

WHAT IMPACT WILL THE HIGH TECHNOLOGY INDUSTRY  
HAVE ON THE INVESTIGATION OF HIGH TECHNOLOGY CRIMES  
BY THE YEAR 2007?

A Project presented to  
California Commission on  
Peace Officer Standards and Training

by

Captain Donald M. O'Keefe  
San Mateo County Sheriff's Office

Command College Class XXXII

Sacramento, California

June 2002

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

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

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

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

Copyright 2002

California Commission on Peace Officer Standards and Training

## CONTENTS

---

LIST OF TABLES	iii	
ACKNOWLEDGEMENTS	iv	
Chapter I	ISSUE IDENTIFICATION	
	> Statement of the Issue	1
	> Introduction	1
	> Environmental Scanning	5
	> Interviews	11
	> Project Goal	16
	> Conclusion	17
Chapter II	FUTURES STUDY	
	> Introduction	18
	> Nominal Group Technique	18
	> Cross Impact Analysis	29
	> Scenarios	31
	> Conclusion	36
Chapter III	STRATEGIC PLANNING	
	> Introduction	37
	> Vision Statement	37
	> External Analysis	38
	> Analysis of the Organizational Culture	42
	> Identification and Analysis of Stakeholders	46
	> Development of Alternative Strategies	48
	> Implementation Plan	54
	> Conclusion	59
Chapter IV	TRANSITION MANAGEMENT	
	> Introduction	61
	> Commitment Planning	62
	> Supporting Technologies	65
	> Transition Structure	65
	> Responsibility Charting	66
	> Conclusion	67

Chapter V	SUMMARY, RECOMMENDATIONS AND CONCLUSION	
	> Summary	68
	> Recommendations	68
	> Conclusion	69
APPENDICES		
	A. Nominal Group Participants	72
	B. List of Trends	73
	C. List of Events	74
NOTES		75
BIBLIOGRAPHY		76

## LIST OF TABLES

Tables		Page
2.1	Trends	21
2.2	Events	25
2.3	Cross Impact Analysis	29
4.1	Current Commitment to Strategic Plan	62
4.2	Responsibility Chart	66

## ACKNOWLEDGEMENTS

I was able to complete this Command College Project with the support and encouragement of many people, including:

Sheriff Don Horsley  
Undersheriff Greg Munks  
Captain Mike Lanam  
The faculty and staff at POST  
My colleagues at the San Mateo County Sheriff's Office  
Fellow students in Command College Class 32  
My wife Ester, family and friends

A special "thank you" to those who participated or assisted with the NGT Panel:

Undersheriff Greg Munks  
Mr. Steve Barretta  
Mrs. Jean Whitney  
Mr. Matt Stannard  
Supervisory Special Agent Chris Woiwode  
Mr. Joe Chiaramonti  
Commander Rich Cinfio  
Deputy District Attorney Jack Grandsaert  
Mr. Charles Robinson  
Captain Russ Nicolopoulos  
Sergeant Lisa Williams

## **CHAPTER ONE**

### **ISSUE IDENTIFICATION**

#### Statement of the Issue

The research for this project seeks to answer the following question: What impact will the high technology industry have on the investigation of high technology crimes by the year 2007? The high technology industry is defined as privately or publicly held corporations that develop and sell high technology products throughout the world. High technology crime is defined as those criminal acts that utilize high technology hardware and/or software to facilitate or commit a crime.

During the past several years, the high technology industry has made significant technological advances that has changed, and will continue to change, the way people of the world interact and conduct business. The importance of emerging technologies and the significance of the global information infrastructure stagger the imagination and create opportunities as well as challenges for end users and law enforcement officials. We must ask ourselves, do we control technology, or does the technology control us and how much of our civil liberties are we willing to give up for public and individual safety?

#### Introduction

Historically, law enforcement has been slow in embracing new technologies and even slower in utilizing technology to its maximum potential. There are countless examples over the years of how criminals have outgunned or outsmarted law enforcement officers due to a tactical edge created by a new technology.

For example, in the 1920s and again in the 1980s, organized crime and criminal street gangs possessed military type weapons to terrorize the public and rival crime groups while law enforcement struggled to maintain order and regain public confidence. More recently, drug traffickers and drug dealers have used computers to facilitate and conceal their transactions and records, utilized various types of technology to communicate amongst themselves and counter-surveillance technology to detect law enforcement officers. Law enforcement is slowly responding to these challenges presented by technology savvy criminals. Unfortunately, law enforcement still has a long way to go.

The technological advances achieved via the Internet, along with instant communication capabilities available through the information superhighway, will continue to tax law enforcement resources, expertise and ultimately effect the quality of criminal investigations throughout the 21<sup>st</sup> century. These trends, coupled with dwindling resources and the lack of qualified law enforcement officers in the future, present a serious challenge to law enforcement's abilities to investigate and prosecute high technology crimes.

This project examines an option for law enforcement agencies to meet the challenges on the horizon controlled by the new technologies being developed by the high technology industry during the 21<sup>st</sup> century. The only way to ensure that law enforcement stays abreast of new technologies is to forge much closer public and private partnership between law enforcement and the high technology industry.

It is true that various types of task forces already exist to address specific community related problems. Community Oriented Policing is the best example of the public and private sector coming together to address the causes of crime as stated in the broken window theory. We even have investigative task forces that use the private sector on a limited basis during the investigation of high technology, financial and other property related crimes as needed. The time has come for the high technology industry to become more involved in computer and technology related crimes.

The main reason is that most law enforcement agencies are poorly equipped and lack the expertise to properly investigate and prosecute the wide variety of high technology crimes facing American law enforcement today, and certainly in the future. When one considers that there are 18,769 local law enforcement agencies in the United States, it becomes obvious that American law enforcement currently faces significant logistical, operational, communication and technological challenges.

The high technology industry has the unique opportunity to protect its investment and at the same time provide expertise to enhance public safety and national security. Many believe that the success of the U.S. economy during the late 1990s and into the 21<sup>st</sup> century is attributable in part to the booming high technology industry, especially in the geographical region known as Silicon Valley, located in the San Francisco Bay Area. The success of the high technology industry and the emergence of new technologies will forever change the way law enforcement views its relationship with the private sector.

During a cyber crime summit hosted by the Stanford Law School in April 2000, former United States Attorney General Janet Reno stressed the need for teamwork between law enforcement and the high technology industry. Attorney General Reno said, “Solutions will not be found in any single sector, we are all victims if computer crime goes unresolved.”<sup>1</sup>

Attorney General Reno told the audience of high technology executives, prosecutors and law enforcement officials, including local, state and federal high tech investigators, that law enforcement and private industry must improve their collaboration to successfully police the Internet to prevent crimes and protect sensitive computer systems. “We do not want invasive government regulation or monitoring of the Internet. The private sector should take the lead in protecting the integrity of the computer systems.”<sup>2</sup>

This research examines the impact that the high technology industry has had on the investigation of high technology crimes, and how alternate strategies need to be developed to address law enforcement’s ability to effectively and efficiently investigate and prosecute high technology crimes in the 21<sup>st</sup> century. The data and information for this project was gathered by interviewing law enforcement officers, government officials, private sector high technology experts, prosecutors, defense attorneys, members of the press, and ordinary citizens. Additional data and information was obtained from literature scanning.

## Environmental Scanning

During the past sixty years, there has been an array of new technologies that has burst upon the world stage and helped to create a standard of living enjoyed by more people than ever before in the history of the human civilization.

Beginning in 1940, the U.S. economy was flooded with new technologies that initially were kept clandestine due to the country's involvement in the war effort. These technologies included mainframe computers, atomic energy, rockets, commercial aircraft, automobiles and television. Following World War II, these technologies were utilized for civilian use and, coupled with the creation of the World Bank and the International Monetary Fund, helped finance these new technologies. This public/private partnership resulted in a tremendous surge in the U.S. economy during the 1950s, which continued well into the 1960s. During the 1970s, the U.S. economy began to slow, which ultimately resulted in high inflation and later a world recession.<sup>3</sup>

With the end of the Cold War and subsequent cut backs in U.S. military strength, new technologies, including the Internet and personal computers, were released for public use as similar technologies were in the 1940s. This surge in technological advances, coupled with a free-market economy and the breakup of corporate giants, cleared the way for a truly global economy that continued throughout the 1990s and into the 21<sup>st</sup> century.<sup>4</sup>

Experts estimate that by 2005 the global population of Internet users will reach approximately 300 million. By 2010, 90 percent of people in the industrialized world and 50 percent of the developing countries will be online.<sup>5</sup> This future forecasting of Internet expansion, wireless technology, and user expertise during the next ten years will create

significant opportunities and as well as threats to the global economy, national security and individual privacy.

For example, in June 2001 the Intel Corporation announced that it had created the world's fastest silicon transistor that turns on and off nearly 1,000 times more quickly than those that power today's microprocessors. The technology will not be available until 2007 but will allow computers to run 215 times faster than the current top-of-the-line Pentium 4. Powerful processors as these are expected to play a key role in the growth of speech recognition and language translation applications. The most amazing part of this creation is that it will use existing technology, using standard materials, and the same kind of structure, which equates to cost savings to the consumers.<sup>6</sup>

Information technology is reshaping the logic of everything from business strategy to work to pop culture. It's also reshaping the logic of crime: what it looks like, how it takes place, and how society chooses to fight it. The nation is experiencing more identity theft, illegally obtaining credit-card numbers, social security numbers, and other types of personal information. As business and financial institutions move towards cashless transactions, electronic banking will no doubt make a person's financial life simpler, but it will also make it easier for criminals to access bank accounts. The Willie Sutton Principle still applies: "Criminals go where the money is."<sup>7</sup>

The Internet, for instance, has made cyber crime easier to commit. In July 2001, a Russian programmer was indicted on charges of violating the Digital Millennium Copyright Act of 1998, which forbids software designed to thwart copyright. The Russian programmer, Dmitry Sklyarov, helped write a computer program for ElcomSoft that strips the copy protection from electronic books made by Adobe Systems of San

Jose, making it possible to duplicate the books freely. FBI agents arrested Mr. Sklyarov when he arrived in Las Vegas to attend a hacker conference.<sup>8</sup> Even though the charges against Mr. Sklyarov were eventually dropped, this case is a good example of how far reaching cyber crime can be.

With the decline in violent street crime during the past few years and the booming economy, Americans feel safer and tend to invest more in the economy. If this trend continues, it will ultimately equate to an increase in white-collar crimes and subsequently the need for law enforcement to rethink its crime fighting priorities. Law enforcement will need to acquire and maintain adequate levels of high technology expertise, be able to secure continual funding sources to purchase high technology equipment and train its personnel. Law enforcement will also need to forge closer working relationships with the high technology industry and other local, state, national and international governmental agencies entrusted with the enforcement of high technology crimes.

The tragic events of September 11, 2001 may be the catalyst that ignites the sense of urgency in both law enforcement and the high technology industry to forge closer working relationships. For example, the recent tightening of security at U.S. airports in response to the terrorist attacks has unleashed a flood of technology designed to intercept potential terrorists before they act. Joseph Tick, who founded Jersey City, New Jersey based Visionics and eigenface, has developed a face recognition program that uses a camera and computer to identify a person in a crowd. This technology has the potential to provide law enforcement with an investigative tool that can be used for crimes other than at airports. This type of technology offers security at the expense of constant surveillance. Whether society is willing to pay that cost is yet to be determined.<sup>9</sup>

## The High Technology Industry's Role

In a 2000 survey of 276 private sector organizations, the FBI discovered that 95 percent suffered a computer intrusion and many of those reported that each incident cost an average of one million dollars.<sup>10</sup> Generally, the high technology industry has the lead responsibility in operating the global information infrastructure, security requirements, standards, design and implementation. It is of vital economic interest for businesses worldwide to cooperate with stakeholders, public and private, to provide for a secure infrastructure.<sup>11</sup>

On July 25, 2001, Senator Chuck Grassley of Iowa told the Senate Judiciary Subcommittee that “the issue of public-private cooperation has become essential to the success of the safeguarding of our national infrastructure. We cannot count on the federal government alone to protect our critical infrastructure from cyber-terrorism, because government doesn't own or operate the networks that carry most of our critical content. The extent to which there is inter-connectivity between the private sector and the government cannot be ignored. So, the private sector is not only needed, it is pivotal in this endeavor. Private industry owns 90 percent of the national infrastructure, yet our country's economic well-being, national defense and vital functions depend on the reliable operation of these system.”<sup>12</sup>

The high technology industry must do its part in the war against cyber crime. The high technology industry must share information while still protecting the privacy of others. Each high technology company should be encouraged to share non-proprietary information concerning threats, vulnerabilities, protective measures and effective information security practices. The industry should also cooperate with law enforcement

in reporting incidents of cyber crime, while respecting laws or other agreements regulating the collection, processing and disclosure of personal data.

