

HOW WILL CALIFORNIA LAW ENFORCEMENT RESPOND TO THE NEED
FOR COMPUTER-BASED EXPERTISE IN THE IDENTIFICATION,
COLLECTION, AND PRESERVATION OF ELECTRONIC EVIDENCE BY THE
YEAR 2006?

A Project Presented to the
California Commission on
Peace Officer Standards and Training

By

Captain Edwin F. Flint
Sacramento County Sheriff's Department

Command College

Class XXXI

Sacramento, California

November 2001

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

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

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

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

© 2001 by the
California Commission on Peace Officer
Standards and Training

This project, written under the guidance and approval of the student's agency, mentor and advisor, has been presented to and accepted by the Commission on Peace Officer Standards and Training, State of California, in fulfillment of the requirements of Command College Class Thirty One.

Edwin F. Flint, Captain Sacramento County Sheriff's Department Student	Date
--	------

Lou Blanas, Sheriff Sacramento County Sheriff's Department	Date
---	------

George Anderson, Captain Sacramento County Sheriff's Department	Date
--	------

Sandy Boyd, Ed.D. Advisor	Date
------------------------------	------

Alicia Powers Senior Consultant POST	Date
--	------

TABLE OF CONTENTS

LIST OF TABLES.....	vi
ACKNOWLEDGEMENTS	vii

CHAPTER I

ISSUE IDENTIFICATION

Introduction.....	1
Issue Statement.....	4
Research Methodology.....	6
Environmental Scan	6
Literature Review.....	8
Interviews	9
Summary	13

CHAPTER II

FUTURES STUDY

Introduction.....	14
Nominal Group Technique.....	14
Trends.....	15
Events.....	23
Cross Impact Analysis	29
Alternative Scenarios.....	31
Optimistic Scenario	31
Pessimistic Scenario.....	33
Surprise Free Scenario	35
Summary	36

CHAPTER III

STRATEGIC PLAN

Introduction.....	38
Strategic Planning Model.....	38
Organizational Description	45
Situational Analysis	46
Strategy Development.....	48
Implementation Plan.....	49
Cost Analysis.....	51
Summary	53

CHAPTER IV

TRANSITION MANAGEMENT

Introduction.....	54
Commitment Plan.....	54
Management Structure	56
Transition Techniques	59
Summary	63

CHAPTER V

CONCLUSION

Project Summary 65
Evaluation Activities..... 67
Recommendations for the Future 68
Implications for Leadership..... 72
Conclusion..... 73

THE APPENDICES

Appendix A, Nominal Group Technique Panel 75
Appendix B, List of Trends 79
Appendix C, List of Events 81

ENDNOTES 83

REFERENCES..... 86

LIST OF TABLES

Tables

1	Trend Summary.....	16
2	Event Summary	24
3	Cross Impact Analysis Matrix	30
4	Opportunity Mapping Matrix.....	42
5	Impact Probability Matrix	44
6	Commitment Chart	55

ACKNOWLEDGEMENTS

I wish to acknowledge and thank all those who have helped me with this project. This includes the Command College academic staff, the NGT panel members: Dr. Kall Loper, Vickie Wright, Robert Morgester, Mike Menz, Mark Menz, Bruce Boles, Dave Spisak, Jeff Ritschard, Glen Sylvester, Carole Adell, Lon Ramian, and Hong D. Li; Sacramento County Sheriff's Captain Jan Hoganson from the Sacramento Valley High-Tech Task Force, my friend and class mentor Captain George Anderson, and a special thanks to Captain Merle Switzer whose help as a facilitator during the Nominal Group Technique was invaluable.

CHAPTER I

ISSUE IDENTIFICATION

Introduction

Revolutionary innovation is occurring in all scientific and technological fields. Just as the industrial revolution brought tremendous growth and opportunity two centuries ago, so too has the information age. This wave of unprecedented change is driven primarily by advances in information technology, but is much larger in scope. Our companies, institutions, government, education and private lives are enabled and dominated as never before by the now ubiquitous computer, Internet and high technology developments.¹ The rapid proliferation of computer systems, telecommunication networks, and other related technologies have created complex and far-reaching interdependencies of critical infrastructures as well as widespread vulnerabilities. While the information age holds great promise, it falls in part upon law enforcement to ensure users do not become victims of New Age crime.

The advent and popularity of the computer and its interconnectivity brought about by the Internet has given birth to a whole new species of white-collar criminals. The computer world and the boundless Internet with its anonymity and ever-changing technology is a great playground for a variety of criminals. They are the outlaws of the electronic frontier, known by aliases such as Phiber Optik and Acid Phreak.² Roaming at will in the most sophisticated computer systems in the world, they plunder confidential information and help themselves to phone service and credit card numbers—simply because they know how to do it. There is ample evidence that criminals are using computers to commit crimes of all types from financial frauds, credit card scams,

prostitution and organized crime to child pornography, pedophilia and all sorts of terrorism.

Investigation and prosecution problems are complicated and numerous. Few officers are adept in investigating computer crime, and few prosecutors are adept at prosecuting computer crime. Companies rarely report computer related crimes, preferring to absorb the financial loss rather than risk the erosion of public confidence and trust. Jurisdictional boundaries and a confusing patchwork of laws make some types of behavior legal in one state and illegal in another. Extradition and prosecutions issues are often unclear. Many of the laws were written before cybercrime was a problem. Encryption is making investigations doubly hard affording criminals protection from law enforcement intrusions.

In a sixth-month period between October 1, 2000 and April 6, 2001, the FBI referred 800 Internet fraud reports to several federal law enforcement agencies, and more than 1,200 cases to local law enforcement officials. Another 40 cases stemming from some 200 complaints were referred to international authorities. According to the FBI, more than two-thirds of these complaints came from some form of alleged auction fraud. Goods that were paid for but never delivered accounted for another 22 percent of the complaints, with credit card fraud complaints comprising nearly 5 percent. The FBI's Internet Fraud Complaint Center (IFCC), which combines consumer fraud complaints with information gathered at the National White Collar Crime Center (NW3C), has received complaints from 89 different countries. Since opening in May 2000, the IFCC has referred some 10,370 complaints to nearly 40,000 law enforcement agencies.³

High technology crime is having a profound impact on law enforcement, particularly in California. In recent years, California has emerged as the largest center of software piracy and counterfeiting, with the escalation of high technology and other computer related crimes not far behind. California has losses estimated at \$6,564 million in industry, \$358 million in tax revenue, \$923 million in high-tech wages, and 19,141 lost high-tech industrial jobs. High technology is accountable for more than half of the state's overall exports sales and employs more workers than any other manufacturing sector in the state.⁴ The statistics and losses for California are staggering, and law enforcement agencies must be able to detect, investigate and prosecute individuals who commit electronic crimes.

In 1998, Senate Bill 1734 was signed into law to address the proliferation of high technology crimes in the State of California. With the adoption of this legislation, it was speculated that California would quickly assume the leadership over other states in confronting high technology crimes. While there has been considerable accomplishment toward this end, general concern remains high regarding unmet needs to victims, training and resources available to law enforcement, public awareness, and the overall responsiveness of the judicial system. A 1998 study on cybercrime by the National Institute of Justice reported, "there is a near-term window of opportunity for law enforcement to gain a foothold in containing electronic crimes, which outpace most agency investigative resources."⁵ Law enforcement must strike quickly and seize the opportunity.

Computer evidence, by its nature, is extremely fragile and is easily modified. This situation is complicated by the fact that potential evidence exists in places that

many law enforcement officers are unaware of. To make matters worse computers can be easily rigged by the crooks to destroy evidence. Some have referred to personal computers as a law enforcement nightmare and a crook's dream. Because of its fragile nature, the first and most important step in dealing with computer evidence involves the preservation of the electronic crime scene. Once electronic evidence has been destroyed or altered, it is highly unlikely that it can be reconstructed.⁶

Law enforcement officers in every jurisdiction are confronted daily with new investigative and evidentiary issues that demand a high level of technical knowledge and skill. The pace of change is relentless. Computer technology now overtakes itself with a new generation roughly every three years.⁷ Most state and local law enforcement agencies lack adequate training, equipment, and staff to combat electronic crimes. Like investigators, prosecutors are scrambling to effectively present cases in this rapidly changing technical world, while judges are confronted with the novel legal questions it presents. Meanwhile, increasingly sophisticated and computer-literate criminals employ new technologies virtually as soon as they appear. And as computer crimes become ever more audacious—and those who commit them ever more sophisticated—law enforcement must somehow keep up.⁸

Issue Statement

The above monograph sets the stage for the issue statement of this paper: “How will California law enforcement respond to the need for computer-based expertise in the identification, collection and preservation of electronic evidence by the year 2006?”

Local law enforcement officers know how to handle a domestic violence call. They know what to do when someone breaks into a home. But many do not know what

to do if a purchase is made over the Internet that never arrives and the money sent disappears. More importantly, there is a significant training void for officers responding to a crime scene where a computer is present. It is not just the issue of computer crimes, but any crime where a computer may contain electronic evidence of a crime. Often the suspect is in a different state, but the case is not significant enough to interest state or federal law enforcement agencies. Most officers with the expertise to investigate cybercrime work for state or federal agencies, large police departments, or a multi-jurisdictional task force. Officers in smaller departments often struggle to deal with a wide range of cybercrimes and training opportunities are limited. Speaking at the recent Info-security Europe conference, Peter Sommer, a lawyer specializing in Internet law, said the police do not have enough resources to tackle Internet crimes, with little prospect for the future.⁹ Law enforcement is not keeping up with the demand for trained personnel in high-technology crimes and the field of computer forensics.

Conducting searches in an electronic environment is a relatively new challenge to law enforcement, which requires a departure from traditional investigative approaches and methods. While basic principles of crime scene searches do not change in the electronic environment, new skills and thought processes must be utilized. Because technology changes so rapidly, the storage devices for electronic evidence may not be apparent to the average officer without on-going training. Another concern is the limited number of trained investigators in the field of computer forensics. A recent article published in the San Francisco Chronicle entitled, "Career Search," focused on the tremendous need for forensic computer technicians.¹⁰

Research Methodology

This project is futures oriented and therefore differs from descriptive and relational research methodologies commonly used in criminal justice studies.¹¹ Unlike descriptive research where inferences are drawn from information on a particular issue, or relational research that examines the interrelationships between variables, futures research is concerned with the effects of social, technological, economic, environmental and political trends on alternative futures ten to twenty years from now. It is based on the premise that undesirable and desirable futures can be avoided or created by intelligently made choices. The three principle goals of futures research are:

1. Form perceptions about the future
2. Study possible alternative futures
3. Make choices to influence desirable futures

To assist in achieving these goals, several methodologies were used to study the future to include environmental scan, literature review and a Nominal Group Technique.

Environmental Scan

Environmental scan involves the systemic collection of information about external circumstances and conditions associated with the issue statement to detect the development of relevant social, technological, economic, environmental and political trends likely to impact on the future of a particular issue. Such information may come from the Internet, newspapers, magazines, professional journals, television and radio as well as other sources. Environmental scan as a process should be continual, so that appropriate information about what is happening or about to happen in the various

environments is always available. Learning to collect relevant information, but also to organize, interpret and use this information is critical to the strategic planning process.

An environmental scan was conducted by reviewing newspapers and magazines, periodicals, books, and information provide by Command College instructors. A scan of the various environments through a number of mediums revealed numerous observations of trends that are currently or will in the future have a significant impact on the issue statement. Some of the more significant developments are listed below:

- The volume and types of high-tech crime continue to increase rapidly, particularly on the Internet
- Identity theft and fraud increases parallel increases of online e-commerce
- The availability of wireless technology for electronic commerce transactions will be exploited by high-tech criminals
- Criminals are becoming more sophisticated and knowledgeable about high-tech crimes
- Technological advances in preventing high-tech crime is often thwarted by changes in criminal modus operandi
- Law enforcement is 4-5 years behind the criminals in computer-based expertise
- Law enforcement and private sector partnerships are essential to controlling high-tech crimes
- The use of encryption by criminals is becoming more problematic for investigators to legally obtain electronic evidence

- High-tech crime investigators and computer forensic specialists are in short supply
- The frequency of terrorist threats made over the Internet is on the increase, particularly threats to commit school violence

There are three major themes that emerge from scanning the various environments for trends impacting the issue statement. First, high technology crime is on the rise and is proportionate to the rapid increase and change in technology. The use of the Internet to commit fraud, identity theft, auctions and information theft leads the way in high-tech crimes. Secondly, law enforcement is having a difficult time coping with the volume and complexity of high technology crimes. The criminals appear to have the upper hand. They are more sophisticated and knowledgeable about technology and use that knowledge to elude law enforcement. Finally, by all indications, law enforcement is ill prepared for the tremendous increase in cybercrime. There is a critical shortage of trained forensic specialists, high-tech investigators, as well as a lack of computer-based knowledge by field officers and supervisors. Additionally, High Technology Crime Investigation Association (HTCIA) investigators believe they lack training, resources and management support to adequately address high technology crime.¹²

Literature Review

Most of the books written on cyber and computer-related crimes were published in the last ten years. The authors, although knowledgeable, are primarily from academic backgrounds and lack investigative experience. Many of the books on cybercrime are theoretical and offer little practicality for investigators. Because of the

rapid change in technology, some of the books are not current on the latest technology and modus operandi issues regarding cybercrime. One of the most informative and technically useful books was Eoghan Casey's, Digital Evidence and Computer Crime, which was written for computer security professionals, law enforcement officers, attorneys and forensic scientists, or anyone who wants to become more familiar with the technical, legal, evidentiary and behavioral aspects of investigating computer-related crimes. Two other recommended books are Neil Barrett's, Digital Crime: Policing the Cybernation, and Dr. Gerald L. Kovacich and William C. Boni's, High-Technology Crime Investigators Handbook: Working in the Global Information Environment. Well-known author, Peter N. Grabosky, will soon be releasing a new book entitled, Electronic Theft: Unlawful Acquisition in Cyberspace. According to critics, and based on Grabosky's excellent reputation as a writer, this should also be a good resource for cybercrime investigators.

Because the field is changing so rapidly, the most current information on cybercrime is found in magazine and newspaper articles, professional journals, reports by government agencies, and newsletters from organizations such as, The High Technology Crime Information Association (HTCIA) and Computer Institute of Security (CIS). As a research tool, the Internet was extremely valuable for locating the latest information on cybercrime.

