computer Hackers Plead Guilty." *Fresno Bee*, 5 December 1992, A10.

Saavedra, Tony. "Firms Hit by Young Hackers Take a Toll on Family Finances." The Fresno Bee, 19 February 1993, A3.

San Francisco Examiner. "Gadgets Ahead of their Time." 2 February 1992, E4.

Vernaci, Richard L. "Phones Getting Smarter." San Francisco Examiner, 29 Dec. 1991, E12.

Vobejda, Barbara. "How Electronic Gadgetry is Changing Childhood." San Francisco Chronicle, 30 July 1991: D3.

Vobejda, Barbara. "Technology Whittles Down Number of Farmers." Fresno Bee, 14 June 1992: E1.

Public Documents

McEwen, J. Thomas. "Computer Ethics." National Institute of Justice Reports (Jan. Feb. 1991): 8-11.

Webster, Barbara A. and J. Thomas McEwen. "Assessing Criminal Justice Needs." National Institute of Justice (August 1992): 4-5.

Webster, Barbara and Michael S. McCampbell. "International Money Laundering: Research and Investigation Join Forces." National Institute of Justice (September 1992): 4-5.

Unpublished Material

Notes and handouts. Criminal Investigation in an Automated Environment. Federal Law Enforcement Training Center, 14 December 1990, Glynco, VA.

Taylor, Charles. 1992. Speech at Command College Graduation Class 15, 15 January, at San Marcos, California.

Interview

Haynes, Mark. Interview with author, 23 May 1993. Telephone interview, Fresno, California.

Television

KXTV 10, 11:00 p.m. News. 30 March 1993. Sacramento, CA.