The high technology industry should provide training and expertise to law enforcement agencies concerning the latest developments in technology. This recommendation will be a challenge any high technology company with a new business idea that radically changes the market. These companies need to weigh the public benefits of allowing law enforcement access to the inner workings of the new technology versus their desire for increased profit margins.

#### Law Enforcement's Role

Law enforcement officials have a critical role to play in preventing, detecting, investigating and prosecuting computer crime. Although the police face many competing priorities, the simple matter is that the public depends on and needs law enforcement for protection against victimization in the online world. Although there was relatively little public demand for a computer competent police force in the past, clearly that is no longer the case. During 2000, the notoriety and media coverage of virus and denial-of-service attacks have certainly increased public awareness of cyber crime. The public is concerned and frightened and is looking to the police for help and leadership.<sup>13</sup>

What can law enforcement do? Many believe that law enforcement should share more information with the private sector. This must be done with greater frequency and efficiency, specifically with respect to warnings of particular threats. The government and law enforcement must also get their house in order, by providing better internal security to deter employees from having access to confidential law enforcement

information. Last but not least, the government needs to improve its ability to detect and prosecute cyber crime. The government must continue to strengthen its own technological capabilities to investigate crime over the Internet. Additional training is needed at all levels of law enforcement to address the changing technology and levels of expertise of law enforcement investigators.<sup>14</sup>

#### Lack of Law Enforcement High Technology Expertise

Another important trend facing law enforcement agencies throughout the United States, especially in California, is the reduction in the number of qualified applicants to fill peace officer ranks. In the San Francisco Bay Area for example, the high cost of living, inability to find affordable housing in particular, coupled with the high number of retirements from the baby boomer generation, have resulted in a competitive market for qualified candidates.

For the first time ever, law enforcement agencies are actively competing for these candidates by offering good salaries and benefits, signing bonuses, attractive compensation packages, housing assistance programs and alternative work schedules. Unfortunately, the good economy has created more lucrative job opportunities in the private sector, especially in the high technology industry. Generation X'ers who have computer and technological skills are working for HP or Oracle instead of pursuing a career in law enforcement. This continuing trend has helped to reduce the number of qualified personnel who have the skills and interests to become high technology investigators.

## Interviews

The impact that the high technology industry will have on the investigation of high technology crimes is unique, in that it will affect everyone associated with the Internet and other forms of technology. The following interviews were conducted with supervisory/management personnel representing law enforcement, the high technology industry, and prosecuting attorneys.

The San Mateo County District Attorney's Office is one of several district attorneys' offices in California that have attorneys specially assigned to prosecute high technology crimes. Deputy District Attorney Jack Grandsaert is currently assigned to the High Technology Prosecution Unit that prosecutes all high technology crimes occurring within San Mateo County.

Mr. Grandsaert believes that Internet crime, such as identity theft and gray market will become the crimes of the future. Mr. Grandsaert feels that very few law enforcement investigators and prosecutors are properly equipped to handle these types of complex investigations. Mr. Grandsaert has seen a dramatic shift from prosecuting crimes of violence during the 1980s and 1990s to the more complex and frustrating high technology crimes.

In many occasions, cyber crime investigations cross several different jurisdictional boundaries resulting in complex legal issues. Law enforcement must also continue to work better with their counterparts in other states and around the world to impact cyber crime significantly. Mr. Grandsaert says that fewer than 10 percent of all high technology crimes are reported, or discovered for that matter, prosecuted, or a suspect convicted. A quick cost benefit analysis clearly indicates that cyber crime

provides the highest financial gain with the lowest chance of discovery, arrest, conviction, fine, or doing any significant jail time.

Mr. Grandsaert predicts that the greatest impact that the high technology industry will have on the investigation of high technology crimes will come from within the high technology industry itself. Mr. Grandsaert says that the high technology industry must do a better job of policing itself through internal prevention efforts and better cooperation during criminal investigations with law enforcement personnel. For example, E-Bay employs a former prosecutor and police detective specifically to assist law enforcement investigators track down cyber criminals.

The high technology industry can also assist law enforcement by providing increased access to proprietary information that each company restricts to its highest corporate officers. This will require that state and federal evidence codes be amended to protect the proprietary information from disclosure during court proceedings. Without this protection, the high technology industry will be reluctant to cooperate with law enforcement for fear that proprietary information and company secrets will become public.

Finally, Mr. Grandsaert believes that law enforcement and the prosecutors must also work together to properly investigate and prosecute high technology crimes. Mr. Grandsaert suggests that the prosecuting attorney should be brought into the investigation early on so that legal mistakes can be avoided. This collaboration will protect the rights of the defendant, the integrity of the prosecution and reduces the possibility of creating bad case law.

The next interview was conducted with Mr. Joe Chiaramonti, who is currently the Director of Security for Sun Micro Systems. Besides being a high technology security professional, Mr. Chiaramonti is also a former FBI agent and high technology crime investigator, which gives him the unique opportunity to comment on this issue from both the law enforcement and the high technology industry side.

Mr. Chiaramonti sees the impact that the high technology industry will have on the investigation of high technology crimes in many ways. Mr. Chiaramonti predicts that the larger high technology companies will step up their efforts to conduct their own preliminary investigations prior to calling in law enforcement. Some high technology companies provide security assistance to other companies based on the theory that the entire industry is ultimately affected by high technology crime. Because of the industry need for security, Mr. Chiaramonti says that there is no competition between high technology security departments. This partnership has created a closely-knit group of high technology security personnel who freely exchange information without the fear of public disclosure.

Mr. Chiaramonti points to the High Technology Crime Investigation Association (HTCIA) as the mechanism used to bring the law enforcement and the high technology industry together to address cyber crime. The HTCIA consists of law enforcement investigators, prosecutors and high technology professionals from various local, state, federal and private organizations. The HTCIA is a non-profit organization with chapters through out the United States and several foreign countries dedicated to encourage, promote and aid in the voluntary exchange of data, information, experience, ideas and knowledge relating to the investigation and security of advanced technologies.<sup>15</sup>

The area of most concern for the high technology industry is the protection of proprietary information contained in a police report. Mr. Chiaramonti says that the high technology industry would probably share more information with law enforcement if it could be guaranteed that proprietary information would not be made a matter of public record during court proceedings.

Mr. Chiaramonti gave an example of a case that is pending in federal court, which may require the disclosure of the victim company's trade secrets. The FBI received information from an informant that a Chinese engineer had downloaded the majority of the company's trade secrets and was ready to leave the country. The suspect was detained at San Francisco International Airport by the United States Customs Service and was subsequently found to be in possession of the stolen trade secrets. In this particular case, the proprietary information was estimated to be equivalent to one hundred fifty man-hours and had an approximate value of 25 million dollars.

Mr. Chiaramonti concluded by saying that the high technology industry will continue to develop new products that will require on-going training for law enforcement to stay current on the newest technologies. The high technology industry has never had a problem with providing this training to law enforcement and will continue this practice to protect their interests and the interests of the consumer.

The final interview was conducted with Supervisory Special Agent Chris Woiwode of the Federal Bureau of Investigation, currently assigned to the San Jose Field Office's High Technology Crimes Investigative Unit. Mr. Woiwode has spent almost twenty years with the FBI, serving in various specialized units before joining the High Technology Crimes Investigative Unit.

Mr. Woiwode believes that the greatest impact the high technology industry will have on the investigation of high technology crimes will be in the form of computer and other high technology related training. The high technology industry will continue to provide technical assistance such as at search warrant scenes and during trial preparation when ever possible. Mr. Woiwode sees the high technology industry taking more of a leadership role in the area of training than ever before.

Mr. Woiwode feels that the some high technology companies, especially the smaller ones, are not as cooperative as they could be when reporting incidents of high technology crimes and lack the sense of urgency when dealing with security issues. Mr. Woiwode told me that the Silicon Valley Chapter of the High Technology Investigation Association is the vehicle that brings law enforcement and the high technology industry together to freely exchange information and work cooperatively to prevent and bring cyber criminals to justice. This association has already helped to facilitate communication between the high technology industry and law enforcement, which has already resulted in a more timely reporting of cyber crime to law enforcement.

During the interview, the idea of assigning high technology investigators from private companies to high technology task forces similar to what is currently done with law enforcement officers was discussed. Mr. Woiwode felt that representatives from the high technology industry should be on the steering committee, but was skeptical about allowing private sector investigators to be part of the investigative task force. He pointed to potential conflicts of interest between the investigator's employer and the case under investigation, as well as how to control the private investigator's access to criminal records and other sensitive on-going investigations.

Finally, Mr. Woiwode saw a need for local and state law enforcement to increase the amount of high technology/computer training in the basic police academy. This approach allows law enforcement to invest in the future by providing high technology training early on in an officer's career. According to Mr. Woiwode, most law enforcement agencies are supportive of the trend towards investigating high technology crimes, but lack the expertise and experience to properly recognize and effectively investigate high technology cases.

### Project Goal

The goal of this project is to forecast the impact the high technology industry will have on the investigation of high technology crimes by the year 2007. An anticipated outcome of this project will be the development of a public sector and high technology industry partnership that goes beyond the traditional roles of the public sector and the high technology industry that can be easily developed and managed. The program can be conceivably implemented within a short period of time, monitored and adjusted as necessary to address the impact the high technology industry will have on the investigation of high technology crimes through the year 2007. Readers of this project should not expect to find an easy solution to this concern from either the public or private sector. The reader should instead see this project as providing some guidelines and examples that can be implemented within a short period of time to address the future role of the high technology industry and the investigation of high technology crimes.

## Conclusion

The information super highway and advances in other forms of computer and associated technology have created instant communication capabilities that allow a person anywhere in the world to commit a crime in the United States without even leaving their residence. These issues are further complicated when more and more of every day life and business practices become more dependent on the Internet. To adequately protect American people from crime associated with the Internet, innovative programs must be developed and implemented in a timely manner.

This chapter has focused on the need for the high technology industry to impact the investigation of high technology crimes. The influence that the high technology industry has and will have on the investigation of high technology crimes is likely to continue in the future at a much greater rate. Using environmental scanning, literature review and interviews, a definition of the problem, as well as a future projection of the issue has been presented. The following chapter will present an analysis of various trends and events, which may significantly impact this issue. In addition, these trends and events will also be examined to see how they influence each other, and look at some possible future scenarios.

## **CHAPTER TWO**

### **FUTURES STUDY**

#### Introduction

Future forecasting is used to project the future and influence positive change. Certain actions can be taken to help bring about a desired change and avoid negative change. One of the tools utilized in future forecasting is the Nominal Group Technique. The results of the Nominal Group Technique are then used in a cross-impact analysis to forecast impact of the events on trends that influence the issue. Following this, possible future scenarios are developed which relate to the impact the high technology industry will have on the investigation of high technology crimes.