Interviews

Captain Jan Hoganson

Captain Jan Hoganson is in charge of the Sacramento Valley High-Tech Task Force located in Sacramento, California. This multi-jurisdictional task force serves nine

counties, and comprises investigators from nine police and eight sheriffs' departments, Sacramento County Probation, six state agencies, and representatives from three district attorney's offices. Established in December 1995, the Sacramento Valley High-Tech Task Force was the first in the state and serves as a model for similar task forces throughout the state and the nation. Days prior to my interview with Captain Hoganson, Governor Gray Davis visited the Sacramento Valley High-Tech Task Force for a briefing on cybercrime and to announce the award of grant funding through California's Office of Criminal Justice Planning (OCJP).

Captain Hoganson was comfortable, but not overly confident, that the five regional high-tech task forces in California were making significant progress in the fight against high technology crime. However, he was concerned that some law enforcement agencies in California were doing little, if anything, in the way of controlling cybercrime. There is a critical need for a sixth high-tech task force in the Fresno area, which is currently in the early planning stage. According to Captain Hoganson, one of the greatest challenges of starting a multi-jurisdictional task force is identifying which agency is in charge. Often there are disagreements and power-struggles over which jurisdiction will serve as the lead agency—in other cases, no one wants to accept leadership responsibility.

Captain Hoganson commented that California is recognized nationwide as a leader in the field of high technology criminal investigation. Other states and even some nations have sent visitors to the state's five high-tech task forces to learn how to train and task organize against cyber criminals. The cyber criminals are aware of our success, which is evident by a recent out-of-state advertisement for cable de-

scramblers on Yahoo stating, “We don’t ship to Sacramento.” Even with California’s success, there is still a critical need for forensic specialists and high-tech crime investigators, as well as on-going training for first responders. Officer awareness and computer-based expertise at crime scenes is crucial to the initial investigation and preservation of electronic evidence.

As mentioned earlier, the resale of stolen cable boxes, which have been re-configured, is big business. Captain Hoganson said cyber criminals across the nation are making billions of dollars off illegal cable converters. It is really quite simple—enterprising entrepreneurs steal, buy, or acquire boxes owned by various cable networks. Depending on the type of box, they either replace the programming chip so it de-scrambles or bypasses the networks’ signals, or they merely configure it to turn on all channels. The cable boxes are then sold for anywhere between \$150 and \$450 each. The same is occurring with Dish Satellite Subscribers (DSS). Thus far, these entrepreneurs have only been able to convert analog signals. If they figure out how to de-scramble digital signals, it will be catastrophic in comparison to analog de-scramblers.

One thing is certain, high-tech crime is an ever-changing, rapidly evolving field where the criminals never run out of ideas and are just a step ahead of Sacramento’s High-Task Force.

Dr. Kall Loper

Dr. Kall Loper is a professor at CSU Sacramento in the Criminal Justice Department. As a leading expert in the field of high technology crimes, Dr. Loper teaches several courses related to digital evidence and computer crimes.

Dr. Loper expressed concern that law enforcement expertise in high-tech crimes is lagging two to three years behind the cyber criminals and does not see how they can catch up given the rapid change in technology and proliferation of computers. The world of computers is an ever-increasing technical field requiring specialized training. Computers are associated with nearly every crime imaginable. Digital evidence can be found in e-mails, electronic journals and personal diaries. The inability to identify, collect and preserve digital evidence is critical to any crime involving a computer.

The whole issue of cybercrime is underreported in Dr. Loper's opinion. The exact extent of cybercrime is unknown. Businesses in the private sector are often hesitant to report network intrusions for fear it will damage public trust and confidence, which ultimately impacts financial profits. By all indications, however, the volume and types of cybercrime are expanding dramatically.

Dr. Loper shared the concern over the apparent lack of computer-based expertise by the first responders to a crime scene. Patrol officers who are first on the scene of the crime must have a basic knowledge of computers and electronic evidence. Dr. Loper suggested, that at a minimum, first responders must have enough training to conduct a computer triage of sorts in order to determine the nexus of the crime to the computer and what level of expertise is required to collect the electronic evidence. For example, the responding officer could handle a stalker case where the suspect keeps a diary on his computer. However, a computer crime involving greater sophistication such as a network intrusion would be bumped up to a detective or forensic specialist. In

other words, law enforcement managers need to develop policy and procedures that identify various threshold levels for investigating computer crimes.

Dr. Loper believes additional computer-based training is required in the basic police academy followed by regular high-tech crime updates and computer refresher training to keep first responders current.

Summary

This chapter provided a review of the overwhelming problems associated with high technology crimes, which set the stage for the issue statement: “How will California law enforcement respond to the need for computer-based expertise in the identification, collection and preservation of electronic evidence by the year 2006?”

Three major themes emerged from scanning the various environments for trends impacting the issue statement. First, high technology crime is on the rise and is proportionate to the rapid increase and change in technology. Secondly, law enforcement is having a difficult time coping with the volume and complexity of high technology crimes. The criminals appear to have the upper hand. Finally, law enforcement appears ill prepared for the tremendous increase in cybercrime. The chapter concluded with a review of the literature and several interviews with professionals in the field of cybercrime.

The following chapter will discuss futures study and the application of the Nominal Group Technique (NGT) to identify future trends and events. The information will be used to develop three possible future scenarios.

CHAPTER II

FUTURES STUDY

Introduction

Futures studies and related research about the future constitute a discipline concerned with laying a foundation of knowledge for improved decision-making about alternative futures.¹³ This chapter will focus on interactive group decision-making and a variety of methods for analyzing likely futures such as trend and event analysis, cross-impact analysis and scenario development. Evidence indicates that groups tend to make better decisions and provide a greater number of alternative solutions than individuals. The accurate identification and evaluation of emerging trends and events is a critical component to any strategic planning process. In order to make the best possible decisions in the development of a model strategic plan, as well as to identify and measure the impact of future trends and events on the issue statement, the Nominal Group Technique process was used.

Nominal Group Technique

The Nominal Group Technique (NGT) is a process for a small group of people to achieve agreement on the answer to a single issue by using alternating private thought and open discussion of ideas. Its purpose is to eliminate social and psychological dynamics of group behavior, which tend to inhibit individual creativity and participation in group interaction and decision-making. During the process the group avoids the normal problems of a few individuals doing all the talking, the rest listening, and very few group members taking the time to actually think about the issue at hand. Studies show that

group members tend to be more creative when everyone is given a structured opportunity to participate.

Twelve panel members were selected comprised of working professionals from the Sacramento County Sheriff's Department, San Francisco Police Department, California State University Sacramento, California Commission on Peace Officer Standards and Training (POST), Sacramento County District Attorney's Office, State of California Attorney General's Office, Intel Corporation, Hewlett Packard, Sacramento Search Group and the Renaissance Consulting Group. All but one of the selected members, the representative from CSUS, participated in the NGT process. The panelists represented a cross-section of law enforcement, educators and the high technology industry. The names and a brief biographical summary of each panel member are provided at Appendix A.

Trends

Trends are a series of indicators or events taking place over time that tend to indicate a direction in which a particular issue may be heading. They are based on the past, present and future, and can be quantitative or qualitative. For the purposes of this paper, each panel member was asked to identify trends they felt are occurring that will have an impact, positive or negative, on the future of the issue statement. Examples of trends could be the rising or lowering of costs for hardware and software; physical size of the hardware; accuracy of the end product or issues associated with security. Trends should be simple observations. They do not need to be complex and should be specific. The trend of security, for example, is a very general trend that can be broken

down to many sub-issues such as: log-on security, hacker security, database storage security, etc.

Approximately one month before the NGT panel convened each participant was furnished with information identifying the issue statement, a brief overview of the NGT process as well as a definition of trends and events. The panel met for one day on April 5, 2001, at the Sheriff's East Station in Rancho Cordova, California. After reviewing the purpose and process of the NGT, clarifying the issue statement, and presenting some background information, the panel was asked to identify emerging trends they felt would have an impact on the issue of computer-based expertise in law enforcement. The panel identified forty-two trends listed in Appendix B from which they ranked the following eight trends in order of priority as to their potential impact on the issue statement:

Table One
Trend Summary

Trends	-5 Years (1996)	Today (2001)	+5 Years (2006)	+10 Years (2011)	Concern (1-10)
1 Availability of training	100	100	200	200	9.0
2 Authentication	80	100	145	180	9.0
3 Volume cybercrime	95	100	173	177	8.0
4 Organized response	50	100	140	150	7.5
5 Use of technology	100	100	150	165	7.6
6 Legal constraints	97	100	153	150	8.0
7 Privacy concerns	42	100	155	184	9.0
8 Jurisdictional issues	60	100	137	186	6.8

The following summarizes the panel members' discussions of the eight trends:

Trend 1: Availability of relative training

The need for computer-based expertise was considered by the panel to be the most significant trend for California law enforcement in the future. They were particularly concerned that law enforcement is not keeping pace with the demand for trained investigators in the field of computer forensics. The turn-around time for computer examinations for forensic laboratories throughout the state is on the increase. Of equal concern is the inability of most patrol officers, and many detectives, to identify and properly recover electronic evidence at a crime scene. As Detective Mike Menz with the Sheriff's High-Tech Task Force pointed out, it is not just computer crimes we are concerned about, but any crime where the suspect has access to a computer, which may contain evidence of the crime. The first responder to the scene of a crime must have a basic understanding of electronic evidence.

Trend 2: Authentication capabilities

There was considerable conversation about authentication of information through digital signatures and access security using biometric systems. A digital signature provides a means of verifying the authenticity of a particular piece of data or information. Although costly to implement and not without flaws, biometric systems appear to be the most promising for controlling unauthorized computer access. Biometric devices are those which look at some physical trait of a potential user and compare it to traits previously recorded, such as fingerprints, voice patterns or geometry of the hand.

A few panel members were optimistic that authentication problems would be resolved through technology in the next ten years. However, others were skeptical that efforts to break Data Encryption Standards (DES) and privacy issues would offset advances in security technology. There was a consensus that knowledge-based controls such as password protection and possession-based controls like magnetic cards would need to be replaced with more sophisticated security measures in the future.

Trend 3: Volume of cybercrime

Panel members, especially from the private sector, voiced real concern about the future direction of cybercrime. One panelist said that when he started his career in high technology, on-line crime was almost nonexistent. In those days the major concern was component theft, now 80% of computer crime is on-line. The panelists fear the rapid growth in technology and e-commerce will only exacerbate the volume and complexity of cybercrime. Some panel members felt we do not have accurate computer crime statistics because of the irregularities in reporting to law enforcement. Some companies are reluctant to report cybercrime to authorities for fear it may adversely impact their business. However, by all indications, cybercrime is on the rise and shows no signs of slowing in the next five to ten years.

Trend 4: Organizational response capacity

The panel members agreed that twenty-first century law enforcement faces numerous problems in regard to cybercrime on the Internet, including jurisdictional and forensic issues. These are both national and international problems requiring an organizational strategy that is tied to the global law enforcement community. Equally

important is the need to build a two-way street for the flow of information and incident data between government and the private sector. Some panel members fear that government's inability to change quickly will be a major stumbling block to keeping pace with technology. Private security has come to the aid of business because law enforcement has been slow to react. There is a tremendous need for organizational leadership in the development of a strategic plan for addressing the major issues of cybercrime. The challenge of international cooperation and coordination of investigations, coupled with diverse, overlapping and sometimes contradictory computer crime laws, regulations and criminal procedures make enforcement of criminal statutes even more difficult—especially when computer crime transcends national borders.

Trend 5: Use of technology

Most panel members were confident that the use technology would continue to grow at a rapid pace. Technological advances will drastically change the way we live and do business. Miniaturization will continue, as well as mobility, flexibility, integration, lower costs, and increased communications, and information collection—all with untold possibilities. Availability and quality of encryption, Internet server providers via satellite and increased infrastructure dependent on technology will be the wave of the future. Access to information has improved tremendously over the past few years, and will continue to do so in the future. Following the path of technology growth, high-tech offenses like Internet fraud, e-mail abuse, computer hacking and virus spreading look set to increase during the next ten years. The panel members believe technological advances will make e-crimes easier to commit and conceal.

Trend 6: Legal Constraints

Panel members from law enforcement were deeply concerned about legal constraints and ambiguity in our current laws. While computer crime has grown relative to the spread of technology, crafting laws that do not infringe on user's rights or stymie law enforcement efforts has been problematic. While the panel supported strong encryption, they were concerned that the widespread dissemination of unbreakable encryption without any accommodation for law enforcement access is a serious threat to public safety and to the integrity of our commercial infrastructure.

Laws need to be technological neutral so they can be applied whether the crime was committed with a pen and paper or e-mail. Under current law, for example, federal officials are unable to prosecute juveniles for computer violations, although juveniles commit many cybercrimes.

Drafting appropriate legislation was viewed as a significant obstacle to effectively addressing cybercrime. International cyber criminals are exploiting the lack of compatibility of international law. A review of criminal laws for consistency of crimes committed in cyber v. real world at the local, state, federal, and international level was deemed crucial. Everyone realizes that we are at a point that business is in transition, technology is in transition and there is a legal transition as well. However, the reality is the legal clock is a lot slower than the business or technology clock.

Trend 7: Concern about privacy rights

This is one of highest priorities for some panel members. With certain e-mail programs, composers of e-mail messages can now get copies of replies and forwarded messages secretly bounced back to them. This devious trick has earned the nickname

e-mail wiretapping, and like most hacker like-activities, it is quickly gaining prevalence. Law enforcement panel members were concerned about constitution restrictions on privacy, which do not apply to the cyber criminals. Some members pointed out that cyber criminals know that a corporation's information about its customers, as well as a company's intellectual capital, can be sold on the open market. Customer data can be used to misappropriate funds, and intellectual capital can be auctioned to the highest bidder.

The panel members recognized the delicate balance between individual privacy rights and the government's need to access personal data. Privacy issues will continue to be a major concern for the individual citizen, law enforcement and businesses.

Trend 8: Jurisdictional issues

One of the biggest problems with the application of traditional criminal law concepts to cyberspace is the difficulty of establishing jurisdiction and venue. Most crimes occur either where the defendant puts in place the actions which cause the prohibited effects or where the victim of the offense is located. Defamatory, malicious or pornographic messages posted on the Internet are accessible globally. Thus, by using the Internet, a user may unintentionally find themselves subject to all nations' jurisdiction. Users of the Internet must be aware of the laws and procedures in every jurisdiction—domestically and internationally.

Legal jurisdiction over cybercrimes in a global economy is an extremely complex problem. Five years ago it was not a problem. According to our panelist from the district attorney's office, jurisdictional matters were resolved on a case-by-case

basis. However, the sheer volume of cases today makes the practice unmanageable. Ten years from now, everyone will be able to do business anywhere in the world.

Some panel members fear the Federal Bureau of Investigation (FBI) would eventually assume responsibility for investigating all cybercrimes. However, the FBI does not have the personnel or funding to take over completely and will have to rely on assistance from state and local law enforcement. Most of the panel members felt the U.S. would have to form partnerships with the international community to address the jurisdictional issue.