#### The Nominal Group Technique

The Nominal Group Technique (NGT) is a structured group process that was used to identify and rank the major trends and events related to this specific issue. A third party usually directs the process and ensures that the information is properly memorialized. It is also used for managing participation in such processes as planning, performance improvement, and measurement. The method is effective at gaining consensus with all types and levels of participation in a wide range of settings. The NGT is a relatively simple but effective process, which is best-utilized in small groups. This process helps to negate many of the negative stereotypes of dealing with groups and individuals, which may tend to be dominated by strong personality types. It is best utilized when the meeting involves judgmental or creative decision-making.

For this project, the NGT panel consisted of eleven individuals who were selected to provide a diverse perspective on the issues surrounding the high technology industry and the investigation of high technology crimes. The NGT panel consisted of an undersheriff, police commander, police technical services manager, two reporters from local newspapers, two special agents from the Federal Bureau of Investigation (FBI) assigned to manage high technology investigative units, two security directors from the private sector high technology industry, deputy district attorney, and a defense attorney (Appendice A).

Prior to the NGT panel meeting, all of the participants received a personal briefing on the topic as well as on the Command College program. Each participant was supplied with literature on the NGT process, and definitions of trends and events. In the interest of time, each participant was also asked to list possible trends and events in advance of the panel meeting related to what impact the high technology industry will have on the investigation of high technology crimes.

On the day of the NGT process, the panel members were formally briefed on the NGT process and any outstanding questions were answered or clarified. The participants were asked to silently reflect on the issue statement followed by a round robin sharing of ideas until the panel members were exhausted of ideas. The number of trends and events were limited to adequately perform the assignment. The panel then generated forty trends and thirty events that the group identified as critical issues.

The trends and events were written down on flip charts and each one was discussed to ensure that the participants understood the statement. The group collectively combined and clarified some of the trends and events and eliminated a few after some discussion. The group rated the trends and events and ultimately identified the top ten trends and events (Appendices B and C).

### Trends

Trends are defined as a series of incidents or events taking place, which seem to indicate a direction in which a particular issue may be heading. A trend is based on the past, present and future and can be quantitative or qualitative.

The group rated the impact of the top ten trends and assigned a level of concern to them. In Table 2.1, -5 represents the amount of impact the trend had on the topic five years ago, +5 represents the amount of impact five years from now, and +10 represents the amount of impact the years from now. The Concern column represents the level of concern given to each trend by the group on a scale of 1–10 with 10 representing the highest. Table 2.1 contains the trend information collected by the NGT group.

The numerical values depicted in Table 2.1 reflect the median of the group's evaluation of the trends. The panel identified all of the trends as impacting the issue, but rated those most likely to significantly influence the issue in the future with a concern level of nine:

## Trends

	Trends	-5 Years	Today	+5 Years	+10 Years	Level of Concern
1	Need for public/private Investigative partnerships	50	100	150	200	9
2	Dependence on the Internet	30	100	200	300	9
3	Gap between criminal proficiency/resources growing faster than law enforcement's capability to investigate.	50	100	150	200	9
4	Number of high technology task forces and forensic laboratories.	20	100	150	250	9
5	Willingness to sacrifice privacy & rights for security and convenience.	15	100	150	150	7
6	Degree of difficulty in solving high technology crimes.	50	100	125	150	7
7	Threat of information and technology infrastructure sabotage.	25	100	200	250	7
8	Use of computers being used to commit a broader range of crimes.	25	100	200	300	8
9	The globalization of crime.	20	100	150	200	6
10	Technology proficient law enforcement workforce	15	100	150	200	8

**Table 2.1**

➤ **Trend 1: Need for Public/Private Investigative Partnerships**

The participants felt that the need for public/private partnerships was not as much of an issue five years ago. The group discussed the lack of law enforcement expertise and saw an increasing need for public/private investigative partnerships over the next ten years and beyond. The private sector was seen as an excellent resource for high technology training, funding and assistance with complicated high technology criminal investigations. The participants did however see a possible conflict of interest between law enforcement and the private sector in the event a major company such as Oracle or IBM were involved in criminal activity. The group felt that the impact of this trend would increase significantly over the next ten years. The group felt that the benefit to law enforcement and the community far outweighed the concerns regarding potential conflicts of interest.

➤ Trend 2: Dependence on the Internet

There was considerable discussion regarding society's future dependence on the Internet. The group felt that our dependence on the Internet would make the system and us more vulnerable to hackers, cyber criminals and terrorists. Even though the group felt that the continued development of the Internet would revolutionize the way we do business, several participants expressed concern that low-income families and non-English speaking immigrants wouldn't have the expertise and finances to use the Internet. To avoid misuse and ensure that all would have access to the Internet, the group stressed Internet security and affordability as two key elements in a successful conversion to an e-economy.

➤ Trend 3: Gap between criminal proficiency/resources growing faster than law enforcement's capability to investigate.

The group voiced professional and personal experiences regarding the difficulty in keeping up with the constant changes in technology. Most of the participants saw this trend as a major threat to law enforcement agencies and their ability to effectively investigate high technology crimes. The group reiterated the need for public/private partnerships, ongoing training for law enforcement officers and technical expertise if law enforcement is to stay ahead of the curve. The group discussed current and future technological changes such as a paperless currency system, electronic blackmail, and cyber terrorism that will require a certain level of law enforcement expertise to understand and investigate these high tech crimes. The group unanimously agreed that this trend has the potential to severely impact law enforcement's ability to investigate high tech crimes and will significantly increase over the next ten years. Unfortunately, the group agreed that law enforcement was already behind the curve.

➤ Trend 4: Number of high technology taskforces and forensic laboratories.

The group agreed that the future success and credibility of the Internet and new technologies would depend on how well law enforcement and private industry work together and share resources to reduce criminal misuses. The law enforcement participants expressed frustration with their lack of in-house personnel with the necessary expertise and experience. This frustration also includes the lack of trained personnel to conduct forensic analysis of computer systems, including hardware and software. The group saw the formation of high technology investigative task forces and regional computer forensic laboratories as essential to the success of future investigations and prosecutions. The group felt that the other challenges facing law enforcement such as 3% at 50, the dwindling applicant pool, and the high cost of living in the San Francisco Bay Area prevent law enforcement agencies from keeping trained personnel. Since no one law enforcement agency can do it all,

regional investigative task forces and forensic laboratories will become the standard in the future.

- Trend 5: Willingness to sacrifice privacy & rights for security and convenience.

One member of the group felt that the public would become more willing to sacrifice individual privacy and rights in return for increased security and convenience in conducting daily business. The group discussed how technology has made our lives easier through ATM cards etc., while at the same time making us more vulnerable to cyber criminals. The group was initially concerned about the potential consequences of this trend, but eventually agreed that Americans were unlikely to sacrifice their privacy and civil rights for security and convenience.

- Trend 6: Degree of difficulty in solving high technology crimes.

The group all agreed that the majority of law enforcement in general was finding it difficult in solving high technology crimes. The reasons given were lack of trained high technology investigators/prosecutors, the global criminal, and lack of funding needed to sustain high technology units. The group agreed that the solution to this trend was increased partnerships between law enforcement and the high technology industry on a global level.

- Trend 7: Threat of information and technology infrastructure sabotage.

The group discussed how the public and private sector is dependent on technology and the accurate information. Any sabotage to the technology infrastructure or disruption of the flow of information will adversely effect the financial stability and security of the United States. The group felt that this trend would continue to be a threat to the public and private sector for years to come.

- Trend 8: Use of computers to commit a broader range of crimes.

The group felt that this trend would continue to increase over the next ten years and present significant challenges to law enforcement and the high technology industry. Several participants felt that cyber criminals will use their ingenuity to take cyber crime to new levels. This trend equates to a broader range of cyber crimes and new ways for cyber criminals to commit and facilitate traditional crimes through the use of computers.

➤ Trend 9: The globalization crime.

The participants discussed how technology has created a new kind of criminal that can commit a crime from anywhere on the planet by simply accessing a computer. The group discussed the complex legal issues involved in investigating; arresting and prosecuting cyber criminals and how their crimes often go unchallenged by law enforcement. Even though the group felt this was a serious problem, they felt that continued international cooperation between governments and law enforcement agencies would help bring this problem under control.

➤ Trend 10: Technology proficient law enforcement workforce.

The participants discussed how the new generation of law enforcement officers would be more technology proficient as society incorporates more high technology into our daily lives. One of the participants felt that the basic police academies should spend more time instructing cadets on how to identify and investigate high technology crimes rather than traditional crimes. The group agreed that law enforcement, with assistance from the high technology industry, must immediately focus more resources on educating its workforce to keep pace with the ever-enterprising cyber criminal.

## Events

Events are different from trends in that events are singular occurrences that transpire at a specific date, time, and have a significant impact. By preparing ourselves, we have the opportunity to change or intervene in the projected event.

The group rated the impact of the top ten events and whether or not the impact would be positive or negative on the topic. Table 2.2 contains the information about events collected by NGT panel. In Table 2.2, 0 represents the year probability first exceeds zero, +5 represents the probability of the event occurring in five years, and +10 represents the likelihood of the event occurring in ten years. The impact column represents the weighted impact of the event on the topic on a scale of 1-10, with 10

representing the most impact, and the + or – column representing the panel’s impression on whether the impact will be positive or negative.

The numerical values depicted in Table 2.2 reflect the median of the group’s evaluation of the events. The panel identified all of the following events as impacting the issue statement, but rated the events most likely to significantly influence the issue in the future with an impact measured at seven or higher:

**Events**

	Events	Year > 0	+5 Years	+10 Years	Impact 1-10	+ or -
1	A license is required to access the Internet.	5	25	50	8	-
2	Massive solar flares eliminate all communication capabilities.	1	20	20	10	-
3	Virtual teaching eliminates the need for human teachers.	10	0	25	5	+
4	“X” virus destroys all private and public sector databases.	1	40	20	6	-
5	Hacker is responsible for a national utility powergrid shutdown.	1	65	50	6	-
6	Civil rights eliminated for terrorist investigations.	1	60	75	7	+
7	Web media renders print media obsolete.	8	0	35	5	+
8	United States airline industry collapses.	1	25	10	1	+
9	Public/private partnerships declared a conflict of interest.	8	0	20	7	-
10	United States borders with Mexico and Canada shutdown.	1	25	35	5	-

**Table 2.2**

- Event 1: A license is required to access the Internet.

If a license were required to access the Internet, it would allow for greater control and security of the information available on the web. For example, the licensing authority could prevent known criminals and sex offenders from accessing the Internet to commit and facilitate their crimes. When crimes did occur while using the Internet, high technology investigators could easily track the offender and immediately have access to the licensee's personal information such as that available from a driver's license today. This event would require a much closer working relationship between law enforcement and the high technology industry to ensure compliance and prevent the misuse of a person's personal information. However, the panel felt that this event would have a negative impact on the high technology industry and Internet users in general.

- Event 2: Massive solar flares eliminate all communication capabilities.

This event, if it occurred, would have disastrous consequences for all nations throughout the world. This event, ultimately causing worldwide chaos, would impact every business, governmental agency and person on this planet. The group discussed the impact of not having any form of telephone service, television, computer, or radio capabilities. Several of the participants reflected on how their personal and professional lives depended on their ability to communicate effectively and efficiently. The loss of all communication capabilities would have a significant impact on high technology crimes. Since criminals wouldn't be able to commit cyber type crimes, they would revert back to traditional crimes such as robbery, burglary, and extortion for their livelihood. Without communication capabilities, law enforcement would be unable to prevent crimes and ineffective in solving any type of criminal activity. Law enforcement would be totally dependent on the high technology industry to resume communication capabilities or develop a suitable alternative.

- Event 3: Virtual teaching eliminates the need for human teachers.