The panel members were given worksheets with instructions on how to rate the status of each trend at a given time and the level of concern they have for each trend regarding its impact on the future. Following a discussion of the ratings and clarification of inconsistencies, the ratings were recorded on the worksheets. The average of the panelists' ratings for each event are shown on the Trend Summary Table.

The today column indicates the status of a trend at present day 2001. The value of 100 is an arbitrary value that indicates the status of the trend at the present time. The panel members were asked to make an educated guess on where a trend has been and where it will be in the future by rating each of the trends five years in the past and five and ten years into the future. They were also asked to give a rating of 1 to 10 for their degree of concern they had regarding a particular trend and its potential impact on the issue statement. A 10 signifies a great deal of concern about a trend while a value of 1 indicates little concern. The purpose of the rating is to identify those trends that could have a significant impact on the issue statement. The value of identifying trends that we are concerned with the most can help us focus our efforts on either

promoting the continuance of a trend or attempting to thwart the advance of a trend if it is in our power to do so.

The Trend Analysis Table indicates a relatively high degree of concern for each of the eight trends, with the greatest concern for training, authentication and privacy. The trend summary indicates a gradual and steady increase of all eight trends over the next ten years. Such increases could be considered either positive or negative depending on one's point of view and how law enforcement responds to each trend. With the exception of trend one, the panelists felt that law enforcement will have some significant challenges to control and direct these important trends in order to shape their future.

Events

The panel next identified a number of events they believed could occur over the next ten years, which could have a significant impact on the issue statement. Events are different from trends in that they are singular occurrences that occur at a specific date and time. For example, an earthquake or windstorm on a certain date is an event. The passage of a new law that would mandate a certain action is an event. The panel was asked to identify those events which could have a significant impact, positive or negative, on the issue statement. Each of the events was discussed as to their relative impact on the issue statement. Of the thirty-four events listed in Appendix C, the panel members identified and prioritized in order of importance eight events in Table Two.

Again, the panel members were given worksheets with instructions on how to rate the probability of each event occurring in the future and the level of impact of each event on the issue statement. Following a discussion of the ratings and clarification of

inconsistencies, the ratings were recorded on the worksheets. An average of the panelists' ratings for each event were entered below on the Event Summary Table.

Table Two
Event Summary

Events	Year(s)>0	+5 Years	+10 Years	+/- Impact	1 – 10
1 Financial attack	1.8	77	90	-	4.8
2 Switch to wireless	3.4	70	93	+	7.4
3 Power outage	4.3	78	95	-	8.9
4 Jurisdiction issues	4.3	86	88	+	7.6
5 Forensic 72 hrs	4.2	94	100	-	7.4
6 Encryption keys	6.9	0	64	-	3.6
7 Local control	4.7	41	61	-	2.2
8 Mandated training	5.0	46	66	+	3.0

The following summarizes the panel members' discussions on the eight events:

Event 1: Cyber attack on major financial institution

There was a consensus among panel members that in the next five years there is a high probability of a terrorist attack via the Internet on a major financial institution, U.S. power grids or some other critical electronic infrastructure of the United States. They likened the cyber attack to our generation's equivalence of the atomic bomb. The widespread use of computers and the Internet has created the possibility for an individual to cause drastic harm to public health and safety by damaging or shutting down computers. With forty percent of the world's computers, the U.S. is a prime target for such an attack.

Event 2: Wireless replaces wire

Not everyone on the panel understood the ramifications of going wireless. After clarification by some of our expert panelists, it was clear that wireless technology would require added security measures through a network of new protocols. As the airwaves get increasingly more crowded with wireless transmissions of voice and data, the field is becoming more complicated in a world of mixed network protocols. Unlike the Internet, which uses only a handful of standard protocols, the wireless world is built on many disparate protocols that do not necessarily work together at all. The panel members felt that if security could be assured, then wireless broadband and other forms of wireless networking show great promise as an alternative to wired services.

Event 3: Major power outage

California, as well as other states, is experiencing power shortages resulting in what has become known as rolling blackouts. The increased demand for electrical power and a shortage of generation facilities could result in a serious problem for California. With the hot summer months ahead, and the increased demand for electricity, the problem could result in a major power outage. The panel members felt that California's power shortages would not improve for at least five years, which is the time it will take to build some new power plants. In addition, some panel members felt the state's power grid system could be the target of cyber terrorism, which would only exacerbate the current situation. In either case the loss of power for an extended period of time could adversely impact the state's electronic infrastructure.

Event 4: Jurisdictional resolution

As stated earlier, one of the biggest problems with the application of traditional criminal law concepts to cyberspace is the difficulty of establishing jurisdiction and venue. The laws defining computer offenses and the legal tools needed to properly investigate such crimes have lagged behind technological and social changes. For example, there is no legal mechanism to enforce a state subpoena in another state at the present time. In the case of many computer crimes, it is not always obvious which of several authorities should be investigating the offense—and even if it can be determined as a police matter, it is not always obvious which law enforcement agency has responsibility. If the state or federal attorney general could resolve the jurisdictional issues, it would be a major step forward in the fight against cybercrime.

Event 5: Forensic in 72 hours

Several panel members felt a 72-hour judicial limitation on the length of time for computer examinations would be a devastating blow to law enforcement given the current status of our forensic laboratories and technicians. According to a panel member from the High-tech Task Force in Sacramento, they are running 160 computers behind with a turnaround time of 90 to 120 days. He also cited a case they are working on that is more than twelve years old. Some do not want government to force them to give up information, but understand why they need it for criminal investigations.

Event 6: Courts cannot compel release of encryption

Supreme Court rules that law enforcement cannot compel a suspect to provide encryption. This decision would mark the first time in history the U.S. Government could not produce evidence by brute force. Evidence cannot be obtained, reviewed, accessed by its sheer nature. For example, in a child-molestation case, investigators

have probable cause to believe the suspect has evidence of the crime in his computer, however, it's encrypted and the investigators cannot break the encryption. So far the courts have not compelled suspects to surrender the encryption key. Some panel members felt every cyber criminal will be encrypting whether or not they want to, just in case the police seize their computer in a criminal matter.

Event 7: Local control of cybercrime

The issue of investigative leadership surfaced on several occasions during the NGT process. The fact that no single government agency is taking the lead in the fight against cybercrime stimulated considerable discussion on who should be responsible. What if the FBI handed all cybercrimes over to the local and state law enforcement agencies? Some panel members felt this would not work because of the global nature of cybercrime. The international community could demand a concerted response worldwide. Some panel members believe it is more efficient to treat cybercrime as any other crime and handle it at the local level. They felt the FBI is too large, change-resistant, and inefficient for the job. They see local law enforcement as more agile and having greater resources. Another problem with the FBI is the agency's reluctance to share investigative information with allied agencies. The panel was divided on whether local control would resolve jurisdictional issues or complicate the problem.

Event 8: POST mandated training for Peace Officers

Panel members were adamant that law enforcement and forensic technicians need specific levels of training and certification to carry out their respective duties when investigating cybercrime, collecting electronic evidence and testifying in court. By having the training mandated by the Commission on Peace Officer Standards and

Training (POST) for all California law enforcement agencies, it would standardize training to better reflect state and local priorities. Like most new programs, the POST mandated cyber training would take time to develop and implement. However, once implemented at the user level it will benefit law enforcement agencies throughout California.

The first column designated yr>0 is an estimate of when the event in question could first occur. The second and third columns designated +5 yrs and +10 yrs indicates the probability of an event occurring within the next five years and ten years respectively. These values are recorded as a percentage. The last column designated Impact -10 to +10 indicates the level of impact that an event would have on the issue statement and whether the impact is considered positive or negative. A rating of 10 would indicate a significant impact while a 1 or 0 would indicate a lesser or no impact. There is no science to these estimates and no right or wrong answers. Each of the panel members was asked to make their own estimate based upon their personal knowledge and experience.

Like the trends, the purpose of the rating is to identify those events that could have a significant impact on the issue statement. The value of identifying events that are of the most concern can help focus efforts on either preparing for such an event or attempting to avoid the event if there is the power to do so. The Table indicates events 1 through 5 have a very high probability of occurring over the next ten years. It also indicates the same five events will have a significant impact on the issue statement, 2 positive and 3 negative. The panelists were optimistic that law enforcement could do

much to prepare for the events having a negative impact with the exception of event 3, major power outage.

Cross Impact Analysis

Cross-impact analysis is a more comprehensive approach to the analysis of the future than a mere examination of possible alternative developments. It is based on the idea that significant interrelationships exist among our various future projections. For example, a future plan based on the widespread use of solar energy would necessarily affect the importation and pricing of oil, which in turn would affect our economic future. In its more technical applications, cross-impact analysis may employ quadratic equations to probe possible interrelationships among trends and events likely to take place in the future.¹⁴

Since trends and events do not necessarily occur independent of each other, and could have potential impacts on each other, it is helpful to conduct a cross impact analysis to determine their interrelationship to one another. The following chart was developed using a scale a of -5 to +5; -5 having the most negative impact; +5 having the most positive impact; and 0 having a neutral impact on the issue statement. The rows denote the events and the columns denote the trends. The table shows the interrelationship between the events and trends when they occur together in the future and their impact on the issue.

Table Three
Cross Impact Analysis Matrix

Trends	1	2	3	4	5	6	7	8
Events								
1	-1	-3	-4	+3	+3	-2	-4	-5
2	0	-3	-2	+2	+3	-3	-2	+4
3	0	-2	-3	+2	-3	0	-3	+2
4	+2	+2	+4	+4	+2	+3	+1	+5
5	-3	-1	-4	+2	-3	-2	-2	-4
6	-1	+2	-3	+3	-3	+1	-3	+3
7	-2	-3	-5	+2	-4	-3	-2	-5
8	-4	+1	-3	+3	-3	+1	-2	+2

The Cross Impact Analysis Matrix indicates a significant impact on trends 3 and 8 whenever most of the eight events occur. Additionally, Event 4 (Jurisdictional resolution) appears to have the most positive impact of the eight events when it occurs with the eight trends. Because trends 3 and 8 registered a significant degree of concern on behalf of the panelists, as did the level of impact of most of the eight events, their interrelationship on one another is not always clear. However, it is safe to conclude that when a high-concern trend occurs with significant-impact event the overall impact on the issue statement is statistically more significant. The table indicates that when certain trends and events occur together the problems are magnified. As a planning

tool, the cross impact analysis can help law enforcement identify and plan for the simultaneous occurrence of trends and events, or prevent such occurrences if possible.

Alternative Scenarios

The purpose of developing scenarios as a planning tool is to identify large-scale forces that impact and affect the future in different ways. It's about making these forces visible, so that if they happen, the planners will at least recognize them. Scenarios or story telling enables managers to make better decisions today based on future assumptions. In a sense, the scenario is a tool that helps us study not only the possibilities of the future, but also our subjective involvement with those possibilities.¹⁵

There are a variety of scenario types; however, this report will focus on three types: optimistic, pessimistic and surprise free. The optimistic scenario predicts a desirable future based on the positive impact of certain trends and events on the issue statement. Optimistic scenarios predict futures that should be exploited. Conversely, a pessimistic scenario depicts an undesirable future based on the negative impact of certain trends and events on the issue statement. Pessimistic scenarios predict futures that should be prevented or avoided. Finally, surprise free scenarios predict futures based on a neutral impact of certain trends and events on the issue statement:

Based on what has been learned from the research, interviews and the analysis of trends and events identified by the NGT panel, the following three scenarios were developed as probable futures on the issue statement.

Optimistic Scenario

By the year 2006, cybercrime cannot be controlled by current law enforcement methods. Advanced technology has created a whole new breed of cyberspace

offenders. However, all is not lost. People continue to see and talk to one another on computers, and as nanotechnology made computers even more portable the new emerging technology continues to protect the information highway. The spin cycle of simplifying systems to make them more universally acceptable and accessible also makes them more vulnerable to intruders. Control of access by optical patterns, DNA identification, voice spectrographs, encryption and other methods slow down hackers and assist law enforcement in the prevention of cybercrimes. The demand for advanced technology parallels the demand for data security and computer access protection.

Communications and networking helps prevent cyberpunks from hacking into computer systems. Due to public pressure, many of the Fortune 500 Companies can no longer pass computer fraud losses onto the consumer. They now have to face the problems of cybercrimes through technology, law enforcement and information sharing. The judicial system established alternative sentencing programs for convicted hackers. Hackers now can choose to work for private and government agencies to help prevent cybercrimes in lieu of going to jail or prison. Many of these hackers have now become fulltime employees as computer fraud specialists. The cooperation of hackers with law enforcement and corporations will continue to play an ever-increasing role in protecting the information highway.

The Turley Police Department was able to startup a high-tech crimes unit with the assistance of the Office of Criminal Justice Planning (OCJP). The Sanger Police Department assigned an investigator to work with the Turley Police Department's new high-tech crimes unit. The department recently created a trilateral agreement with

Hewlett Packard and the Intel Corporation to share information and technology in the fight against cybercrimes. The private sector has provided the police department an alternative source of funding and resources. Additionally, there are plans to establish a sixth regional high-tech task force in Fresno County, which will represent twenty-two local, state, and federal agencies.

Also by the year 2006, efforts to bring crimes such as murder, rape, robbery, burglary and auto theft under control through a combination of technology and proactive community policing are in place, such as computer-controlled smart houses and cars to thwart burglars and auto thieves. There is a continued effort to create a cashless society to eliminate the monetary rewards of robbery and other cash related crimes. Implanted bodily function monitors and chemical drips such as “sober-up” drugs and synthesized hormones keep most of the sexually and physically violent offenders under control. More importantly, proactive policies seeking out crime-breeding situations and taking steps to eliminate them before the crime occurs are alleviating much of the burgeoning violence among young people. The end result by the year 2006, law enforcement will have more time and resources to concentrate on cybercrimes.

Pessimistic Scenario

The year is 2006 and a new paradigm has emerged. The world is considered a unified and peaceful global society, sophisticated and technologically advanced. Third world countries reap the benefits of lightening speed technology, elevating them to a new plateau in society. Traditional warfare is not politically correct in the New World Order (NWO). The United States, Russia, and China still hold their titles as superpowers and continue to have significant nuclear capabilities. Together they

formed a Tri-Lateral Commission to prevent global proliferation of nuclear arms. The World Court established by the United Nations during the Clinton Administration settles global conflicts and disputes between nations. But while the physical world appears at peace, the clueless society had been slumbering and a new frontier of war games blossomed in epic proportions causing global conflict, vulnerability, security breaches, and terrorism in a new world called Cyberspace.

Sophisticated networks of international thugs, thieves and criminals emerge as a real and problematic national security threat. Over the past years, Russian, Chinese, Nigerian, Middle Eastern, and Italian gangs enthusiastically embraced globalization and technology to expand their criminal domains and elude police. In an emergency, the U.S. National Security Council calls for the world's law enforcement agencies to begin treating Internet terrorism, cybercrimes and copyright violations committed by these perpetrators as crimes against the NWO. They dicker over jurisdiction in the World Court by means of reciprocity, denying sovereignty of nations, and stirring the already heated debate of civil liberties.

In retaliation, the global underworld launches an all-out attack against NWO's critical information infrastructures and declares war in the universe of Cyberspace holding the global society hostage. The 3-day attack cripples global computer networks to an almost shutdown of medical services, telecommunications, electrical power grids, banking and financial institutions and oil and gas production. Global terrorists capitalize on the confusion, bribing corporations and nations for millions of dollars in return for information security and reduction of the threat to completely destroy the electronic infrastructure.

The disruption of the global economy by this act of cyberwar triggers an economic recession in many countries. In the U.S., rioting by disenfranchised citizens in New York, California and Florida stretches law enforcement resources to the limit. California is most impacted due its large economy and advanced technology. Law enforcement in general is ill prepared to contend with such civil and criminal chaos on a national level, let alone on a global level. It takes years for NWO to fully recover from the underworld's cyber attack.

Surprise Free Scenario

By the year 2006, anyone who is computer literate can become a cyber crook. The crime itself will often be virtual in nature—sometimes recorded, more often not—occurring only in cyberspace with the only record being fleeting electronic impulses. Access to cyberspace will expand geometrically, and technology is making the information highway even more user-friendly and affordable for millions of potential cyber crooks.

The opportunities for hacking and cracking will escalate with wireless telephones, computers, faxes, and televisions interconnected to provide instantaneous communication and transmission of materials among individuals. The wide appeal of new multi-media communication systems will create such a huge volume of subscribers that the price will plummet, making access by all possible. Advances in copying technology will encourage piracy and counterfeiting of valuable items like currency and telephone cards.

Although cybercrime is increasing worldwide, and there is every reason to believe the trend will continue well into the twenty-first century, law enforcement will

expend increasingly more resources to deal with the growing problems associated with cybercrime. Increased cooperation between private industry and government helps to control electronic crime and protect the nation's critical infrastructures. Many of today's privacy, legislative and jurisdictional issues will be resolved. Local, state, federal and international law enforcement agencies will form partnerships to investigate cybercrime.

The norm will be for law enforcement to cast a wide net in order to seize every opportunity and resource available in the fight against cybercrime. An increasing number of officers will be assigned to cybercrime investigations. Instead of checking out a patrol vehicle, many officers will be working online at a desktop computer. The Turley Police Department has several trained investigators working electronic crime cases. There are still more cybercrime cases than there are investigators; however, the chief and the community seem to be satisfied with investigating only the most serious offenses.

The war on cybercrime is at a stalemate—there are no winners or losers in 2006. Although the incidents of cybercrime continue, law enforcement is capable of responding to any significant increases.

Summary

This chapter began with an introduction to the concept of futures studies and related research about laying a foundation of knowledge for improved decision-making about alternative futures. A group of professionals from the public and private sectors participated in the Nominal Group Technique to identify trends and events likely to have an impact on the issue statement. The panel members rated each trend and event regarding its impact on the future and recorded their findings in summary tables for

presentation. A Cross Impact Analysis Matrix was presented to demonstrate the interrelationships between trends and events when they occur at the same time. Based on this information, three possible scenarios for the future were developed: optimistic, pessimistic, and surprise free.

The next chapter is dedicated to the development of a strategic plan to help law enforcement meet the needs for computer-based expertise by the year 2006, based on the pessimistic scenario. The strategic plan will be designed for a mythical organization known as the Turley Police Department.

CHAPTER III

STRATEGIC PLAN

Introduction

The purpose of developing a strategic plan is to provide a framework for action to assist the Turley Police Department respond to the need for computer-based expertise by the year 2006. The Applied Strategic Planning Model is used to provide a structure for the department's planning process.¹⁶ This model is applicable to any size organization as well as multiple organizations.

Strategic planning is a structured process by which the guiding members of an organization envision its future and develop the necessary plans and procedures to achieve that future. It involves identifying organizational objectives and specifications for how they will be accomplished. The process forces decision makers to assess the environment, examine alternatives futures, and decide on appropriate courses of action. Strategic planning enables those responsible for leading change to unleash the energy of the organization behind a shared vision and a shared belief that the vision can be fulfilled.

Strategic Planning Model

There are many strategic planning models from which to choose; however, they all must address three basic questions: Where are we going, what is the environment, and how do we get there?¹⁷ The Applied Strategic Planning Model described in Leonard Goodstein, Timothy Nolan and J. William Pfeiffer's book, Applied Strategic Planning: How to Develop a Plan that Really Works, was selected for this project because of its continual focus on application and implementation throughout the entire

process. The Applied Strategic Planning Model involves the following nine sequential steps:

1. Planning to Plan

Planning to plan is not just a play on words. It clearly identifies that there are significant steps in the planning process that need to be completed if planning is to be an effective management tool. Planning to plan includes developing answers to the following questions and making necessary decisions to implement those answers prior to the initiation of any actual planning process:

- Who should be involved in the planning process?
- What is their level of commitment to the planning process?
- Who are the important stakeholders?
- What information do we need to plan successfully?
- Who will get the information we need?
- What resources do we need?

Identifying stakeholders is a crucial component in planning to plan. Some stakeholders should be involved in the development of the strategic plan, while others may be needed in strategy development discussed later in this chapter.

2. Values Audit

A values audit is an examination of various values and cultures internal and external to the organization. It is the first actual step in the planning process:

- Personal values
- Organizational values and culture
- Philosophies of operation

- Stakeholder analysis

The values audit is one of the most important and one of the most difficult steps in the Applied Strategic Planning process. It requires in-depth analysis of the most fundamental beliefs that underline organizational life and decision-making. Without the values audit, unresolved differences in assumptions, values, beliefs and philosophy will surface continually in the planning process, blocking progress and interfering with the development of a strategic plan.

3. Environmental Scan

Throughout the process planners must be aware of what is happening in five critical environments that could impact the strategic plan. The first letter of the five environments comprise the popular acronym STEEP, which stands for:

- **S**ocial
- **T**echnological
- **E**conomic
- **E**nvironmental
- **P**olitical

Brown and Weiner (1985) define environmental scanning as “a kind of radar to scan the world systematically and signal the new, the unexpected, the major, and the minor.” The social environment includes demographics, life-styles and cultural values. The technological environment concerns advances in research and the subsequent diffusion of new technologies into every aspects of our lives. The economic environment is examined for economic factors in the regional, national and global society. Environmental concerns are evaluated from an environmental perspective,

raising issues from energy conservation to population growth. The political environment includes evaluating local, regional, national and global politics. It is important to remember that STEEP environments are interrelated—changes in one may lead to changes in another.

4. SWOT Analysis

Also known as WOTS UP, the acronym SWOT stands for the organization's internal strengths and weaknesses and its external opportunities and threats. The purpose of the SWOT analysis is to identify emerging opportunities and threats in the organization's external environment. It should further identify the organization's strengths and weaknesses for meeting these opportunities and threats. These four factors must be considered for their potential positive or negative effect on the organization and its efforts to achieve a desired future:

- Strengths (internal focus)
- Weaknesses (internal focus)
- Opportunities (internal and external focus)
- Threats (external focus)

During the SWOT Analysis it may be helpful to employ a process known as Opportunity Mapping to assist in identifying those weaknesses that will produce the greatest benefit if considered in the strategic plan. Opportunity Mapping is a tool to help allocate resources based on a value-benefit analysis.¹⁸ The following matrix graphically depicts how the technique works:

Table Four
Opportunity Mapping Matrix



The vertical axis represents value and the horizontal axis represents performance. The greatest opportunity exists in Quadrant 1 where the perceived performance is low, but the value is high. Consequently, if the performance in Quadrant 1 is improved, there is greater benefit to the organization.

5. Mission Formulation

Mission formulation involves developing a clear statement of what business the organization is in and for what purpose. The mission statement should address the following questions:

- a. What function(s) does the organization perform?
- b. For whom does the organization perform this function?
- c. How does the organization go about filling this function?

d. Why does this organization exist?

Once an overall mission statement has been developed for an organization, mission statements that are more specific and concrete should be developed for separate units or divisions of the organization.

6. Goal / Objective Development

Goal and objective development involves the organization's attempt to spell out in some detail the paths by which the organization's mission is to be accomplished:

- Goals should be specific, measurable, achievable, results oriented and time specific
- Objectives provide direction, establish standards and serve as motivators

7. Performance Audit / Gap Analysis

A performance audit / gap analysis provides a clear understanding of the organization's performance shortfalls and identifies gaps between current performance and the desired performance to accomplish the mission:

- Performance Audit = Analysis of current organizational performance
- Gap Analysis = Difference between current and desire performance

8. Contingency Planning

Necessitates making assumptions about the future that may negatively impact the organization and developing alternative courses of action:

- Identifying most important opportunities and threats
- Designating trigger points to initiate alternative plans
- Determining which action steps for each trigger point
- Reaction plans to unanticipated events

The two key concepts in contingency planning are probability and impact. In other words, contingency plans involve potentially high-impact events that do not have the highest probability of occurring.¹⁹ The following matrix graphically shows how contingency planning fits into the Applied Strategic Planning process:

Table Five
Impact-Probability Matrix

Impact ↑ High ↓ Low	<u>QUADRANT 1</u> Contingency Planning	<u>QUADRANT 2</u> Applied Strategic Planning
	<u>QUADRANT 3</u> Planning not Required	<u>QUADRANT 4</u> Operational Planning
	← Low	High →
	Probability	

Applied Strategic Planning is primarily focused in Quadrant 2, while contingency planning focuses on Quadrant 1. Obviously, no serious strategic plan should focus much of its time in the other quadrants unless there are special circumstances that would justify such an investment.

9. Implementation

Involves putting the strategic plan into motion at all levels:

- Initiation of operational and tactical plans
- All stakeholders are actively involved
- Plan is integrated into everyday management decisions

- On-going monitoring and evaluation

Applied Strategic Planning provides an effective model for organizational leaders to envision a future and develop the necessary plans and procedures for organizational transformation. If applied with intelligence, commitment, and conviction, Applied Strategic Planning will enable an organization to create and achieve its ideal future.

Organizational Description

The purpose of describing the organization is to better understand the organizational structure, culture and its environment. In the context of strategic planning, this usually begins with scanning the various social, technological, economic, environmental, and political environments to determine their potential impact on the organization. Secondly, a SWOT analysis of the organization's strengths, weaknesses, opportunities and threats is necessary to determine if the organization's present organizational structure will support the strategic plan. Finally, a performance gap analysis is critical to decide whether or not the organization has the capacity to successfully implement the strategic plan. If the strategic plan cannot be implemented because of a performance deficiency, the gap between the current performance of the organization and the desired performance required for successful realization of the strategic plan must be identified.

Turley is a full service charter city located in Fresno County east of Sanger. In the past ten years Turley's 32 square miles of rich agriculture lands have given way to sprawling residential and business communities. High-tech industries like Cisco, Hewlett Packard and Intel Corporation have relocated to Turley to escape the high property costs and traffic congestion of the Bay Area. Turley is attracting a stream of

newcomers seeking affordable housing, safe schools and good paying jobs. The City's population of 84,000 is expected to reach 130,000 by the year 2006.

The Turley Police Department has 86 sworn and 16 non-sworn personnel who serve at the direction of the chief of police. The organization is divided into three divisions and several bureaus. Although the Turley Police Department has an excellent reputation in the law enforcement community as a progressive, well-trained agency, the organization has paid little or no attention to the explosion of computer related crimes impacting the community. The department does not have a high-tech unit internally nor are they a member of a regional high-tech task force.

The Turley police chief is not particularly knowledgeable about computer crime and is ambivalent to reports of skyrocketing incidents of identity theft, intellectual crimes and network intrusions by hackers. Additionally, the chief does not feel he has the resources to adequately address cybercrimes and there is no regional high-tech task force in Fresno County to assist the police department. Subsequently, the issue of high-tech crimes and computer-based training for department personnel is of little or no concern to the chief at present.

Situational Analysis

Before any detailed plan for an organization's journey into the future can be implemented, the organization must accurately determine its present location. The situational analysis provides the exact coordinates of the organization's location on the important, relevant dimensions. The United States Army's standard, "Five-Paragraph Operations Order," begins with a situational analysis of the enemy, friendly forces, and the battlefield environment. The military situational analysis is essential to the

commander's strategic battle plan.²⁰ A key focus of situational analysis involves the simultaneous study of the organization's internal strengths and weaknesses and of the external opportunities and threats (SWOT) that may positively or negatively affect the organization in its efforts to achieve a desired future. The SWOT analysis process is one of the steps in the Applied Strategic Planning Model.

The Turley Police Department is receiving an increasing number of complaints from citizens and the business community about Internet crimes. The president of the local Chamber of Commerce, speaking on behalf of the business community, complained to the city council that computer crime was having an adverse impact on local businesses. The problem came to the forefront when Mayor Cooper's wife ordered a Bissell carpet cleaner over the Internet using her credit card. When the mayor's wife received the bill 30 days later and the carpet cleaner had yet to arrive, she called the police. To make matters worse, the police department refused to respond to the scene citing they did not have the knowledge or resources to investigate Internet crimes.

Turley's police chief suddenly discovered a newfound interest in computer crimes when he came under intense scrutiny by the city council for not having trained personnel to investigate computer crimes. The City Manager gave the chief 120 days to develop a strategic plan for improving the computer-based expertise of department personnel, and to organize a high-tech crimes unit to investigate computer crimes. Currently the department lacks investigators and first responders who have adequate skills and training to detect, collect and preserve electronic evidence. The department does not offer computer training in its basic recruit academy nor as part of its yearly in-

service officer training. The above situational analysis describes the department's inability to form a high-tech crimes unit.

Strategy Development

The word strategy is derived from the Greek word *strategos*, meaning “the art of general”.²¹ Strategy addresses the where dimension of strategic planning rather than the how. Strategy determines the overall direction of the organization. It requires the chief and the planning team to think strategically in terms of where the organization should be going rather than how it will get there. Strategic plans provide the organization with a strategy for dealing with relatively uncontrollable environmental factors that affect the achievement of organizational goals and objectives. Strategy provides both logic and a first level of detail to show how a vision can be accomplished. Strategy development requires the following considerations:²²

1. Defining strategic areas that affect the direction of the organization
2. Establishing these areas in priority order
3. Determining the organizations driving force, both present and future
5. Identifying changes that must take place if a new direction is necessary
6. Formulating a strategy statement that establishes the clear direction of the organization

When strategic planning is done without putting effort into clearly determining an appropriate strategy, it tends to be largely an extrapolation of what has gone on in the past. This frequently results in managers making decisions based on operational rather than strategic perspectives. During strategy development, planners gather all kinds of

data about the environment to identify new strategies and assess their feasibility. This information is used to develop the implementation plan.