The group saw this event as having a positive impact on the issue and a real opportunity for the high technology industry to provide innovative training to the law enforcement community. Even though the human element in education is always important, virtual teaching methods will allow more law enforcement officers to receive high technology training without leaving their departments. The group felt that the quality of training would increase and training costs would decrease over time, since officers would not have to travel outside their jurisdictions to receive the training.

- Event 4: “X” virus destroys all private and public sector databases.

The participants considered this event and decided that future breakthroughs in technology could make this event a reality. With the public and private sector using the Internet more to conduct business, the possibility of viruses will increase. Both the public and private sector depends on databases to conduct daily business and maintain records. If these databases were destroyed, law enforcement and the high technology industry would be unable to prevent or effectively investigate cyber crime. This event, if it occurs, would cause havoc on a global level. Even though the probability was high the first five years, the group felt that it would decrease in the next ten years due to closer public/private partnerships.

- Event 5: Hacker is responsible for a national utility powergrid shutdown.

The group discussed this event at length and felt that this event would be a very attractive target to terrorists and hackers alike. This event would be a serious threat to our economic and national security. Threats such as a national powergrid shutdown reinforce the need for public and private sector partnerships to prevent these occurrences before they happen.

- Event 6: Civil rights eliminated for terrorist investigations.

This event generated considerable discussion within the group since the terrorist attack on September 11, 2001. The participants spoke of how the events of September 11<sup>th</sup> have changed the way we all view our personal safety as well as the security of our country. The continued threat of terrorist attacks and biological warfare have changed the way some people think about civil rights and constitutional protections. Some members thought that these extraordinary times required extraordinary measures to ensure the security of our citizens and country. These panel members felt that it was permissible to eliminate civil rights in terrorist cases if we could prevent an attack similar to the one on September 11<sup>th</sup>. Other panel members thought that any elimination of civil rights, even to prevent terrorist attacks, would be the first step in eroding the core values of the American Constitution. They felt that the government would ultimately abuse their new powers and use the terrorist exemption to expand their authority into the investigation of traditional crimes. The elimination of civil rights for terrorist investigations would increase law enforcement’s ability to secure evidence against terrorist groups, resulting in more arrests, save human lives, and reduce property damage. The group agreed that the events of September 11<sup>th</sup> had an everlasting impact on their lives, and in some cases, dramatically changed the way they view the justice system.

- Event 7: Web media renders print media obsolete.

The panel felt that this event would provide more information to the public than is currently available through the print media. However, several participants expressed concern that low income and non-English speaking persons wouldn't have access to the Internet and wouldn't be able to take advantage of this new technology. There would be a significant number of people who both the public and private sector couldn't reach that would ultimately lead to a discriminatory delivery of information to the public.

- Event 8: United States airline industry collapses.

The group discussed this event and felt that it was highly unlikely that the entire United States airline industry would collapse. If severe economic times resulted in airlines filing bankruptcy, the panel felt that the United States government would nationalize the airline industry to prevent any major disruptions in air travel. However, the group indicated that a government takeover of the airline industry might be in the best interests of the American people.

- Event 9: Public/private partnerships declared a conflict of interest.

The panel felt that this event was highly unlikely and predicted that the contrary would occur. The participants all agreed that public/private partnerships would be the norm in the future and discounted any court decision that would eliminate this practice.

- Event 10: United States borders with Mexico and Canada shutdown.

The panel discussed this event and felt that closing the Canadian and Mexican borders had benefits in controlling the flow of illegal drugs and immigration, but would adversely affect trade with other nations, including international tourism. Law enforcement and the high technology industry would ultimately sever critical partnerships with other nations dedicated to preventing and investigating cyber crime. This event would take the United States back to the days of isolationism and possibly cause global economic and political instability.

## Cross Impact Analysis

Following the NGT process, a cross-impact analysis was completed by Lieutenant Glenn Nielsen of the Atherton Police Department and myself to illustrate the impact of the events on the various trends. Table 2.3 reflects the ten trends and events on a scale of one to five, with five representing the highest impact and one representing the lowest impact upon the topic. Additionally, the impact is presented as having either a positive or negative influence upon the topic. The results are used to identify the trends and events that are most likely to affect the problem statement favorably.

### CROSS IMPACT ANALYSIS

	<b>Trends</b>									
<b>Events</b>	T-1	T-2	T-3	T-4	T-5	T-6	T-7	T-8	T-9	T-10
E-1	+1	+3	+3	0	+4	0	0	+2	+1	0
E-2	+3	-3	0	0	0	-2	0	+2	+3	-3
E-3	0	-3	0	0	0	0	0	0	0	-2
E-4	+5	-3	+2	+3	0	+3	-3	-2	+3	-2
E-5	+3	-1	+1	+3	+3	+1	-3	-1	-1	0
E-6	0	0	+4	0	+3	+3	+3	+3	+3	0
E-7	0	+3	0	0	-1	0	-3	-1	0	0
E-8	+3	0	0	0	0	0	0	0	0	0
E-9	-5	-3	-3	+3	0	-4	-2	-2	-2	-3
E-10	0	+2	0	0	+1	0	0	0	0	0

**Table 2.3**

Discussed below are the influences that selected events have upon selected trends where the impact was rated 4 or higher upon the issue statement.

- 1) E4 – “X” virus destroys all private and public sector databases. +5  
T1 – Development of public/private sector partnerships.

The results of the cross impact analysis indicate that the introduction of an “X” virus that destroyed all private/public sector databases would have a significant impact on the development of public/private sector partnerships. The theory being that a catastrophic event such as an “X” virus would cause such turmoil that the event would force the public and private sector to work closer together for its own survival. Sometimes it takes a catastrophe for people or organizations to see the need to work together for a common goal. Even though the event itself would be devastating, the rebuilding stage would have a very positive effect on the impact the high technology industry would have on the investigation of high technology crimes.

- 2) E9 – Public/private partnerships declared a conflict of interest. -5  
T1 – Development of public/private sector partnerships.

The results of the cross impact analysis indicate that if private/public partnerships were declared a conflict of interest, investigative partnerships between the private and public sectors would terminate. This event would have a significant negative impact on law enforcement’s ability to prevent and solve high technology crimes. The results would cause severe economic conditions not only in the United States, but also throughout the world. The formation of private and public investigative partnerships is the only way law enforcement can keep up with the high technology criminal.

- 3) E1 – A license is required to access the Internet. +4  
T5 – Sacrifice privacy & rights for security and convenience.

The results of the cross impact analysis indicate that requiring Internet users to obtain a license would have a significant effect on an individual’s privacy and civil rights. The licensing and policing of the Internet could reduce the number of criminal acts being perpetrated and facilitated via the Internet. Ever since the terrorist attacks on September 11, 2001, Americans are reconsidering their stance on privacy and civil rights for greater security and convenience in this age of information technology. This event would have a significant impact on how the high technology industry influences the investigation of high technology crimes.

- 4) E6 – Civil rights eliminated for terrorist investigations. +4  
T3 – Criminal proficiency /resources growing faster than law enforcement’s capability to investigate.

The results of the cross impact analysis indicate that if civil rights were eliminated for terrorist investigations, then law enforcement would be better able to prevent and respond to terrorist threats that utilize high technology communications systems such as the Internet and wireless technology. Even though this event was seen as having several advantages for law enforcement, especially since the terrorist attacks on September 11, 2001, the group cautioned that any elimination of civil rights for whatever reason could have severe implications for our country. The elimination of civil rights in terrorist cases would allow the private sector to provide unlimited information to law enforcement in a more timely manner and without the need for a court order. This event would have a significant impact on how the high technology industry interacts and influences the investigation of high technology crimes.

- 5) E9 – Public/private partnerships declared a conflict of interest. -4  
T6 – Difficulty in solving high technology crimes

The results of the cross impact analysis indicate that any legislation that would prohibit private sector cooperation with law enforcement would significantly impact law enforcement’s ability to maintain investigative expertise. Recent research suggests that the private sector will take a more active role in providing law enforcement with the latest training and technical assistance. The loss of any private sector involvement will adversely affect law enforcement’s ability to investigate high technology crimes.

### Scenarios

Scenarios are developed based on input from the Nominal Group Technique, literature search and environmental scanning, and are used to forecast alternative futures and are essentially future stories. Once scenarios are identified, strategic planning can be undertaken to plan for and influence the projected future desired outcomes. The three scenarios presented describe pessimistic, optimistic, and normative perspectives.

## Normative Scenario

It is now 2007; Ken has seen law enforcement come a long way since the ABC Police Department in 1985 first hired him. Some of the newer officers still don't believe him when he first got hired, ken wrote all his reports by hand, and only used a typewriter when he had to write a memorandum to the Sergeant, usually to request vacation or because he was in trouble. The newer officers find it hard to understand how any police officer could do his job without computers, mobile data terminals, and handheld devices that allow an investigator access to every criminal justice database at the press of a button. Ken was one of the few officers early on that envisioned that high technology could be used to solve crimes and save lives.

Ken has always been a strong supporter of private/public partnerships in the investigation of high technology crimes, but has never been able to get his superiors to embrace the concept. Ken is concerned that ABC Police Department only has a handful of officers who can investigate high technology crimes and is afraid that the department will not identify future high technology investigators and will someday lose a high profile case due to poor investigation. Ken has developed several close-working relationships with his counterparts in the private sector and senses their frustrations. Most are former law enforcement officers who are either retired or left the police department for better salary and benefits in the private sector. These former law enforcement officers see on a daily basis the staggering losses their employers are taking because of high technology crimes and are frustrated by law enforcement's inability to keep up with the technology or seek private sector assistance for training or technical support.

It is now two years later and Ken has promoted to Sergeant and is assigned to night watch patrol. He is stunned to read in the local newspaper that a jury acquitted an alleged serial Internet pedophile due to sloppy investigative work by the ABC Police Department. Ken calls his old partner, Dave, who is now the Detective Bureau Commander to find out what happened. Dave explains that since both he and Ken left the Detective Bureau, the other trained high technology investigators have either retired or taken more lucrative jobs in the private sector. In addition, no one has shown any interest in investigating high technology crimes, which has resulted in a tremendous loss of expertise and respect in the criminal justice community.

#### Optimistic Scenario

It's now 2012; Ken and Dave are pleased to see that their hard work has finally paid off. The ABC Police Department is seen as a leader in the investigation of high technology crimes and has had several successful prosecutions for identify theft, corporate intellectual theft, and cyber terrorism. Because of the ABC Police Department's efforts in forging a unique private/public investigative partnership, several other law enforcement agencies in the region have also created their own partnerships with the private sector.

Based on Ken and Dave's vision, the larger computer firms have formed a task force to address the investigative limitations of law enforcement agencies in California. This task force consists of the high technology industry, regular citizens, the American Civil Liberties Union, prosecutors, and law enforcement. The Task force has been instrumental in identifying training, equipment, and technical needs of prosecutors and

law enforcement investigators at all phases of the case. This partnership has resulted in extensive training for law enforcement investigators and has allowed them to procure the latest high technology equipment and to develop their expertise before the technology is sold to the public.

Within four years, this private/public law enforcement partnership has now spread throughout the United States and has helped to reduce high technology and associated crimes by 50 percent! Because of the grass roots effort that was begun in California by Ken and Dave at the ABC Police Department five years ago, cyber criminals find it hard to commit their crimes successfully. The borders that have prevented effective law enforcement in the past have been taken down and created better economic stability throughout the United States. The rest of the world has seen what the United States has achieved and the ABC Police Department now offers high technology law enforcement training to foreign law enforcement officers.

#### Pessimistic Ending

It's now 2009 and after two years of trying to convince the chief of the need to work closer with the high technology industry, Ken and Dave are finally successful. They ultimately established a task force to determine their needs and address any concerns. Ken and Dave follow the Nominal Group Technique that Dave learned at the POST Command College to determine trends and events that may impact these types of private/public partnerships. The task force consists of the high technology industry, law enforcement, prosecutors, and members of the public. The task force identifies several critical areas that are limiting law enforcement from successfully investigating high

technology crimes. The task force determines that when a high technology crime occurs, the victim Computer Company will make their personnel and other resources available at no cost to the police agency.

After only six months, the ABC Police Department has investigated several high technology crimes, and with the unlimited assistance of the victim companies, all the cases have resulted in convictions. The ABC Police Department is now gaining national recognition for their collaborative approach to crime solving. Unfortunately, the American Civil Liberties Union (ACLU) has filed a lawsuit in federal court alleging that the ABC Police Department has violated the civil rights of several defendants and has misused the information provided to them by the high technology industry. To complicate matters, the media learns that Dave accepted a free trip paid by MBI Computer Company for his excellent work during a complicated investigation. The chief is under criticism again and several high technology companies are worried that they will be sued as well and fear that the negative publicity will affect their profit margins.

The situation is not good for the ABC Police Department and the private/public partnership is now in jeopardy. The department scrambles to gain public support for the collaboration and hope they intervene on the department's behalf. The task force meets with the ACLU, but cannot come to an agreement on how to develop the necessary checks and balances to ensure that police tactics don't violate the public's civil rights. The inclusion of the ACLU in the process has caused some confusion about the issue and the private/public partnership is tenuous. The media is brought in towards the end of the process, but its stories just create more confusion, as different opinions of civil and constitutional issues are argued amongst the proponents and opponents.

## Conclusion

The Nominal Group Technique has been instrumental in identifying trends and events that are likely to have a significant impact on the issue of what impact the high technology industry will have on the investigation of high technology crimes by the year 2007. The feedback received from the Nominal Group Technique suggests that public/private partnerships in the investigation of high technology crimes were imperative to future law enforcement success of cyber crime.

During the group discussions, the participants overwhelmingly agreed that high technology's impact on the investigation of high technology crimes would come in the form of public/private partnerships. The participants specifically felt that this partnership would be in the form of a multi-agency public/private investigative task force. The three scenarios presented possible alternatives of law enforcement will address this issue. The Nominal Group Technique and the scenarios can be looked upon as law enforcement's mapping for the future.

The next chapter will focus on developing a strategic plan to help facilitate and manage a desirable future for the organization and individuals. The information obtained from environmental scanning and the Nominal Group Technique will be used to set a course of action for where the organization wants to go and how it will get there.

## **CHAPTER THREE**

### **STRATEGIC PLAN**

#### Introduction

A strategic plan utilizes a structured approach to address issues of concern. The purpose of a strategic plan is to help facilitate and manage a desirable future for the organization and individuals. Considering identified trends and events that have potential to impact the issue is critical to the development of a solid strategic plan. The persons responsible for the design and implementation of the plan must look for opportunities to influence the future and bring about positive change. Strategic planning seeks to bring about those trends and events that have a positive impact on the issue and prevent the trends and events that affect the issue negatively.

Law enforcement will need a strategic plan to successfully implement a public/private partnership for the investigation of high technology crimes. The following strategic plan includes information from environmental scanning as well as the Nominal Group Technique process.

#### Vision Statement

In order to achieve the desired goal and to keep those involved focused on the process, it is essential that a vision statement be developed. The vision statement must reflect the values and core objectives of the organization and it can be used to set a course of action for where the organization wants to go and how it will get there. The following is an example of such a vision statement:

It is recognized that law enforcement's primary responsibility is to provide for the safety and security of the community it serves. Together, the high technology industry, the end users, and law enforcement form a unique community that has revolutionized the way we communicate and conduct our daily business. To that end, law enforcement is committed to working cooperatively with this community to prevent and investigate cybercrime whenever possible without violating the civil rights of others.

The goal of this project is to establish a road map for law enforcement agencies to interact effectively as equals with the high technology industry and prevent high technology crimes. This means bringing the best and brightest from both law enforcement and the high technology industry together to assist with implementing new strategies.

The desired outcome of this plan will result in less cyber crime and an increase in the public's confidence in using the Internet and other related technology to enhance the quality of life. None of this will occur if cyber criminals are allowed to infect the Internet with viruses, steal our identity or life savings, molest our children, or terrorize our country. The only way society will take full advantage of the current and future benefits of high technology will be through a well-designed and implemented public/private partnership strategy.

### External Analysis

Navigating through significant changes requires analysis of various factors affecting change. One method is the STEEP model. The STEEP model examines the proposed change from five perspectives external to the organization that may influence the desired change: Social, Technological, Economic, Environmental and Political.<sup>16</sup> The results of the STEEP analysis can have a significant influence on the strategy to

implement a program forming a high technology public/private partnership to investigate high technology crimes. Some of the issues to consider when implementing a high technology public/private partnership include:

### Social

- Confidentiality for computer users (Opportunity).

Americans have an intense desire for confidentiality and privacy in their every day lives. This is also the case in the cyber community where personal information can be accessed and misused without much expertise.

- Information overload (Threat).

The constant change in technology has created a new term in our culture called information overload. People have access to more information faster than ever before in the history of mankind. Having the ability to access information at their fingertips creates both opportunities and threats and must be managed accordingly.

- The changing role of law enforcement (Threat).

Historically, law enforcement has concentrated heavily on being visible to the community to prevent crime. The information age has challenged law enforcement to meet the new threat, cyber crime.

- Crime information and trends more accessible to citizens (Threat).

The Internet has created a vehicle for citizens to access crime information and trends from their homes and businesses. A better-informed community requires that law enforcement be more responsive to community needs than ever before.

- Jobs exceed labor force (Threat).

Private sector employers will target public employees with attractive compensation packages including stock options. Law enforcement officers are more willing to change departments for better pay, cost of living and housing opportunities and no longer have loyalty to one organization.

## Technological

➤ Access to technology (Threat).

The more technology dependent society becomes, the more important it is that all persons have equal access to the technology. Failure to provide equal access to the technology will ultimately widen the gap between the haves and have-nots.

➤ Accessibility of encryption (Threat).

The ability to encrypt information can greatly reduce the possibility that the information /data can be corrupted or misused. On the other hand, encryption can be used by the criminal element to thwart law enforcement investigations.

➤ Technologically proficient law enforcement workforce (Weakness).

The information and technology age has resulted in the need for more technologically proficient law enforcement officers than ever before. The global criminal respects no boundaries and is a threat to American law enforcement from any geographical location on the earth.

➤ Creation of high technology task forces and regional forensic laboratories (Opportunity).

Law enforcement has known for some time that no one agency (local, state, or federal) has the personnel, expertise, or resources to investigate multi-jurisdictional crimes on its own. The formation of high technology task forces and regional forensic laboratories will become more important in the 21<sup>st</sup> century.

➤ Threat of information and technology infrastructure sabotage (Threat).

With the increased dependence on the Internet and new technology, infrastructure sabotage will become the number one threat to domestic and national security. It would be difficult to find one public or private organization that doesn't depend on information and technology to conduct its daily business.

## Environmental

➤ Increasing population (Threat).

A larger population equates to increased demands for law enforcement services, including the potential for more complex high technology crimes.

- Diverse community (Threat).

A more diverse community requires that law enforcement be sensitive to the needs of all ethnic and racial groups. The lack of trained law enforcement officers that know the language and culture of the community will effect the level of services rendered.

### Economic

- Change in growth and reliance on E-commerce (Threat).

E-commerce is steadily growing and will in time eliminate the need for currency and coins. This radical change in the manner in which we purchase goods and services will require that law enforcement and the high technology industry work closer than ever before.

- Impact of a strong economy (Opportunity).

A strong economy will increase the availability and purchase power for technology related items.

- Incentives needed to retain experienced personnel (Weakness).

Experienced law enforcement high technology investigators will look closer at private sector jobs due to attractive compensation packages and flexible work hours.

### Political

- Shifting of law enforcement resources (Threat).

The explosion of high technology crimes has resulted in some state and federal funding for high technology investigative units. Dwindling funding sources may force law enforcement officials to shift their focus from addressing quality of life issues to fighting cyber crime.

- Federal government's interest in cyber crime (Opportunity).

The federal government (via the Justice Department) has challenged the high technology industry to work closer with local, state and federal law enforcement agencies to help prevent cyber crime.

- Relaxing government restrictions on privacy and civil rights issues (Threat).

The impact of cyber crime and cyber-terrorism has many persons calling for fewer restrictions on law enforcement while tracking down these criminals. The argument for fewer restrictions say that it will catch more criminals and save lives. Opponents say that it will erode the constitution and draw the United States closer to a police state.

- Public awareness of high technology crimes (Opportunity).

The media and the general public have increased awareness of the impact of high technology crimes on society. This awareness may result in public sympathy and mandates to develop public/private partnerships.

### Analysis of the Organizational Culture

Every organization, whether public or private, must regularly examine itself with as much objectivity as possible to determine its health and to better plan for change. Prior to developing and instituting any change in an organization, a look at how the members are likely to accept that change, and whether or not they will support or hinder the change is essential. One method that can be utilized for such an analysis of a planned change is WOTS UP: a weakness, opportunities, threats, and strengths underlying planning model. Using this model, the following is an analysis of issues likely to impact change from inside a typical law enforcement organization:

#### Weaknesses – Objections to public/private sector partnerships

- Insufficient support from within the organization, law enforcement community, or high technology industry.

No sense of urgency may exist within the organization, law enforcement community, or high technology industry to support this partnership.

- Insufficient political support within the organization.

No sense of urgency may exist by those political figures ultimately responsible for approving the partnership.

- Insufficient funding for law enforcement.

Even though this concept may gain approval by all involved, insufficient public funds may be available to finance law enforcement's segment of the partnership.

- Reluctance on the part of law enforcement and/or the high technology industry to exchange critical information.

Law enforcement and/or the high technology industry may have the all the intentions of cooperating at the start of the partnership, but events may cause either party to be selective on what information is passed between both parties. This holding back of information may be due to conflicts with other ongoing criminal cases or the divulgence of industry/trade secrets.

- The lack of trained high technology law enforcement personnel.

Law enforcement agencies all over the country are having trouble recruiting and retaining qualified law enforcement officers. In addition, some agencies are even having trouble getting officers to request high technology investigative assignments. If this trend continues, some law enforcement agencies may bear the brunt of staffing high technology task forces.

Opportunities – potential benefits to public/private investigative partnerships.

- Increased number of criminal prosecutions and convictions of cyber criminals.

A well-designed and implemented public/private sector partnership will ultimately result in more prosecutions and convictions of cyber criminals.

- Improved public confidence in law enforcement.

With the help of the high technology industry, the public will reap the benefits of this collaboration by an economic resurgence based on the continued high technology boom and an increased sense of public safety in cyber space.

- The ability of the high technology industry to learn from law enforcement.

The most cost-effective way of investigating cyber crime (or any crime for that matter) is to prevent cyber crime before it happens. The high technology industry can learn from law enforcement's experience with community policing to prevent cyber crime before it occurs instead of concentrating on the bottom line and permitting the practice of acceptable losses.

- Lower private sector losses will result in lower costs to the consumer.

Someone will ultimately pay the price for cyber crime. That dubious honor usually rests with the consumer through higher costs of the product. That why it's in the consumer's our best interests to support strategies that work to prevent cyber crime to ensure that all ethnic and racial groups have affordable access to high technology.

Threats – potential adversity than can threaten the plan.

- Legal Action by American Civil Liberties Union or other groups concerned about “big brothers” easy access to private sector information.

The desired outcome of any collaborative effort is the free exchange of information and expertise. There is always a possibility that law enforcement officers or members of the high technology industry will provide the other with sensitive or confidential information regarding others that can or will be misused.

- Law enforcement executives and/or governmental officials unwilling to adopt the plan.

Should law enforcement or other governmental officials refuse to participate in this plan, implementation is doomed from the start. The high technology industry will see move as an example of the government's lack of commitment to addressing cyber crime.