Implementation Plan

The role of organizational leaders in the implementation of the strategic plan cannot be overemphasized. Whether it is the chief law enforcement official, the district attorney or the CEO of a corporation, they must lead the implementation effort and be totally committed to it. It is therefore imperative for leaders to have a coherent implementation plan for any major change initiative.

Unfortunately, implementing change does not adhere to a simple, step-by-step process. There is no ironclad list or easy recipe for implementing success. In fact, a recent book attempting to pull together the best in practice recognized discord among its contributors on basic questions as whether there is a logical sequence to implementing change. However, over the last two decades the growing body of research examining the change process has produced a number of implementation checklists such as John P. Kotter's, "Eight-Stage Process of Creating Major Change."²⁴ Each stage was selected to address one of the eight fundamental errors that most often undermine transformation efforts:

1. Establishing a sense of urgency
 - Examining the market and competitive realities
 - Identifying and discussing crises or major opportunities
2. Creating the guiding coalition
 - Selecting a group with enough power to lead the change
 - Getting the group to work together like a team

3. Developing a vision and strategy
 - Creating a vision to help direct the change effort
 - Developing strategies for achieving that vision
4. Communicating the change vision
 - Constantly communicate the new vision and strategy
 - Leaders must role model behavior expected of employees
5. Empowering broad-based action
 - Getting rid of change obstacles
 - Changing systems or structures that undermine the vision
 - Encouraging risk-taking and nontraditional ideas
6. Generating short-term wins
 - Planning for visible improvements or wins
 - Creating those wins
 - Rewarding those who make the wins possible
7. Consolidating gains and producing more wins
 - Using increased credibility to change all systems, structures and policies that don't fit together or fit the transformation vision
 - Hiring, promoting and developing people that can implement the change vision
 - Reinvigorating the process with new projects, themes and change agents
8. Anchoring new approaches in the culture

- Improved performance through customer and productivity-oriented behavior, more and better leadership and more effective management
- Articulating the connections between new behaviors and organizational success
- Developing means to ensure leadership development and succession

The first four stages in the transformation process help to defrost a frozen status quo. Stages five through seven then introduce many new practices. The last stage grounds the changes in organizational culture to help make them stick.

Cost Analysis

Several supporting functional elements incorporate the strategic plan into the workings of an organization, the most important of which is the budget.²⁵ The budget is a detailed financial plan listing the resources or funds needed for a particular program, project, product, or unit. The budget of the functional units of the organization need to be integrated into a single budget that is the personification of the organization's strategic plan. The process by which the organization's management reviews the variances from budget, positive and negative, is the most obvious and clear-cut way of identifying the degree to which the strategic plan is being executed. When costs are underestimated in the planning process, which is typical, the budget can be quickly exceeded and the implementation process may have to be modified or placed on hold.

A comprehensive budgeting process begins with a detailed analysis of the strategic plan to provide economic forecasts. These forecasts, designed to meet

organizational goals, produce guidelines for use in the budget preparation. Although some organizations develop budgets at the top management level for distribution throughout the hierarchy, most agree that the departments and individuals responsible for implementation should be able to contribute to the development of the budget. A serious drawback to many budgets is their rigidity in the face of changing conditions. Budgets are forward-looking and should provide means of adjustment should changes affect the forecasts on which they are based. One way to insure financial flexibility in budgeting is to build-in a reserve account for changing conditions and emergencies.

Developing a budget to address the need for computer-based expertise for law enforcement will prove to be one of the more challenging aspects of the strategic plan, particularly for government agencies. In addition to computer training, there is a significant and immediate need for up-to-date technological tools and equipment for state and local law enforcement agencies to conduct electronic crime investigations. Most electronic crime cases cannot be thoroughly investigated and developed without the benefit of higher computer technology, which is beyond the budgets of many law enforcement agencies. The sophistication of technology used by offenders is increasing at a pace that significantly taxes the resources of the public sector at the state and local levels.

Turley's police chief should carefully evaluate the current budget situation to determine if funds from other divisions could be reallocated to high-tech crimes investigations and training. Grant funding offered through the Office of Criminal Justice Planning (OCJP) and the COPS Universal Hiring Program (UHP), U.S. Department of Justice, should be exploited to their fullest extent. The chief should form partnerships

with the high-technology industry to share high-tech information, obtain free hardware and software products, and share in training costs. If need be, the chief should be prepared to submit a mid-year budget request to the city council for additional funding. The Turley Police Department could assume a leadership role in developing a regional task force in Fresno County with other regional law enforcement agencies to consolidate resources and share information.

Summary

The purpose of this chapter was to develop a strategic plan to help the police department respond to the need for computer-based expertise. The strategic plan is a structured process by which the guiding members of an organization envision its future and develop the necessary procedures and operations to achieve the future. The 9-step Applied Strategic Planning Model was used to provide a framework for the plan's development.

Next, a description of the organization and a situational analysis was provided to better understand the organizational structure, culture and its environment. Strategy development determines the overall direction of the organization. It requires fresh thinking in a no-holds-barred atmosphere to make certain that the future is more than a carbon copy of the past.

To ensure effective implementation of the strategic plan, John P. Kotter's Eight-Stage Process of Creating Major Change was suggested to guide the planning team during the implementation process. Finally, a cost analysis pulls together all of the financial information required to support the strategic plan.

CHAPTER IV

TRANSITION MANAGEMENT

Introduction

In order to fully implement a strategic plan that requires some degree of organizational change, a transition must occur. Change is not the same as transition. Change is situational—the new job, a new policy or training program. Transition is the psychological process people go through in order to adapt to the new situation or environment they find themselves in. Unless transition occurs, change will not work. That's what happens when a great idea falls flat. According to Bridges (1991), the failure to identify and prepare people for transition is the single largest problem that organizations encounter when they implement major change initiatives.²⁶

The purpose of transition management is to insure that transition does take place so change can occur. It includes a commitment plan, proposed management structure, and techniques for managing the transition process.

Commitment Plan

The success of the strategic planning effort will be in direct proportion to the degree of commitment the key stakeholders make to the plan and the planning process. The committed person brings energy, passion and excitement to the change process. The commitment plan involves identifying a “critical mass” of stakeholders whose active participation is essential to the strategic plan. Critical mass is defined as the smallest number of groups or individuals whose support is necessary for successful change to occur and whose opposition will likely lead to failure. Commitment charting provides a method for assessing the critical mass and developing a strategy for getting the

necessary commitment.²⁷ Because the same level of commitment is not always necessary from everyone, a simple commitment chart is used with three kinds of commitment: let it happen, help it happen, and make it happen. The following commitment chart can be used to identify the critical mass and assess the level of commitment required for each individual or group:

Table Six
Commitment Chart

Key Players	No Commitment	Let It Happen	Help It Happen	Make It Happen
1. Police Department			X→	O
2. Sheriff's Department				XO
3. District Attorney	X→		O	
4. POST			X→	O
5. Business Community		O	←X	
6. State Attorney General			XO	
7. Local FBI Office		X→	O	
8. High-Technology Firms	X→		O	

An O indicates the minimum commitment required from the individual or group for change to occur. An X represents the present level of commitment. An X with an arrow indicates the direction it needs to move in order to achieve the minimum commitment. When the required commitment matches the present commitment, i.e., O and X appear in the same box, no additional work is required. The commitment chart provides a graphic depiction of commitment shortfalls and where additional support is required to implement the strategic plan. For example, Turley's police chief is somewhat ambivalent and is content to just "let it happen." As the chief executive officer and principle change agent for the department, a greater commitment is required of the chief. The chief will need to make it happen.

Understanding the level of commitment required from stakeholders is crucial to managing an issue, which further depends on how quickly and how effectively the planning team handles stakeholder concerns. If the planning team waits to act until an issue matures the issue has been interpreted by someone else and may defy management. Success requires influencing stakeholders to change their perceptions while those perceptions can still be changed. The key to success in the strategic planning process lies in getting the involvement and commitment of everyone in the organization. Remember, the purpose of planning is not to produce plans; it is to produce results, and this requires total organization commitment. A group of people truly committed to a common vision is an awesome force. They can accomplish the seemingly impossible.²⁸

Management Structure

Chief Executive Officer

The chief of police (or key decision maker) should be perceived as the person providing direct and active leadership to the strategic plan. The chief executive officer's primary strategic planning duties include approval of and, in many cases, direct involvement in such things as:

- Development of the organization's mission
- Identification and prioritization of critical issues
- Strategy development
- Identification and articulation of organization goals and objectives
- Preparing an executive summary

Naturally, there will be other areas where the chief needs to be involved as well. Even though others carry much of the detail work out, the chief has to provide the visibility and leadership in making sure the strategic plan is developed and implemented.

Planning Team

The planning team is generally made up of five to seven key executives including the chief and major department heads impacted by the strategic plan. Members of the planning team function as an extension of the chief and should have authority to cross divisional boundaries when necessary.

Consultant

Although the Applied Strategic Planning Model is relatively easy to understand, it needs to be understood by the members of the planning team at a very high level of comprehension. An experienced consultant can be invaluable and is recommended to provide the planning team formal training on the process, as it will serve as a template for the team's activities over a period of several months. Another role of the consultant is to serve as a facilitator. A facilitator helps the planning team deal with small-group process issues that are so vital to a successful planning process. The consultant can also serve as a coach or expert in the strategic planning process.

Transition Monitoring Team

One of the persistent problems during transition is for decision makers and those implementing decisions to be clear on precisely what impact the decisions and actions will have. Leaders usually assume that all the feedback they need should come up through normal communication channels and will be voiced at staff meetings in reply to

the question, “How are we doing?” This is where a transition monitoring team is valuable. The transition monitoring team is a group of five to seven people from a cross-section of the organization. The team meets every week or two to take a pulse of the organization in transition. It has no decision-making power and is not intended to suggest courses of action. Rather, its purpose is to facilitate upward communication and to do three other things:

1. Demonstrate a genuine concern for how things are going
2. Review plans and communications before they are announced
3. Correct misinformation and provide rumor control

It is recommended that some members from the strategic planning team serve on the transition monitoring team for continuity between plans and operations and clarification of issues.²⁹

When developing a management structure it is important to rely less on managerial authority, formal rules and procedures, and narrow divisions of work. Instead, the chief should create teams that share information and delegate responsibility and authority to the lowest level possible. In effect, organizations are moving from the hierarchical and bureaucratic model that has characterized corporations since World War II to what we now call task-driven organizations, where what has to be done governs who works with whom and who leads.³⁰ In community policing circles, this concept is referred to as employee empowerment and is one of the twelve principles of Community Oriented Policing and problem Solving (COPPS).

Transition Techniques

In addition to Kotter's checklist for implementation described in Chapter III, this section provides a six-phase change strategy developed by Stella Louise Cowan. As transition manager, the chief of police assumes the leadership role in managing the transition process. To assist in this process, the chief can use the following six-phase change strategy:³¹

Phase I. Create awareness and a sense of urgency

The chief must decide when and how others in the organization should get involved in the strategic plan. Information sharing of the plan throughout the organization is absolutely essential if the plan is to be implemented. Often change is precipitated by some crisis that essentially demands some response by the organization, such as the city manager's mandate for the chief to change the way the police department responds to computer crime. People need to understand why change is necessary for change to occur. The chief should develop a shared vision throughout the organization that embodies a sense of urgency. People need visions to make the purpose more concrete and tangible. The more people in the organization who understand the chief's vision and share a sense of urgency, the easier it will be for change to occur, particularly if there is consensus about the need for change.

During this phase, the chief explains the need to develop computer-based expertise for first responders and investigators within the organization. The current state of cybercrime in California, coupled with the information developed during the strategic planning process, provides a powerful motivation for change. Continual communication of this information is critical in preparing people for the upcoming

change. Members of the organization who do not get the information they need may turn to co-workers and other sources for information, and that information may not be accurate or supportive.

Phase II. Engage the culture

Engaging the culture is about getting others involved in the change. It can involve briefings, meetings, newsletters or any vehicle that provides the chief an opportunity to engage people in dialogue about the change. It also provides employees an opportunity to ask questions, offer suggestions and listen to the chief. The chief can dispel rumors or information that can derail the change process. It's a time for the chief to demonstrate sincerity and confidence for his strategic plan.

During this phase, support systems may be introduced to help employees cope with the upcoming changes. Some employees may go through a grieving process and support systems can help them deal with the wide range of emotions that can stifle effective change. Once it is understood that transition begins with letting go of something, then the first step has been taken in the task of transition management. Finally, if everyone recognizes the problem, it is likely to be solved much faster. Selling problems implicates everyone in the solution. If you want to be part of the solution—get involved. If you don't—don't complain.

Phase III. Transform the culture – process and people

In this phase, specific actions identified in the strategic plan are implemented to transform the organizational culture, operations and staff assignments. Such actions might include training, policy formation, clarifying new job assignments, changes in the

organizational structure, new technology, redesign of performance system, and implementing feedback mechanisms.

As changes are implemented there will be some confusion and frustration with the process. The transition monitoring team can provide coaching, problem solving and provide a feedback mechanism for employees. This is a time for the chief to monitor and adjust strategies where necessary to facilitate the transition process. It is possible that some processes could be improved. If one is identified, the chief can win the support and confidence of others by being flexible.

It is wise for the chief to be highly visible during these times. People look for leadership during times of crisis, and some may feel as though they are in crisis. The chief will want to be encouraging and empathetic, yet keep his/her staff focused on the vision through communication. The chief should take advantage of small wins or other progress to reward employees. This tends to encourage people when they can see tangible examples of what the chief desires.

Phase IV. Monitor impact and results

Feedback and evaluation systems will help the chief monitor the progress and results of organizational changes. Questions that will need to be answered include such things as: Are employees adapting to the changes? Are the changes meeting customer needs? Are new systems or process changes progressing as expected? Are problems being addressed in a timely manner? Are the projected results being obtained?

Phase V. Respond to feedback

Feedback mechanisms inform the chief of unintended deviations from plans and objectives, which may signal a need for adjustments in the transition process. Based on the feedback obtained, there could be ongoing, appropriate adjustments to the change strategies. These changes could impact processes, job descriptions or any other aspect of the change initiative. However, the vision should be used as a filter when making adjustments. Additionally, feedback may identify a need to increase or decrease the rate of change. The most important aspect of feedback mechanisms is for the process to be a two-way conversation. The chief must ensure that responses are provided to comments and suggestions from people involved in the change process. Without a two-way dialogue there is no communication.