- Lack of interest or commitment from law enforcement or the high technology industry line staff.

The plan will struggle or fail if the people actually doing the work the lack interest or commitment to see the vision through.

- Shift in law enforcement priorities.

If law enforcement priorities change, law enforcement might re-think its commitment to the high technology industry. The success of this collaboration requires that both parties maintain their commitment to the vision.

- The lure of the high technology industry fades.

For the past several years, the high technology industry has attracted the best and brightest people to the business. A significant change in job opportunities or economic conditions may result in the loss of qualified private sector personnel.

Strengths – support of the program.

- Similar collaborative efforts have been implemented in the past.

The concepts of collaborative public/private sector efforts have been successful in the past. Community policing strategies have utilized public/private sector collaborative efforts in the past to address quality of life issues in local neighborhoods. The success of these programs in the past will help promote this plan.

- Utilizing the skills of the Generation X law enforcement officers.

The majority of the law enforcement investigators who will be involved in this plan will undoubtedly be Generation X'ers. These individuals will be able to adapt to the non-traditional law enforcement role and utilize their intelligence and technical skills to the fullest.

- Save taxpayer money.

Private/public sector partnerships will ultimately save taxpayer money, which will help make the plan cost effective in the public's mind. The money saved from cyber crime can be used to fund other public and private programs intended to benefit society.

- Allow law enforcement to take a proactive versus reactive role with cybercrime.

Law enforcement and the high technology industry will in time be so successful in their partnership, that they will ultimately spend more time on preventing cybercrime than investigating violations of cyber laws.

- The ability to share public/private investigative resources and expertise.

The benefit of any partnership or task force is the ability to share resources and expertise. No one law enforcement or high technology company has all the knowledge and expertise to produce their product or provide a certain service by themselves.

## Identification and Analysis of Stakeholders

To increase the opportunity for the plan to be successful, the identification of key individuals and groups and their stake in the plan is necessary. These stakeholders are individuals or groups who can impact the plan, or who might be impacted by it. The stakeholders may be either internal or external to the organization and to varying degrees have influence on the implementation of the plan. Some stakeholders can be described as emerging, in that their influence upon the implementation of the plan is either minimal or anticipated at a later time. The successful implementation of this or any plan is dependent upon the stakeholders' ability to work collaboratively.

The persons charged with implementing the plan must recognize the roles that the stakeholders play. The stakeholders may support the change, or be opposed, and there may be a sampling of both intertwined within each stakeholder group. Those attempting to implement change must work to maintain the support of those stakeholders who favor the process, and work to gain the support or develop a plan that incorporates the positions of those opposed to the plan. The stakeholders involved in developing a partnership between law enforcement and the high technology industry along with their respective roles are listed below:

### Local, State, and Federal Elected Governmental Officials

- Critical to full buy-in of plan and providing the necessary funding.
- Dedicate the necessary resources to form the public/private partnership.
- Provides political support for plan when needed.
- Recognizes the need for public/private partnerships to investigate high technology crimes.

### High Technology Industry Executive Management Team

- Critical to full buy-in of plan and long-term financial support of costs associates of program.
- Recognizes the social, political and economic costs of cybercrime.
- Permits the sharing of sensitive intellectual information.
- Committed to providing quality and affordable high technology products.
- Dedicates the necessary resources to form the private/public partnership.

### High Technology Industry Technical and Security Personnel

- Provide the necessary technical support to law enforcement.
- Work cooperatively with law enforcement during investigations.
- Assist with policing the high technology industry from inside.
- Encourage prevention within the high technology industry.
- Liaison with counterparts in the law enforcement community.

### Local, State, and Federal Law Enforcement Administrators

- Critical to full buy-in of plan and providing the necessary funding.
- Dedicate the necessary resources to form public/private partnerships.
- Monitor progress of the program and make any necessary changes.
- Liaison with counterparts in the high technology industry.

### Local, State, and Federal Law Enforcement Supervisors and Investigators assigned to High Technology Crime.

- Perform the day-to-day case investigations.
- Critical to the buy-in of the plan.
- Suggest changes and modifications to existing program.
- Recruit law enforcement investigators for future positions.

- Liaison with counterparts in the high technology industry.

#### High Technology Regional Steering Committee (public/private sector partnership)

- Responsible for program design and meeting goals and objectives.
- Responsible for establishing policy and procedures.
- Responsible for the most efficient use of personnel, resources and funding.
- Responsible the operational effectiveness of the program.

#### High Technology User/Community

- Daily user/consumer of high technology services.
- Provide positive and negative feedback to the high technology industry and law enforcement regarding safeguards imposed on the community.
- Supportive of new programs designed to make technology safe and available for all.
- Opposed to increased taxes and expenses of government services.
- Concerned with privacy and constitutional issues.

### Development of Alternative Strategies

As part of any strategic plan, the development of alternatives is often prudent.

Three alternative strategies have been developed to address the problems associated with instituting high technology public/private partnerships.

#### Alternative Strategy I: Remain with the Status Quo

The simplest course of action to address the issue of how to implement a partnership between the high technology industry and law enforcement is to do nothing and continue with our current practices. Although this is a realistic alternative, this strategy offers nothing to address the issue of public/private partnerships. In fact,

agencies that don't participate in public/private high technology investigative partnerships in the future will mostly see their investigations suffer, resulting in cyber criminals being acquitted or not being charged at all. The reality is that poorly investigated high technology cases will soon draw the attention of judges, prosecutors, and defense attorneys, which cause significant negative exposure to the law enforcement agency. When public/private investigative partnerships become the industry standard, agencies not buying into this concept will suffer the consequences.

#### Alternative Strategy II: Increased Level of Participation

Another alternative is to informally participate in a public/private investigative partnership on a limited basis. This partnership may consist of combining investigative personnel or utilizing a regional forensic high technology laboratory on a case-by-case basis. Even though this form of task forcing has resulted in countless successful prosecutions, they lack the full-time commitment that is needed to address the growing number and variations of cyber crime effectively. The major problem with this alternative is that smaller law enforcement agencies may only investigate cyber type crimes two to three times per year. At this rate, a high technology investigator would never gain the necessary experience and/or expertise to investigate a cyber crime effectively.

#### Alternative Strategy III: Proposed Public/Private High Tech. Investigative Task Force

Developing a public/private high technology investigative task force is a significant undertaking for any governmental agency or even for the high technology

industry. The purpose of the program is to bring together the best and brightest from both law enforcement and the high technology industry to investigate and prosecute cyber criminals. This proposal is intended to take the task force concept that is currently used extensively in the public safety community to new and higher levels. This program will undoubtedly test the commitment and trust that the public and private sector must have to make this partnership successful.

The task force would consist of law enforcement officers from local, state and federal law enforcement agencies. The Federal Bureau of Investigation (FBI) would be designated as the lead agency due to its nationwide jurisdiction and extensive financial and technological resources. The local and state law enforcement officers assigned to the task force would be cross-designated as federal officers to allow them peace officer status anywhere in the United States. The state prosecutors would be cross-designated as United States Attorneys to assist their federal counterparts with vertical prosecution. The private sector representatives would be assigned to the task force as civilian analysts and would not have any peace officer powers or access to restricted law enforcement information. The private sector investigators and technicians/analysts would provide logistical, technological and high technology security assistance.

The bulk of the task force personnel would come from local and state law enforcement officers employed by police agencies from two contiguous counties. This particular kind of task force formation builds upon already established law enforcement relationships and creates a manageable infrastructure. The task force would operate out of a facility that meets the federal guidelines for sending and receiving sensitive and top secret information. This facility would house the various investigators, prosecutors and a

computer forensic laboratory to investigate complex high technology crimes. Each member of the task force would remain an employee of his or her respective agency and the agency would be responsible for paying the employee's salary/benefits and overtime. The agency would also provide their investigators with an undercover vehicle, safety equipment and agree to pay the costs of sending their investigator to any high technology related training. If the task force were able to secure any additional funding to cover any or all of these expenses, the FBI, as the lead agency, would monitor the distribution of the funds to the various participants.

The task force Steering Committee would establish policies and procedures for investigating high technology crimes submitted to the task force from local, state and federal law enforcement agencies. The task force would also accept cases directly from the high technology industry, thus making it easier for victim companies to report high technology crimes, which help to forge closer working relationships with the high technology industry. Since prosecutorial resources are limited on both the state and federal levels, each high technology case would be evaluated to determine which court system would give the best probability for a successful prosecution.

#### Steering Committee

The success of any program depends on the goals and objectives established with input from as many of the stakeholders as possible. One stakeholder group that will have significant impact on the success or failure of this program is the High Technology Task Force Steering Committee. The Steering Committee would consist of senior management representatives from the local, state, and federal law enforcement and

prosecutorial agencies participating in the task force. The Steering Committee should be large enough to represent the participants involved in the task force, but small enough to conduct normal business.

The task force would operate under a memorandum of understanding and meet on a monthly basis with a pre-determined agenda. The Steering Committee would elect a chairman and vice-chairman from the committee members who would serve one-year terms. The Steering Committee would establish the goals and objectives of the task force and monitor the monthly progress of the task force, making adjustments and changes when necessary. Since the task force would need continuous political support from both the public and private sector, Steering Committee members would be called upon to champion the cause of the task force on an ongoing basis.

#### Personnel

The personnel that will comprise this task force would consist of full and part time local and state law enforcement officers from the two contiguous counties that would work side by side with their federal and private sector counterparts. These investigators should have a good understanding of computer technology, Internet capabilities, network security and criminal investigation procedures.

Each investigative team will consist of a local or state law enforcement officer, federal officer and private sector investigator. The investigative team will have access to support staff that includes civilian analysts and forensic computer analysts. The team will confer with the prosecuting attorney who would be handling the case for assistance with legal advice and case strategy.

The private sector investigators would provide their unique perspective and expertise to the task force that can only come from having inside knowledge of the latest advances in industry hardware and software. It is anticipated that the private sector investigators and technicians would become the backbone of the high technology investigative task force. Unlike the law enforcement investigators who may transfer back to their respective agency every 2-3 years (promotions, normal transfers, etc.), the private sector investigators and technicians will most likely stay with the task force for longer periods of time. These individuals would provide the institutional knowledge and stability that any task force or organization needs to continually be successful.

Even though the Steering Committee would be responsible for setting task force goals and objectives, the task force would need a Commander to monitor the day to day operations. The Commander should be a management level person from one of the participating agencies and have prior supervisory experience in a multi-agency investigative task force. The Commander would be responsible for preparing and monitoring the annual task force budget, equipment, evidence, and meeting the goals and objectives set forth by the Steering Committee. The Commander would also be responsible for monitoring the cases under investigation and determine which cases should receive additional investigative support or be suspended due to a lack of investigative leads.

### Funding Sources

Every successful program has several critical elements that can be attributed to its continued success. One of those elements is identifying and receiving adequate funding

sources. The high technology investigative task force will need to identify and secure funding from several governmental sources. There are several avenues for the task force to obtain the funding they will need to investigate complex high technology crimes.

One option for funding would come exclusively from the federal government. As the lead federal agency, the FBI would subsidize the task force and provide all the necessary funding except for participant salary/benefits and overtime. Another option would be for the Steering Committee to establish a contribution schedule that would require each participating agency to contribute a certain amount of money to operate the task force. The best potential alternative for a funding source would probably come from state and federal high technology grants. Grants allow local and state agencies to participate in various task forces by providing a separate funding mechanism not dependent on general fund monies.

### Implementation Plan

A program designed to bring the public and private sector together to investigate high technology crimes requires a carefully designed plan to help assure successful implementation. Paying early attention to the issues and persons involved in the program implementation will encourage those supportive of the program and may deter the program's critics.