Phase VI. Sustain the change and the commitment

Shared visions are sustained because of a reinforcing process of increasing clarity, enthusiasm, communication and commitment. As people talk, the vision grows clearer. As it gets clearer, enthusiasm for its benefits builds thus sustaining the change and commitment.³² The chief must continue to communicate the shared vision to sustained change and commitment.

To institutionalize change, managers and leaders should demonstrate by example their commitment to the transition process, reward risk-taking, and incorporate new behaviors into the day-to-day operations of the organization. By reinforcing the new culture, they affirm its importance and hasten its acceptance.³³

Once the desired results are being achieved and the change initiative has taken hold, the chief will want to take steps to sustain the change and commitment. This is

sometimes referred to as freezing an organization. In other words, freezing takes place to maintain the achievement of desired results from the organization by avoiding unnecessary change.

Sustaining a commitment to organizational changes also involves developing enabling structures designed to encourage and sustain the new culture. Such enabling structures include ongoing training, policy formation, and department rewards and recognition programs that promote the change process.

Each time a significant milestone is reached in implementation, a celebration is needed. Organizations that regularly attend to such accomplishments with verbal praise and recognition are clearly demonstrating to their employees two things: the organization's commitment to the accomplishment of its strategic plan and the organization's awareness that the accomplishment of the plan requires everyone's involvement and hard work.

Summary

The purpose of this chapter was to develop a transition management plan. It began with a commitment plan that involves identifying a critical mass of those whose active participation is essential to the implementation of the strategic plan. Commitment charting was introduced as a method of charting the critical mass and assessing the level of commitment required for each individual or group. The key to success in the strategic planning process lies in getting the involvement and commitment of significant stakeholders.

A management structure for the planning, development and implementation of the strategic plan was suggested which includes the chief executive officer, planning

team, consultant, and a transition monitoring team. In developing a management structure it is important to rely less on managerial authority, formal rules and procedures, and narrow divisions of work. Instead, the chief should create teams that share information and delegate responsibility and authority to the lowest level possible.

The last chapter provides a project summary, evaluation activities, and recommendations for the future, implications for leadership, and final comments and conclusions.

CHAPTER V

CONCLUSION

Project Summary

The purpose of this project was to examine how California law enforcement will respond to the need for computer-based expertise in the identification, collection and preservation of electronic evidence by the year 2006.

The project began with scanning the environment to collect information about external circumstances in order to detect the development of relevant social, technological, economic, environmental and political trends likely to impact on the future of computer-based expertise in law enforcement. Magazine and newspaper articles, seminar reports and professional journals were collected from Internet searches. Three major themes emerged from scanning the various environments for trends impacting the issue statement. First, high technology crime is on the rise and is proportionate to the rapid increase and change in technology. Secondly, law enforcement is having a difficult time coping with the volume and complexity of high technology crimes. The criminals appear to have the upper hand. Finally, law enforcement appears ill prepared for the tremendous increase in cybercrime.

A literature review of numerous books and several interviews with practitioners provided additional insight and knowledge from experts in the field of cybercrime. Most books on cybercrime were published in the last ten years and are theoretical, offering little practicality for law enforcement investigators. Because of the rapid change in technology, some of the books are not current on the latest technology and modus

operandi issues regarding cybercrime. It was not surprising to find that the literature review tended to support the three emerging trends from the environmental scan.

Next, a group of handpicked professionals from the public and private sectors participated in a Nominal Group Technique to identify trends and events likely to have an impact on the issue statement. The panel members rated each trend and event regarding its impact on the future and recorded their findings in summary tables for presentation. A Cross Impact Analysis Matrix was presented to evaluate the interrelationships between trends and events. The cross-impact analysis can help law enforcement identify and plan for the simultaneous occurrence of trends and events, or prevent such occurrences if possible.

The information from the environmental scan, Internet searches, literature reviews, interviews and the NGT were used to develop three likely scenarios: optimistic, pessimistic and surprise free. The pessimistic scenario was selected as the most probable future for the mythical Turley Police Department. A strategic plan was developed to provide a framework for action to assist the Turley Police Department respond to the need for law enforcement computer-based expertise in the pessimistic future. The Applied Strategic Planning Model was used to provide a formal structure to the planning process. The strategic plan included an organizational description, situational and cost analysis, strategy development, and an implementation plan utilizing Kotter's, "Eight-Stage Process of Creating Major Change" checklist.

Strategic planning, in and of itself, is an academic pursuit of little direct use to any organization. The payoff of strategic planning is in its application and in the execution and implementation of the strategic plan. To effectively implement the

strategic plan, a transition management process was developed with a commitment plan for stakeholders, a proposed management structure, and some helpful transition techniques from Stella Louise Cowan's six-phase change strategy model provided a step-by-step process to assist in managing the transition process.

Evaluation Activities

Evaluation is an essential aspect of the management process and is critical to the effective implementation of any strategic plan. Evaluation activities involve listening and responding to feedback from employees and stakeholders; collecting and interpreting relative data and information; continuous scanning of the environment for potential threats and opportunities; making appropriate adjustments to plans and operations when necessary; reporting and budgeting; and monitoring key activities to ensure that operations are consistent with organizational goals and objectives.³⁴ As a management control system, evaluation activities should be incorporated into each step of the Applied Strategic Planning Model discussed in Chapter III.

Each law enforcement agency in California will need to identify a team of individuals to monitor the progress of their agency's strategic plan and report to the sheriff or police chief on their findings. Obviously, each agency will have to conduct a periodical needs assessment concerning the degree to which cybercrime is impacting their community and the required training and other resources needed to address the problem. The members should be selected from the strategic planning team or transition monitoring team for consistency and continuity of the agency's strategic plan.

As new cybercrime training programs are implemented at the state and local level, the curriculums will require frequent evaluations and updates to insure such

training programs are providing California law enforcement with the most relevant and current information available. Regional evaluation committees should be formed of local, state and federal law enforcement, the district attorney's office, and representatives from the high-tech industry. The evaluation committee should convene regularly to discuss and evaluate the status of cybercrime and make recommendations to POST on law enforcement training curriculums on cybercrime. Committee members should attend annual training seminars and training conferences to stay current on the latest technologies and investigative techniques on cybercrime. Certification programs should require annual training and testing to validate individual technical proficiency of expert witness testimony and search warrant affidavit information.

Recommendations for the Future

As with other law enforcement challenges, the issue of computer-based expertise is a complex problem and cannot be address in a vacuum. It will require a more global approach to the whole spectrum of cybercrime to be successful. Consideration must not only be given to training, but also to other resources such as funding, personnel and equipment. It will require a coordinated response from local, state, and federal government agencies, as well as the high-tech business community.

The ability of California law enforcement to detect, investigate and prosecute cybercrimes is a growing concern. Law enforcement officers and forensic scientists need specific levels of training to perform their respective roles when investigating electronic crimes, collecting and examining evidence, and providing courtroom testimony. The lack of training was considered the most significant trend identified by the NGT panel and is also the issue statement for this paper. POST academic

standards should be developed and applied toward certification programs that insure uniform training levels for law enforcement personnel throughout the state. Both entry-level and advance computer-based training are needed for law enforcement officers, parole and probation officers, as well as prosecutors and judges. Because computers are used in nearly every type of crime, first responders who secure the initial crime scenes require basic training in electronic evidence recognition and collection techniques.

Given the rapid change in technology, one-time computer-based training programs will provide little value if not followed up with regular training updates and periodical seminars designed to keep pace with the cyber criminals. To assist in identifying the most current training opportunities, law enforcement needs a comprehensive directory of electronic crime training and other resources available throughout the state. Many investigators and prosecutors are calling for a national clearinghouse of online information and technical guidance to assist local law enforcement agencies with cybercrime investigations.³⁵ It is critical to publicize a list of available training, high-tech organizations and associations, and professional seminars if such resources are to be exploited to their maximum potential. An online training directory or self-help Web site of the latest investigative techniques and tools would be extremely valuable to law enforcement. Sometimes the most valuable information is on what to avoid or what procedure or technique doesn't work. Such information can save valuable resources and result in more successful investigations.

Law enforcement will not be able to conduct training or investigate cybercrime without additional resources. Both officers and investigators need up-to-date

technological tools and computer equipment to properly conduct electronic crime investigations. Most electronic crime cases cannot be thoroughly investigated and developed without the use of higher end computer technology. Computer systems, software, hardware, intrusion detection tools, decryption technology, and other forensic equipment are expensive and beyond the budgets of most local law enforcement agencies. Even when special equipment is available, it is frequently out of date or otherwise unusable due to the rapid change in technology. A recent request by FBI Director Louis J. Freeh for additional funding from Congress to fight cybercrime indicates the problem is not confined to agencies like the Turley Police Department.³⁶ Physical space for a forensic laboratory or computer workstation is a pressing need in many agencies as well.

Forming partnerships between law enforcement and private industry can provide another source of high-tech training and information. Many firms have their own information security units that detect and investigate electronic crime. These units provide computer security training to employees and often work closely with local law enforcement. Increased cooperation and exchange of technical information between private industry experts and law enforcement is critical to controlling cybercrime. The private sector can assist law enforcement by reporting incidents of electronic crime committed against their systems, helping to sponsor training, joining task forces and sharing information and equipment for examining electronic evidence. Cybercrime investigators need the private sector's full support and cooperation to control electronic crime.

As some law enforcement agencies begin to address electronic crime, they grapple with how best to investigate crimes involving computers. They are uncertain whether to develop their own electronic crimes unit, join an existing regional high-tech task force, or form a partnership with other law enforcement agencies to create a new high-tech task force. Belonging to an agency that is just now beginning to explore the issues surrounding electronic crime is a common situation. Each agency should conduct an internal and external needs assessment to determine which investigative approach is best given their available resources. According to many experts, California is leading the Nation in the fight against cybercrime. Captain Jan Hoganson as well as others, believe that California's success is largely due to the creation of five regional high-tech task forces.

The laws applicable to cyberspace are problematic and are intimately related to training. Effective, uniform laws that keep pace with electronic crime need to be promulgated and applied at the federal and state levels. Technology is changing so rapidly that legislators cannot keep up with the pace. Often electronic crimes outpace legislation, such as with the latest trends of cyber stalking and hate e-mail. The disparity in penal statutes between states impedes interstate pursuit of cyber criminals. This is a serious problem with electronic crime because it usually occurs outside discrete physical and jurisdictional boundaries. Regardless of the skill of the investigator, the investigation can be hampered in developing a case for prosecution by differences in or lack of penal statutes.

Implications for Leadership

Law enforcement managers can no longer ignore the growing and complex problems associated with cybercrime and the critical need for computer-based training for law enforcement. The implication for law enforcement leadership is clear—we must lead a coordinated response to establish minimum training standards at the state and local level if we are to meet the demand for computer-based expertise for California law enforcement by the year 2006. This coordinated response must include forming partnerships with the private sector, especially high technology businesses and Internet service providers. Although California has experienced success with its five regional task forces, there are many agencies doing little or nothing in the fight against cybercrime. Senior law enforcement managers and elected officials need to be more aware of the rapid growth of electronic crime and its impact on their communities. They must get involved at every opportunity in the war against cybercrime.

The success of the strategic planning effort and its implementation will depend largely on the degree of commitment by chief law enforcement executives. State and local law enforcement agencies need immediate assistance in developing computer investigating units, creating regional computer forensics capabilities, organizing task forces, and establishing partnerships with private industry. Such assistance will not be possible without the active support of law enforcement leaders. Combining expertise and pooling resources is one of the only ways that smaller law enforcement agencies can stay ahead of cyber criminals.

Conclusion

There are three major themes that emerge from this project that will have a significant impact on the issue statement. First, high technology crime is on the rise and is proportionate to the rapid increase and change in technology. The abuse and misuse of information through computers will continue to increase dramatically as hundreds of millions of people communicate and engage in commerce, work, education, and many other social activities. The use of the Internet to commit fraud, identity theft, auctions and information theft leads the way in high-tech crimes.³⁷ Second, law enforcement is having a difficult time coping with the volume and complexity of high technology crimes. The criminals appear to have the upper hand. They are more sophisticated and knowledgeable about technology and use their knowledge to elude law enforcement. Today's electronic crimes cannot be effectively investigated with equipment and procedural techniques developed during the infancy of the information age. Finally, by all indications, law enforcement is ill prepared for the tremendous increase in cybercrime. There is a critical shortage of trained forensic specialists, high-tech investigators, as well as a lack of computer-based knowledge by field officers and supervisors.

The outlook for curtailing cyberspace crime by technology or conventional law enforcement methods is bleak. Most agencies do not have the personnel or the skills to cope with such offenses, and to date all high-tech approaches have been met by almost immediate turnabouts by hackers or crackers.³⁸ In the future, many more users will possess skills far beyond those of today's cyber criminals—a process termed by experts

as the democratization of computer crime. Electronic crime will get more sophisticated as cyber criminals lead law enforcement toward higher technology.

Cybercrime probably cannot be controlled by conventional methods. Technology is on the side of the cyberspace offender and motivation is high—it's fun, exciting, challenging, and profitable. As individuals see and talk to each other over computers in the next few years, and as nanotechnology makes computers even more portable, new technology will emerge to protect data. But simplifying systems to make them more universally acceptable and accessible will also make them more vulnerable to intruders. The only real help is one that has not proven very successful in recent decades: conscience and personal values—the belief that theft, deception, and invasion of privacy are simply unacceptable.³⁹

Experts predict that computer crime and crimes perpetrated across the Internet will be California law enforcement's biggest problem in the future. This future is not far off.⁴⁰

APPENDIX A

Nominal Group Panel

Dr. Kall Loper, Professor California State University Sacramento

Dr. Loper is an Assistant at California State University Sacramento and faculty member of the University's Criminal Justice Department. Prior to that he was a doctoral fellow and instructor at Michigan State University. His dissertation, entitled the Criminology of Computer Hackers: A Qualitative and Quantitative Analysis, uses field observations of hackers to build 'profiles' or prediction models of hacker's skill based on their on-line interactions. His other works include an article on the detection and investigation of E-mail spoofing, and he is co-authoring an upcoming textbook on computer crime from Wadsworth Publishing. Dr. Loper is an active member of the High Technology Crime Investigation Association and is the 2000-2002 Program Committee member in the area of computer crime for the Academy of Criminal Justice Sciences.