### Stakeholder Negotiations

Stakeholders are those who may either help the program become successful or those who may hinder the implementation of the program. Stakeholders are:

- Individuals or groups impacted by what we do.
- Individuals or groups who can impact what we do.
- Snaildarter: unanticipated individuals or groups who will unexpectedly emerge and throw the implementation of the program off track.

To implement a successful public/private sector high technology investigative task force program, it will be necessary to negotiate with the stakeholders early in the process to establish support and to develop strategies to deter program detractors. Though complete consensus among all those involved is most likely not a reality, collaborative efforts can lead to consensus with most of the issues.

Local, State, and Federal Elected Governmental Officials – Their approval is essential to the development of the program and they must be convinced that the program is necessary, the goals are achievable and that the amount of staff time necessary to implement the program is sufficient and appropriate.

The Local, State, and Federal Elected Governmental Officials will negotiate:

- The necessary resources to form the public/private partnership.
- The political support for the plan when needed.
- The level of funding needed to participate in the program.

The Local, State, and Federal Elected Governmental Officials will not negotiate:

- The specific terms and provisions of the public/private sector high technology investigative task force.
- Which high technology cases will be investigated and which ones will not be.

High Technology Industry Executive Management Team – As with the elected governmental officials, their approval is essential to the development of the program.

These individuals must be convinced that the program is necessary, the goals are

achievable and that the amount of staff time necessary to implement the program is sufficient and appropriate. The individuals are managers from the high technology industry that have the decision-making ability to commit resources.

High Technology Industry Executive Management Team will negotiate:

- The sharing of sensitive intellectual information.
- The necessary resources to form the private/public partnership.
- The allocation of funds necessary to participate in the program.
- The commitment to produce quality high technology product.

High Technology Industry Executive Management team will not negotiate:

- The specific terms and provisions of the public/private sector high technology investigative task force.
- Which high technology cases will be investigated and which ones will not be.

High Technology Industry Technical and Security Personnel – These individuals will perform the investigative duties along with law enforcement, and the success or failure of the program will be a direct result of their efforts. These personnel will consist of technicians who have the expertise and experience to forensically examine software and hardware and security investigators that know the inner workings of the human side of the high technology industry.

High Technology Industry Technical and Security Personnel will negotiate:

- The necessary technical support to law enforcement.
- How they work cooperatively with law enforcement during investigations.
- How they will police the high technology industry from inside.
- How prevention efforts will occur within the high technology industry.

High Technology Industry Technical and Security Personnel will not negotiate:

- Political issues related to the high technology industry.

Local, State and Federal Law Enforcement Administrators – Their participation is essential to the implementation and day-to-day management of the program. Ultimately, they will benefit from the program by having a more effective and experienced high technology investigative workforce and a high rate of successful prosecutions.

Local, State and Federal Law Enforcement Administrators will negotiate:

- Providing the necessary resources to form public/private partnerships.
- Monitoring the progress of the program and make any necessary changes.
- The necessary funding to support the program.
- The political support for the program.
- The staff time available to develop, implement and manage the program.

Local, State and Federal Law Enforcement Administrators will not negotiate:

- Which high technology crimes will be investigated and which ones will not.

Local, State, and Federal Law Enforcement Supervisors and Investigators assigned to High Technology Crimes – This group, as with their private sector counterparts, will perform the investigative duties and the success or failure of the program will be a direct result of their efforts.

Local, State, and Federal Law Enforcement Supervisors and Investigators assigned to Investigate High Technology Crimes will negotiate:

- The management of the day-to-day case investigations.
- The amount of high technology training for the public and private sector.
- How they will work cooperatively with the private sector.
- How they will protect civil rights while investigating cyber crime.

Local, State, and Federal Law Enforcement Supervisors and Investigators assigned to Investigate High Technology Crimes will not negotiate:

- Political issues related to high technology crimes.

The High Technology Regional Steering Committee – The Steering Committee is responsible for achieving the goals and objectives of the program. The Steering Committee is also responsible for the overall effectiveness of the task force.

The High Technology Regional Steering Committee will negotiate:

- Who will set on the Steering Committee.
- The task force policy and procedures.
- The most efficient use of personnel, resources and funding.
- The criteria to measure the success of the program.

The High Technology Regional Steering Committee will not negotiate:

- Which high technology case will be investigated and which ones will not.

The High Technology User/Community – This group is divided between those that demand a free and unrestricted use of the Internet as well as other technologies and those that want stricter controls on what information can be obtained from electronic media. If there is a Snaildarter among the stakeholders, it will probably come this group in the form of the American Civil Liberties Union (ACLU).

The High Technology User/Community will negotiate:

- The daily use of high technology services.
- What the community standard will be in regards to the cyber policing.
- The support given to law enforcement and the high technology industry.
- Civil rights and privacy for Internet/technology users.

The High Technology User/Community will not negotiate:

- Law enforcement actions that violate civil rights.
- Law enforcement programs that waste taxpayer dollars.

### Monitoring and Feedback

A process to monitor the success of the program is imperative to determine its effectiveness and to determine if the goals and objectives of the program have been achieved. Criteria that can measure how the public/private sector high technology investigative task force is performing include the number of arrests, the number of convictions, the amount of stolen property recovered and the amount of criminal assets seized. Additionally, customer satisfaction can be measured via interviews and surveys.

This program, like any new program of this magnitude, may be revised from time to time to ensure its effectiveness. Through careful monitoring of the program and its impact on high technology crimes, problems can be identified, addressed and resolved.

### Conclusion

Chapter three provides a structured approach to prepare for desired change that will impact the organization and law enforcement's ability to provide quality services. Because of this need for a structured approach, an external and internal analysis of the organization was conducted, stakeholders were identified, and several alternative solutions were analyzed leading to the selection of a preferred program and ultimately an implementation plan was developed.

With the foundation set for the proposed program through strategic planning, it is imperative that a comprehensive program be developed to implement the change. This

will be discussed in the Transition Management phase of the project, which will be the topic of the following chapter.

## **CHAPTER FOUR**

### **TRANSITION MANAGEMENT**

#### Introduction

A Transition Management Plan is imperative to the success of a new program. The Transition Management Plan can spread over many years and encumber a significant amount of personnel and financial resources. Commitment to the program from the stakeholders and the identification of relevant issues impacting the program are critical to developing an effective program.

The formation of a joint public/private sector high technology investigative task force that can be utilized through out the United States must be comprehensively developed and carefully managed. Any program of this nature is a long-term obligation for both law enforcement and the high technology industry. To aid in the successful implementation of such a program that has several ramifications, it is important that all of the stakeholders and the specific legal, ethical and political issues are addressed up front.

Several questions will need to be addressed before the project is ever launched. What impact will the implementation of such a program have on law enforcement agencies as well as other law enforcement agencies? Will such a program that requires free exchange of information with non-law enforcement personnel accomplish the desired goals?

As previously stated, the program being proposed may not enjoy the full support of all the stakeholders. No matter how careful the program developers are to identify all the potential stakeholders, the possibility of snaildarters exist. Snaildarters are individuals or entities that inhibit the development of a program. They may or may not

have been previously recognized, but their hidden agendas were unknown. Snaildarters must be recognized as having influence on the process and their positions must be included into a development plan. Understanding the positions and arguments of stakeholders is imperative to resolve differences.

### Commitment Planning

Consensus among the stakeholders on the implementation of a public/private sector high technology investigative task force may never be completely achieved. Since complete agreement of the terms may not be feasible, working towards consensus on most of the terms may be a more practical goal. Critical mass members are those individuals and groups whose support is essential to accomplish the desired change. Table 4.1 displays the current commitments of these critical mass individuals and the desired level of commitment necessary to accomplish the strategic plan. An X represents their current position and an O represents their desired position.

### **CURRENT COMMITMENT TO STRATEGIC PLAN**

<b>Critical Mass Members</b>	<b>Block the change</b>	<b>Let Change happen</b>	<b>Help Change happen</b>	<b>Make change happen</b>
<b>Elected Governmental Officials</b>		X		O
<b>High Technology Executive Mgmt.</b>		X		O
<b>Police Executive Management</b>		X		O
<b>High Technology Security Personnel</b>		X		O
<b>Law Enforcement High Tech. Inv.</b>		X		O
<b>Steering Committee</b>		X		O

Table 4.1

Those identified as key in the process can be categorized three ways:

1. Change Strategist: Those who lay the foundation, manage the boundaries, and craft the vision.
2. Change Implementers: Those who develop and enact the steps, manage the coordination, and make it happen.
3. Change Recipients: Those who adapt, or fail to adapt to the change.

Below is a description of the commitment to the change necessary to implement a public/private sector high technology investigative task force.

#### Elected Government Officials: Change Strategist

The Elected Government Officials are responsible for setting policy, fiscal management, political ramifications and for long term planning. Elected government officials will closely scrutinize any program that redirects government personnel or financial resources. Their support is essential to help the change happen.

#### High Technology Industry Executive Management: Change Strategist

The High Technology Industry Executive Management Team is responsible for setting policy, fiscal management, political ramifications, and for long term planning. The High Technology Industry Management Team will closely scrutinize any program and redirect private sector personnel or financial resources. Their support is essential to help the change happen.

### Police Management: Change Implementers

The Police Management Team is responsible for providing personnel and financial support to High Technology Investigative Task Force. The Police Management Team will work closely with the Steering Committee and provide them with guidance and political support when necessary. Police management support is essential to help the change happen.

### High Technology Security Personnel: Change Implementers and Change Recipients

This group will be instrumental in the development of the program and will be the ones conducting the cyber crime investigations along with law enforcement and providing the necessary training and technical assistance to law enforcement. High technology security support is essential to help the change happen.

### Law Enforcement Investigators: Change Implementers and Change Recipients.

This group will be instrumental in the development of the program and will be the ones conducting the cyber crime investigations along with the high technology industry. The law enforcement investigator's support will be essential to help make the change happen.

### Steering Committee: Change Implementers

The Steering Committee is responsible for the overall management and achieving the goals and objectives of the task force. Additionally, they are responsible for staffing the task force and appointing a Commander to assist in the development and implementation of the plan. Throughout the life of the task force, the Steering

Committee (through the Commander) must continue to work with the critical mass members to refine the goals and objectives and ensure the success of the task force. The Steering Committee's support is essential to help the change happen.

### Supporting Technologies

Once the critical mass has been identified and their level of commitment has been determined, an environment must be created that will allow for the transition of a high technology investigative task force. Bringing these individuals or groups together to problem solve may generate additional support for the program and create an atmosphere of collaboration that can make the program even stronger. This method of problem finding further allows critical mass members to identify future problems and address them up front.

Successful transition can also be achieved through educational intervention. This provides participants with an understanding of the necessary steps to implement the high technology investigative task force and also with an opportunity to understand the needs and perspectives of the other participants. Formal meetings between law enforcement and the high technology industry, internal/external correspondence and questions and answer sessions can facilitate this transitional method.

### Transition Structure

Selecting the best person to head the transition is critical and that person must have the full support of all those involved in the transition. To implement a high technology investigative task force between law enforcement and the high technology

industry, the most likely person will be a member management level person from a participating law enforcement agency. This manager must have solid management skills, strong interpersonal skills, and knowledge of budgets and be able to work cooperatively with other law enforcement agencies both inside and outside the task force.

### Responsibility Charting

A responsibility chart provides the framework to identify the responsibilities of the involved individuals or groups during the transition to a joint law enforcement and high technology industry investigative task force. This method clarifies the roles and responsibilities and can reduce conflict during the transition period. Table 4.2 presents a responsibility chart for transition to a joint law enforcement and high technology industry investigative task force.