Vickie Wright, State Attorney General's Office, Crime Prevention Center

Ms. Vickie Wright has twelve years experience as a Crime Prevention Specialist with the Sacramento County Sheriff's Department, Citrus Heights Police Department and currently with State Attorney General's Office. She is also an instructor in Cultural Diversity, Intercultural Communications, Community Relations, Media Relations and Crime Prevention for the Sacramento County Sheriff's Department's Training Academy and coordinator and instructor for the Basic Crime Prevention Class at the Sacramento Regional Training Center, which is affiliated with American River College. In addition, Vickie is a member and liaison to the California Crime Prevention Officer's Association, the California Rural Crime Prevention Task Force and an Advisory Board Member for Crime Victims United of California as well as past Law Enforcement Advisory Board Member of the Citizen's Crime Alert Program.

Robert Morgester, State Attorney General's Office, High-Tech Task Force

Mr. Morgester is a Deputy Attorney General and High Technology Crime Prosecution Coordinator for the California Attorney General's Office in Sacramento where he has been employed since April of 1999. Prior to his employment with the Attorney General's Office, Mr. Morgester was a Deputy District Attorney with the Sacramento County District Attorney's Office for 10 years. As a Deputy District Attorney, Mr. Morgester participated in the creation and implementation of the Domestic Violence Home Court Project and the Sacramento Valley High-Technology Crimes Task Force. He is a state recognized authority on high technology crime prosecutions and has testified as an expert on high technology crime in both California's Senate and Assembly, in addition has taught and lectured extensively on high technology crime issues throughout the United States. Mr. Morgester has previously worked with the American Prosecutors Research Institute, California Department of Justice, California District Attorney's Association, National Association of Attorneys General, Northern

California District Attorney Investigator's College, Sacramento Valley High Technology Crimes Task Force, and SEARCH on curriculum development for law enforcement training on high technology crime issues.

Mike Menz, Sacramento County Sheriff's High-Tech Task Force

Mr. Michael Menz (Mark's brother) joined the Sheriff's Department as a reserve officer in 1985. He left in 1987 to work full time as a police officer for the City of Santa Cruz. He returned to Roseville to work as a police officer in 1990 and finally came back to the Sheriff's Department in 1998. Michael is considered an expert in high technology related crime and computer network intrusion crime. He is a published author, an ICI certified instructor and an adjunct professor for the University of New Haven's Criminal Justice program. He is currently the Secretary for the International board of the High Technology Crime Investigation Association, a 2600 member association of investigators from around the world. Michael is responsible for computer forensics and training and investigations and has conducted or assisted in excess of 500 hi-tech investigations and conducted over 300 forensic examinations. Michael also holds both an A+ certification as well as a California POST ICI certification for the Investigation of Computer Crime and a California POST Advance Officer certification.

Mark Menz, Sacramento Search Group

Mr. Menz joined the Kroll Technology Group as the Director of Training, Computer Forensics & Security in the Sacramento office in April of 2001. In addition to providing instructional services, he assists with technology related investigations and security as well as computer forensics. Mark is considered an expert in high technology crimes and computer network systems design. He is a published author, an ICI certified instructor and an adjunct professor for the University of New Haven's Criminal Justice program. Mark is formerly a System Specialist at SEARCH Group, Inc. the prestigious government-funded training institute. Mark provided training and investigative support to criminal justice agencies nationwide (over 3000 law enforcement officers) in the identification and investigation of high technology related crimes and the examination of seized computer media. Mark has been an instructor and lecturer in both private industry and public schools on information system design, system security and peripheral design. Prior to joining the SEARCH Group Mark was the Deputy Operation Director and Chief Information Manager for Compac Engineering and one of the founders of Progressive Image Technology (later called PLAY, Inc.). Mark also holds both an A+ and Sans' GIAC certifications as well as a California POST ICI certification for the Investigation of Computer Crime and is an ICI certified instructor.

Bruce Boles, Hewlett Packard Executive

Mr. Bruce Boles has been a Hewlett Packard employee for over 23 years. He is currently the Customer Advocacy Manager for the HP Services – North America Order Administration organization. He is responsible for the organization's quality system including managing customer feedback / surveys, business planning, management /

quality consulting, project management / facilitation, and quality training. Bruce has worked in many functions during his HP tenure including manufacturing engineering, marketing and quality. Outside of HP, Bruce is involved with a Boy Scout Troop in Rocklin and participating in improvement projects within the Rocklin School District.

Dave Spisak, Commission on Peace Officer Standards of Training (POST)

As a Senior Law Enforcement Consultant for POST, Dave Spisak's projects include: design; development and delivery of cultural diversity coursework; developmental disability; hate crime; domestic violence; interactive video (IVD) training for narcotics identification; narcotics law; under the influence testing and narcotics investigations. Dave also produced 2-hour satellite broadcasts including: White Gangs; Hispanic Gangs; African-American Gangs; Southeast Asian Gangs; Hate Crime; Cultural Diversity; and Law Enforcement Awareness of Disabilities (LEADS). His responsibilities include evaluation of the effectiveness of various educational and training programs, field surveys, training needs assessments and evaluation of various educational software, products and services. Prior to his present 10 years of employment with POST, Mr. Spisak worked for 25 years with the San Diego Police Department with such assignments as Commanding Officer of Special Investigations; Central Investigations; Public Information/Media; Community Relations; Research and Analysis; and Traffic Operations. Also served as undercover detective with vice and criminal intelligence assignments as well as routine patrol and supervisory assignments. Mr. Spisak has an M.S. Advanced to Candidacy for Criminal Justice Administration, and B.S. Political Science from San Diego State University. He holds his Basic, Intermediate, Advanced, and Management Certificates from POST and is a Training Graduate, National Academy, Federal Bureau of Investigation, 128th Class.

Jeff Ritschard, Sacramento County District Attorney's Office

Mr. Jeffrey R. Ritschard is a Deputy District Attorney employed by the Sacramento County District Attorney's Office. He joined the district attorney's office in 1988. He has been assigned to various special teams including the Career Criminal Unit, the Major Narcotics Unit, and the Special Assault and Child Abuse Unit. Mr. Ritschard was assigned to the Sacramento Valley High-Technology Task Force in September 1999. He is responsible for addressing legal issues, reviewing search warrants, making filing decisions, and the prosecution of task force cases in Sacramento County. Mr. Ritschard is a member of the California District Attorney's Association's committee on high technology crimes. He serves as the legislative liaison for the committee. Mr. Ritschard received his undergraduate degree in political science from California State University, Hayward and his Juris Doctorate from the University of California, Davis.

Glen Sylvester, San Francisco Police Department, High-Tech Crimes Unit

Carole Adell, Renaissance Consulting Group

Ms. Carole T. Adell is President of Renaissance Consulting Group, an international consulting firm serving private and public sector clients based in Sacramento, California. Her expertise is in strategic planning, organization development, human resources, research, measurement and evaluation. She is a large-group strategic planning model expert; an accomplished researcher and evaluator; and a third-party employment law investigator. Consulting results include: world-wide logistics and financial strategic plans for Hewlett-Packard; design, research and evaluation of criminal justice programs and services for criminal justice agencies in Stanislaus County, California; and, development of a best-practices audit for employers and third-party investigations for Littler-Mendelson the nation's largest labor law firm.

Lon Ramlan, San Francisco Police Department Computer Forensic Analysis

Lieutenant Lon Ramlan has served in the San Francisco Police Department for more than 20 years. Lon has worked various assignments throughout the department including uniformed patrol, special enforcement, investigations and administration in the ranks of police officer, sergeant, inspector and lieutenant. He is currently the Commander of the Crime Scenes Investigation unit. Lon is a qualified ICI instructor and has presented computer crime training for various state, national, university and private sector programs. He also serves on the National Cybercrime Training Partnership (NCTP) networking portfolio.

Hong C. Li, Intel Corporation

Dr. Hong Li is an information security architect at Intel Corporation. Before joining Intel, she was a senior security engineer at SAIC (Science Applications International Corporation), where she worked on a system management and integration contract for the Department of Justice (DOJ). Prior to SAIC, Hong worked for ECUTEL, where she was a lead software engineer and architect for the design and development of a Mobile IP product suite. Before switching her career into information technology, Hong worked as research associate for the U.S. Naval Research Laboratory and Penn State University on liquid crystal materials and electro-optical devices. She received her Ph.D in electrical engineering from Penn State University in 1995, and BS in electrical engineering from Jiaotong University, China in 1988.

APPENDIX B

List of Trends

- Law enforcement use of digital cameras for evidence at crime scene
- New technology is faster, smaller, wireless, more powerful, portable
- Legal review of state, federal and international criminal laws for consistency between crimes committed in cyber world v. real world
- Inability of law enforcement to get information because of encryption
- No consistency in training everyone getting into the training field
- Offsite storage facilities
- Hi-tech crime statistics used for allocation personnel and resources
- The proliferation and re-purposing of personal data
- Competition for skilled employees between both public and private
- Increase availability and quality of encryption
- Sophistication of detection and prevention tools (firewalls, etc)
- Cybercrime is victimless by morphing images or information
- Increase government regulations on privacy issues
- Privatization of law enforcement for cybercrime investigations
- Volume of data v. court ordered turnaround times on forensics
- Authentication and credibility of data and persona
- Internet Service Provider (ISP) via satellite
- Web privacy standards (company generated privacy policies)
- Business and government partnerships to share knowledge and resources
- International cyber criminals exploiting the lack of cooperation and compatibility in international laws

- False information dissemination and use of it for criminal activities
- Lack of state and national forensic resources
- Civilian v. police assignments and capabilities
- Increased infrastructure dependence on technology
- Gap between law enforcement policy and reality regarding cybercrime
- Volume of data and e-commerce
- Employees who take jobs to commit crimes and use company resources
- Hackers hired as company consultants
- Make digital evidence recovery scientific instead of investigative
- First responder awareness and lack of training
- Availability of personal information—web-based
- Frustrations with inability to share data and resources
- High-tech training requirements including time, costs, and consistency
- Availability and use of anatomizes
- The use of digital signatures
- Full disclosure of electronic evidence for defense attorneys
- Immediate dissemination of information and hacking tools
- On-scene forensic examinations
- Jurisdiction
- Increased funding for training and prosecution of high-tech crimes
- Continued lack of leadership for developing a strategic plan
- Cybercrime volume and diversity as more people use computers

APPENDIX C

List of Events

- Digital signature enacted in June 2000
- Post office becomes central certificate authority
- Hippa interpretation of health information Policy and Privacy Act
- Loss of Microsoft monopoly
- Major terrorist attack on U.S. infrastructure via Internet
- Cyber cops that are loaned, funded and shared with hi-tech companies
- Laws will be passed to make digital evidence more admissible in court
- POST forms a cybercrimes advisory council
- Speech recognition replaces the keyboard
- U.S. courts rule law enforcement cannot compel production of encryption keys from criminals
- Wireless technology replaces wires as standard
- California allows out-of-state video testimony to be admissible
- Biometrics identifications replaces numeric identification
- DNA used as method of authentication
- FBI deputizes local agencies to handle national cybercrime
- Small island declared sovereign nation and used as offshore data storage area
- University introduces educational computer program for law enforcement s
- Every crime will have a cyber element
- Kill someone identification in cyber-world rather than really kill someone
- Restrictions on encryption products will be further relaxed.

- POST mandates cybercrime training standards for California
- California legislation defines types of private information that can be disseminated on Internet.
- Government coordinates all data related to individuals making it available to law enforcement units in the field
- Intel introduces startreck type holodecks
- Extended power blackouts in California
- Artificial intelligence becomes commonplace
- Laid-off workers from hi-tech companies with computer skills going to the dark side
- California announces its first virtual school for kids.
- Vehicles are registered on line
- California has its first on-line grade school—like we have in college now.
- Supreme Court rules that forensics have to be done in 72 hours
- CHP takes over all local law enforcement of cybercrimes
- Transient commits cyber fraud in 18 countries
- State Attorney General calls a symposium to solve cybercrime jurisdiction in California

ENDNOTES

¹ Neil Barrett, Digital Crime, Policing the Cybernation (London: Kogan Page Limited, 1997), p.15.

² Bruce Sterling, The Hacker Crackdown, Law and Disorder on the Electronic Frontier (New York: Bantam Books, 1992), p.233-234.

³ Brian Krebs, "Internet Fraud Reports Continue To Pour In – FBI," Newsbytes. Internet. <<http://www.newsbytes.com/news/01/164918.html>> Accessed: 2 May 2001.

⁴ 2001 Annual Report on High Technology Crime in California, California High Technology Crime Advisory Committee, April 20, 2001.

⁵ Ibid.

⁶ Michael R. Anderson, "Safe Seizure of The Computer," New Technologies, Inc., Internet. <<http://www.secure-data.com>> Document 50745, 6 February 1998, p. 1.

⁷ Wayne P. Williams, "The National Cybercrime Training Partnership," The Police Chief, February 1999, p. 18.

⁸ Ibid.

⁹ Madeline Bennett, "High-tech vigilantes face legal threat," ZD Net News, Internet <<http://www.zdnet.com/zdnn/stories/news/o,4586,2716730,00.html>> , Accessed: 14 May 2001.

¹⁰ Carrie Kirby, "Cyber Sleuths," San Francisco Chronicle, 26 February 2001, B3.

¹¹ Thomas Mahoney, D.P.A., "Writing A Criminal Justice Research Paper," The Journal of California Law Enforcement, 10 May 1998, p. 6-10.

¹² Dr. Gerand L. Kovacich and William C. Boni, High-Technology-Crime Investigator's Handbook (Boston: Butterworth Heinemann, 2000), p. 270.

¹³ Wilma S. Longstreet and Harold G. Shane, "Curriculum for a New Millennium," (Allyn & Bacon, 1993), p. 166.

¹⁴ Ibid. p. 172.

¹⁵ Lawrence Wilkinson, "How to Build Scenarios," Hotwired Presents, 1995, p. 1-9.

¹⁶ Leonard Goodstein, Timothy Nolan, and J. William Pfeiffer, Applied Strategic Planning, How to Develop a Plan That Really Works (New York: McGraw-Hill, Inc., 1993), p. 7-35.

¹⁷ Louis E. Boone and David L. Kurtz, Principles of Management (2d ed. New York: Random House, 1984) p.129.

¹⁸ Tom Esensten, Lecture entitled, "Strategic Planning," (Organizational Effectiveness Consulting, n.d.), p. 8.

¹⁹ Goodstein, Applied Strategic Planning, How to Develop a Plan That Really Works, p. 310.

²⁰ "FM101-5." United States Army Field Manual, 1987.

²¹ Boone, Principles of Management, p.125.

²² Ibid., p. 129.

²⁴ John P. Kotter, Leading Change (Massachusetts, Boston: Harvard Business School Press, 1996), p. 21.

²⁵ Goodstein, Applied Strategic Planning, How to Develop a Plan That Really Works, p. 341.

²⁶ William Bridges, Managing Transitions Making the Most of Change (Massachusetts, Reading: Perseus Books, 1991), p. 5.

²⁷ Todd D. Jick, Notes entitled, "Implementing Change," (Harvard Business School, 1991), p. 198-199.

²⁸ Peter M. Senge, The Fifth Discipline, The Art & Practice of The Learning Organization (New York: Doubleday, 1990), p.721.

²⁹ Goodstein, Applied Strategic Planning, How to Develop a Plan That Really Works, p. 71-90.

³⁰ Ibid.

³¹ Brian Cowley, "The Man Who Changed Everyone's Life – The Ubiquitous Ideas of F.A. Hayek," Internet <http://www.iedm.org/home_en.html>.

³² Senge, The Fifth Discipline, The Art & Practice of The Learning Organization, p.721.

³³ Hollis Stambaugh et al., "State and Local Law Enforcement Needs to Combat Electronic Crime", National Institute of Justice Research in Brief, August 2000, p. 5.

³⁴ Boone, Principles of Management, p.5-9.

³⁵ Hollis Stambaugh et al., "Electronic Crime Needs Assessment for State and Local Law Enforcement", National Institute of Justice Research Report, March 2001, p. 34.

³⁶ "FBI wants more money for fighting cybercrime." SV News Services. Internet. <<http://www.ciol.com/content/news/repts/00033001.asp>>. Accessed: April 16, 2001.

³⁷ Donn B. Parker. "Fighting Computer Crime: A New Framework for Protecting Information." Wiley, John & Sons Incorporated. August 1998. "Annotation." Barnes & Noble.com. Internet. <<http://rl.us.rmi.yahoo.com/rmi/http://shop.barnesandnoble.com/booksearch/isbnInquiry.asp/rr...>>. Accessed: March 30, 2001.

³⁸ Gene Stephens. "Crime in Cyberspace." The Futurist, September-October 1995, p. 28.

³⁹ Ibid.

⁴⁰ Lois Pilant. "Fighting Crime in Syberspace." The Police Chief, August 1997, p. 28.

BIBLIOGRAPHY

- 2001 Annual Report on High Technology Crime in California. California High Technology Crime Advisory Committee, 20 April 2001.
- Anderson, Michael R. "Safe Seizure of The Computer." New Technologies, Inc., Internet. <<http://www.secure-data.com>> Document 50745, 6 February 1998.
- Barrett, Neil. Digital Crime, Policing the Cybernation. London: Kogan Page Limited, 1997.
- Bennett, Madeline. "High-tech vigilantes face legal threat." ZD Net News, Internet <<http://www.zdnet.com/zdnn/stories/news/0,4586,2716730,00.html>> , Accessed: 14 May 2001.
- Boone, Louis E. and Kurtz David L. Principles of Management. 2d ed. New York: Random House, 1984.
- Bowker, Arthur L. "Sentencing Issues for High Tech Cases in Federal Court." HTCIA International. High Technology Crime Investigation Association. March 2001, Vol. 2, Issue 1.
- Bridges, William. Managing Transitions Making the Most of Change. Massachusetts, Reading: Perseus Books, 1991.
- Casey, Eoghan. Digital Evidence and Computer Crime. Great Britain, Cambridge: Academic Press, Cambridge University Press, 2000.
- Cha, Ariana Eunjung. "Hackers Feast On Complacency." The Washington Post, 9 March 2001. Internet. <<http://www.washingtonpost.com/wp-dyn/articles/A43993-2001Mar8.html>>. Accessed: 15 March 2001.
- Chen, Anne. "Digital detectives track hacks." ZD Net News. 22 April 2001. Internet. <<http://www.zdnet.com/zdnn/stories/news/0,4586,2708810,00>>. Accessed: 30 April 2001.
- Christensen, John. "Bracing for guerrilla warfare in cyberspace." CNN Interactive, 6 April 1999. Internet. <<http://www.cnn.com/TECH/specials/hackers/cyberterror>>. Accessed: 16 April 2001.
- Claburn, Thomas. "Fear of a Hacked Planet, A new cure for cybercrime may be worse than the disease." MSN Computing Central. 11 April 2001. Internet. <<http://msn.zdnet.com/msn/zdnet/story/0,12461,2701068-hud00025hm3,00.html>>. Accessed: 13 April 2001.

-
- Coronado, Ramon. "Woods ID thief gets 200-to-life." Sacramento Bee. 28 April 2001. Internet. <http://www.sacbee.com/news/news/local07_20010428.html>. Accessed: 28 April 2001.
- Cowley, Brian. "The Man Who Changed Everyone's Life – The Ubiquitous Ideas of F.A. Hayek." Internet. <http://www.iedm.org/home_en.html>
- Crouch, Cameron. "Experts ponder securing the wireless world." CCN.com. 13 April 2001. Internet. <<http://www.ccn.com/2001/TECH/industry/04/13/wireless.security.idg/index.html>>. Accessed: 16 April 2001.
- Esensten, Tom. Lecture entitled, "Strategic Planning." Organizational Effectiveness Consulting, n.d.
- Evans, Arian. "The Great Hack Attack, Or why the weakest link in security is always human neglect." Arstechnica. 15 March 2001. Internet. <<http://www.arstechnica.com/wankerdesk/01q1/greathack-1.html>>. Accessed: 15 March 2001.
- Evans, James. "Cyber-crime laws emerge, but slowly." CCN.com. 5 July 2000. Internet. <<http://www.ccn.com/2000/TECH/computing/07/05/cyber.laws.idg>>. Accessed: 16 April 2001.
- "FBI wants more money for fighting cyber crime." SV News Services. Internet. <<http://www.ciol.com/content/news/repts/00033001.asp>>. Accessed: 16 April 2001.
- Fiery, Dennis. Secrets of a Super Hacker. Washington, Port Townsend: Loompanics Unlimited, 1994.
- "FM101-5." Staff Officer's Guide. United States Army Field Manual. 1987.
- Frank, Diane. "Companies taking over cyberalerts." Federal Computer Week. 5 April 2001. Internet. <<http://www.fcw.com/fcw/articles/2001/0402/web-Saic-04-05-01.asp>>. Accessed: 9 April 2001.
- Goodstein, Leonard, Nolan, Timothy, and Pfeiffer, J. William. Applied Strategic Planning, How to Develop a Plan That Really Works. New York: McGraw-Hill, Inc., 1993.
- Gupta, Poornima. "Study of government computers faults Security." SiliconValley.com. Gigabit Ethernet Conference and Exhibition. 5 April 2001. Internet. <http://www.siliconvalley.com/docs/news/reuters_wire/10531441.html>. Accessed: 9 April 2001.

Hall, Dennis. "Cybercrime, Logging on With a Vengeance in the Year 2000." Police. July 2000.

"Internet Crimes Against Children." OVC Bulletin. U.S. Department of Justice, Office of Justice Programs, Office for Victims of Crime. 16 May 2001. Internet. <<http://www.ojp.usdoj.gov/ovc/publications/bulletins...>>. Accessed: 16 May 2001.

Jick, Todd D. Notes entitled, "Implementing Change." Harvard Business School, 1991.

Kirby, Carrie. "Cyber Sleuths." San Francisco Chronicle, 26 February 2001, B3.

Kopelev, Sergio. "Behind the 8 ball, Agencies must get into the game and address the growing problem of white-collar crime on the Internet, because the criminals appear to be winning." Law Enforcement Technology. March 2000.

Kotter, John P. Leading Change. Massachusetts, Boston: Harvard Business School Press, 1996.

Kovacich, Dr. Gerand L. and Boni, William C. High-Technology-Crime Investigator's Handbook. Boston: Butterworth Heinemann, 2000.

Krebs, Brian. "Cyber Crime Fighters Face Legal Obstacles." Newsbytes. 24 January 2000. Internet. <<http://www.newsbytes.com/pubNews/00/142666.html>> Accessed: 16 April 2001.

Krebs, Brian. "Internet Fraud Reports Continue To Pour In – FBI." Newsbytes. Internet. <<http://www.newsbytes.com/news/01/164918.html>> Accessed: 2 May 2001.

Lewis, Glenn. "Identifying the owner of a web site." HTCIA International. High Technology Crime Investigation Association. September 2000, Vol. 1, Issue 2.

Longstreet, Wilma S. and Shane, Harold G. "Curriculum for a New Millennium." Allyn & Bacon, 1993.

MacIntosh, Nancy. "Implications and Applications of the Internet in Policing." Gazette. Vol. 62, No.1 2000.

Mahoney, D.P.A., Thomas. "Writing A Criminal Justice Research Paper." The Journal of California Law Enforcement. 10 May 1998.

Mcewan, Tom. "Cybercops, Court-defensible evidence from computer forensics." Law and Order. March 1995.

-
- McGuire, David. "Internet A Fertile Spawning Ground For Tax Scams – Senator." Newsbytes. 5 April 2001. Internet. <<http://www.newsbytes.com/news/01/164168.html>>. Accessed: 16 April 2001.
- Meeks, Brock N. "Hackers hit 155 government sites." MSNBC. Internet. <<http://www.msnbc.com/news/555308.asp>> Accessed: 9 April 2001.
- Meinel, Carolyn P. The Happy Hacker. Arizona, Show Low: American Eagle Publications, Inc., 1998.
- Menz, Mark. "One name, many addresses: The Problem of Tracing Dynamic Domain Names." HTCIA International. High Technology Crime Investigation Association. March 2001, Vol. 2, Issue 1.
- Menz, Mark and Menz, Mike. "Just what is High Technology Crime?." HTCIA International. High Technology Crime Investigation Association. September 2000, Vol. 1, Issue 2.
- Morrison, Richard D. "Cyber-Investigator-The New Detective?." Law Enforcement Technology. August 1997.
- New, William. "FBI struggles to retain cybercrime experts." GovExec.com. 5 April 2001. Internet. <<http://www.govexec.com/dailyfed/0401/040501td.html>>. Accessed: 9 April 2001.
- O'Harrow Jr., Robert. "Identify Thieves Thrive in Information Age." The Washington Post, 31 May 2001. Internet. <<http://www.washtech.com/news/regulation/10124-1.html>>. Accessed: 16 April 2001.
- Parker, Donn B. "Fighting Computer Crime: A New Framework for Protecting Information." Wiley, John & Sons Incorporated. August 1998. "Annotation." Barnes & Noble.com. Internet. <<http://rl.us.rmi.yahoo.com/rmi/http://shop.barnesandnoble.com/booksearch/isbninquiry.asp/rr...>>. Accessed: 30 March 2001.
- Paynter, Ronnie L. "Riding the Cyber Wave." Law Enforcement Technology. November 1999.
- Pfeiffer, J. William. Applied Strategic Planning. New York: McGraw-Hill, Inc, 1993.
- Pilant, Lois. "Fighting Crime in Syberspace." The Police Chief, August 1997.

-
- Power, Richard. Tangled Web, Tales of Digital Crime from the Shadows of Cyberspace. Indiana, Indianapolis: Que, 2000.
- Rasch, Mark D. "11. Criminal Law and The Internet." The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues. Computer Law Association, 1996. Internet. <<http://www.cla.org/RuhBook/chp11.html>>. Accessed: April 15, 2001.
- Robertson, Colonel Michael D. "Law Enforcement Response to Cyber-Crime." The Police Chief. January 2000
- Savage, Marcia. "Survey Shows Growing Losses From Cyber Crime." Planet IT, 24 March 2000. Internet. <http://www.planetit.com/techcenters/docs/e_business/news/PIT2000032450005>. Accessed: 16 April 2001.
- Scalione, Robert. "CRIME ON THE INTERNET: Can the Law Keep Up With a New Generation of Cyberspace Hackers?" Fall 1996. Internet. <<http://wings.buffalo.edu/Complaw/CompLawPapers/scalion.html>>. Accessed: 16 April 2001.
- Schwartau, Winn. Cybershock, Surviving Hackers, Phreakers, Identify Thieves, Internet Terrorists and Weapons of Mass Disruption. New York: Thunder's Mouth Press, 2000.
- Schwartau, Winn. Information Warfare, Cyberterrorism: Protecting Your Personal Security in the Electronic Age. 2d ed. New York: Thunder's Mouth Press, 1996.
- Senge, Peter M. The Fifth Discipline, The Art & Practice of The Learning Organization. New York: Doubleday, 1990.
- Stambaugh, Hollis et al. "State and Local Law Enforcement Needs to Combat Electronic Crime." National Institute of Justice Research in Brief, August 2000.
- Stambaugh, Hollis et al. "Electronic Crime Needs Assessment for State and Local Law Enforcement." National Institute of Justice Research Report, March 2001.
- Stephens, Gene. "Crime in Cyberspace." The Futurist, September-October 1995.
- Sterling, Bruce. The Hacker Crackdown, Law and Disorder on the Electronic Frontier. New York: Bantam Books, 1992.

-
- Stockham, Kirk. "The SCSI/LPT Duplication Process for the Problem Laptop." HTCIA International. High Technology Crime Investigation Association. March 2001, Vol. 2, Issue 1.
- Stranberg, Keith. "Cyber Crime Today." Law Enforcement Technology. April 1999.
- Streitfeld, David. "Investigators Fight Dot-com Fraud in Silicon Valley." The Washington Post. 22 April 2001. Internet. <<http://www.washtech.com/news/regulation/9213-1.html>>. Accessed: 24 April 2001.
- Sullivan, Bob. "Watch a hacker work the system." MSNBC. 27 March 2001. Internet. <<http://www.msnbc.com/news/550567.asp?cp1=1>> Accessed: 2 April 2001.
- Taylor, Paul A. Hackers. London: Routledge, 1999.
- Tewari, Vinay. "Are our cops ready to tackle cyber-crime?" The Times of India. Internet. <<http://timesofindia.com/210500/21home5.htm>>. Accessed 19 April 2001.
- Thomas, Pierre. "Governments ready to fight cyber-crime in new millennium." CCN.com. 2 January 2000. Internet. <<http://www.ccn.com/2000/TECH/computing/01/02/cyberterrorism>>. Accessed: 19 April 2001.
- Treglia, Stephan. "Obtaining Subpoenaed Information From Cable Companies." HTCIA International. High Technology Crime Investigation Association. March 2001, Vol. 2, Issue 1.
- Weinstein, Bob. "If You Can Hack It, Demand Is Great in Forensics." San Francisco Chronicle. 31 December, 2000, sec. CL, p. 15.
- Wilkinson, Lawrence. "How to Build Scenarios." Hotwired Presents, 1995.
- Williams, Wayne P. "The National Cybercrime Training Partnership." The Police Chief, February 1999.