### **RESPONSIBILITY CHART**

Decisions	Participants					
	Elected Officials	High Tech Mgmt	Police Mgmt.	High Tech Security	High Tech Police	Steering Comm.
<b>Set Initial Planning Meeting</b>	<b>I</b>	<b>I</b>	<b>R</b>	<b>I</b>	<b>I</b>	<b>A</b>
<b>Select Project Manager</b>	<b>I</b>	<b>I</b>	<b>R</b>	<b>S</b>	<b>S</b>	<b>A</b>
<b>Select Transition Team</b>	<b>I</b>	<b>I</b>	<b>R</b>	<b>I</b>	<b>I</b>	<b>A</b>
<b>Establish Goals and Objectives</b>	<b>I</b>	<b>I</b>	<b>R</b>	<b>I</b>	<b>I</b>	<b>A</b>
<b>Develop Policy Guidelines</b>	<b>I</b>	<b>I</b>	<b>R</b>	<b>I</b>	<b>I</b>	<b>A</b>
<b>Develop Program Standards</b>	<b>I</b>	<b>I</b>	<b>R</b>	<b>I</b>	<b>I</b>	<b>A</b>
<b>Develop Evaluation Criteria</b>	<b>I</b>	<b>I</b>	<b>R</b>	<b>S</b>	<b>S</b>	<b>A</b>
<b>Set Implementation Date</b>	<b>I</b>	<b>I</b>	<b>R</b>	<b>I</b>	<b>I</b>	<b>A</b>
<b>Present Program to Employees</b>	<b>I</b>	<b>I</b>	<b>R</b>	<b>S</b>	<b>S</b>	<b>I</b>
<b>Set Evaluation Date</b>	<b>I</b>	<b>I</b>	<b>R</b>	<b>S</b>	<b>S</b>	<b>A</b>
<b>R = Responsibility (not necessarily Authority)</b>			<b>S = Support (put resources towards)</b>			
<b>A = Approval (right to vote)</b>			<b>I = Inform (to be consulted before action)</b>			

Table 4.

## Conclusion

This chapter identified those individuals who are critical in the implementation process of a joint law enforcement and high technology industry investigative task force, their specific responsibilities and desired commitment levels. These law enforcement and private sector professionals will be asked to implement a program that has the potential to radically change the manner in which high technology crimes are investigated. The implementation of this program will require patience, leadership, and commitment by all the stakeholders regardless of their position.

The next chapter will summarize the research that was conducted for this project, recommend a workable model and conclude with specific examples of what impacts may be expected if the model was to be implemented.

## CHAPTER FIVE

### SUMMARY, RECOMMENDATIONS AND CONCLUSIONS

#### Summary

The impact of the high technology industry on the investigation of high technology crimes has been addressed throughout this project and forecast to the year 2007. This was done through issue identification that included environmental scanning and interviews. Trends and events related to the topic were also analyzed. This project presents a position that the high technology industry will play a major role in the investigation of high technology by the year 2007. The premise is based on the current and anticipated changes in computer and other high technologies and the inability of law enforcement to maintain the necessary expertise to effectively investigate high technology crimes in the future.

Even though the San Francisco Bay Area would be a model geographic area for this project, the concern and need for law enforcement and high technology industry partnerships is nationwide. Once the preferred option to address the issue has been identified, specific implementation strategies were presented to make the necessary change happen. This was followed by a transition management plan to ensure the success of the changes.

#### Recommendations

The results of the literature review and interviews conducted reveal that the problems facing law enforcement and the high technology industry have reached an alarming level and all projections indicate that the problem will become worse by the

year 2007. Doing nothing to address the issue will result in an increase in cyber crime, a decrease in public confidence in the Internet and other high technologies and a real threat of cyber terrorism that will threaten the security of the United States.

This project recommends the development of a joint law enforcement and high technology investigative task force that utilizes the expertise and resources of the private sector in a more collaborative approach than ever before. Combining law enforcement and private sector personnel from two contiguous counties would form the basis of the high technology investigative task force. This model would be duplicated throughout the State of California, on a national basis and ultimately internationally. This is a non-traditional role being suggested for the private sector, and comes with some risk. But, when you consider the overall benefits to law enforcement, the high technology industry and the community, doing business as usual is an unacceptable alternative for the 21<sup>st</sup> century.

### Conclusion

If steps are not taken promptly to address the issue of high technology crime and law enforcement's inability to stay one-step in front of the cyber criminal, the outlook for the future will be bleak for our technology dependent society. High technology experts forecast that by the year 2007, 90 percent of the homes in the United States will have a computer. This could lead to a significant increase in cyber crime, cyber terrorism, child victimization and other types of electronic crimes.

We need not wait until 2007 to see the results of these consequences. High technology crimes are increasing and these are only the ones that are reported to law

enforcement. Many high technology investigations either lack proper investigative follow up or are not investigated at all. Communities, such as in the San Francisco Bay Area that have dedicated high technology investigative units, continue to have success, but they could be even more successful if private industry is allowed to play a greater but supervised role in the investigation of high technology crimes.

History has demonstrated what will happen, and continue to happen, if private industry fails to play a greater role in the investigation and prevention of high technology crimes. The negative impacts of continuing on the present path would result in a decrease in consumer and public confidence in the nation's technologies, economy, and governmental agencies that support these activities. The end result would severely affect the safety and security of the country and its ability to promote democracy around the world. Any future societal and economic growth cannot occur without proper controls and monitoring of the technology that supports its growth.

The benefits of a law enforcement and high technology industry partnership in the investigation of high technology crimes provide hope for the future. The most obvious benefits would result in better communication between the public and private sector, increased trust, leading to more high technology crimes being reported and prevented, better trained law enforcement officers/investigators in the field of high technology crime, resulting in more successful prosecutions of high technology criminals. Other benefits would include increased public confidence in the high technology industry and continued economic stability of America and other world markets.

The impact that the high technology industry is going to have on the investigation of high technology crimes is not going to be felt overnight. It will take a well-coordinated and multi-disciplinary approach to properly address the issue before positive results can be seen. We must continue to forge closer relationships with the high technology industry or face the consequences in the future.

## APPENDICE A

### LIST OF NOMINAL GROUP PARTICPANTS

Mr. Greg Munks	-	Undersheriff, San Mateo County Sheriff's Office
Mr. Steve Barretta	-	IT Manager, San Mateo County Sheriff's Office
Mrs. Jean Whitney	-	Reporter, San Mateo County Times
Mr. Matt Stannard	-	Reporter, San Francisco Chronicle
Mr. Chris Woiwode	-	Supervisory Special Agent, Federal Bureau of Investigation – High Technology Task Force
Mr. Joe Chiaramonti	-	Director of Security, Sun Micro Systems
Mr. Rich Cinfio	-	Commander, San Carlos Police Department
Mr. Jack Grandsaert	-	Deputy District Attorney, San Mateo County District Attorney's Office
Mr. Charles Robinson	-	Attorney, San Mateo County Private Defender Program

## APPENDICE B

### LIST OF TRENDS

- 1) Hackers getting bolder and sabotaging law enforcement systems.
- 2) Gap between criminal proficiency and resources growing faster than law enforcement capability to investigate.
- 3) Threat of information and technology infrastructure sabotage.
- 4) Use of computers to commit a broader range of crimes.
- 5) Change in growth and reliance on E-commerce.
- 6) Dwindling financial support to sustain investigations.
- 7) Lower production cost of technology devices will become more available.
- 8) Confidentiality for computer users.
- 9) Change in consumer protection for release of personal information.
- 10) Multi-jurisdictional approach to investigating Internet crimes.
- 11) Need for public/private investigative partnerships.
- 12) Dependence on the Internet.
- 13) Change in coordination of communications between law enforcement agencies.
- 14) Concerns over freedom of speech on the Internet.
- 15) Number of high technology task forces and forensic laboratories.
- 16) Use of high technology to track children and seniors.
- 17) Emphasis on training for law enforcement officers on high technology crimes.
- 18) Inability to predict trends.
- 19) Demand for new technology will result in criminal exploitation.
- 20) Accessibility of encryption.
- 21) Need to stay current with the rapid change in technology.
- 22) Information overload.
- 23) Willingness to sacrifice privacy and rights for security and convenience.
- 24) The use of technology will help solve traditional crimes.
- 25) Technology proficient law enforcement workforce.
- 26) The loss of trained high technology investigators to the private sector.
- 27) Closer interaction between the public/private sector.
- 28) Incentives to retain experienced personnel.
- 29) Degree of difficulty in solving high technology crimes.
- 30) Industrial espionage.
- 31) Emphasis by the news media on high technology crimes.
- 32) Consequence of misinformation by the news media.
- 33) Crime information and trends more accessible by citizens.
- 34) The changing technology and processes requires more education for attorneys, judges and jurors.
- 35) More emphasis on high technology training for law enforcement officers.
- 36) Cyber-terrorism and cyber-stalking.
- 37) Mobility of cyber crime due to wireless applications.
- 38) The globalization of crime.
- 39) Counterfeiting of high technology hardware and software.
- 40) No borders for high technology crimes.

## APPENDICE C

### LIST OF EVENTS

- 1) Law enforcement powers given to private sector high technology investigators.
- 2) Hacker disables the Internet.
- 3) Visa database headquarters destroyed by bomb.
- 4) "X" virus destroys all private and public sector databases.
- 5) Creation of worldwide web & Internet.
- 6) Creation of 2<sup>nd</sup> worldwide web.
- 7) Mind controlling chip place in experimental patient.
- 8) Development of mid controlling devices.
- 9) Human cloning legalized.
- 10) Nintendo replaces major league baseball.
- 11) American landmarks destroyed by terrorist.
- 12) Non-silicone based technology is developed.
- 13) Clean/renewable power source is developed.
- 14) Terrorist induces military action via the Internet.
- 15) Poor economy changes the amount of funding for high technology purchase and maintenance.
- 16) Passage of privacy law that restricts media access.
- 17) Hacker is responsible for a national utility powergrid shutdown.
- 18) Public/private partnerships declared a conflict of interest.
- 19) Web media renders print media obsolete.
- 20) Civil rights eliminated for terrorist investigations.
- 21) Mandatory national identification cards issued.
- 22) War erupts on American soil.
- 23) Gun control laws are repealed for personal safety.
- 24) Virtual teaching eliminates the need for in human teachers.
- 25) A license is required accessing the Internet.
- 26) Stolen nuclear bomb exploded in the United States.
- 27) United States airline industry collapses.
- 28) United States borders with Mexico and Canada shutdown.
- 29) Massive solar flares eliminate all communication capabilities.
- 30) United States currency replaced by electronic money.
- 31) Federal and State grant funding discontinued.
- 32) Police officer arrested for theft of funds via the Internet from Visa.
- 33) Surveillance technology reduces the need for police officers on the patrol.
- 34) Hacker acquitted due incompetent investigation by FBI.
- 35) Part 1 crimes decreased by 50%.
- 36) Private industry offers signing bonuses for qualified law enforcement officers.

## NOTES

---

<sup>1</sup> Mintz, Howard. "Reno Urges Teamwork on Battling Cybercrime." San Jose Mercury News. April 5, 2000. Online. Silicon Valley News. Accessed: September 22, 2001.

<sup>2</sup> Ibid.

<sup>3</sup> Schwartz, Peter and Leyden, Peter. "The Long Boom: A History of the Future, 1980-2020." WIRED. July 1997. Accessed: June 15, 2001.

<sup>4</sup> Ibid.

<sup>5</sup> Police Futurist, "Scanning, Trends & Events" Spring 2001. Volume 9, Number 1

<sup>6</sup> The Argus, Associated Press: "Intel Unveils the "Worlds Fastest" Transistors. June 10, 2001.

<sup>7</sup> Futurist, Cyber Crime. Gene Stephens. Class handout December 6, 2000.

<sup>8</sup> Kirby, Carrie. The San Jose Mercury News: "Charges dropped in copyright case." December 14, 2001.

<sup>9</sup> Staedter, Tracy. Technology Review. "Face Recognition." November 2001.

<sup>10</sup> Geewax, Marilyn. San Francisco Chronicle. "The Cost of Cyber Crime." December 1, 2001.

<sup>11</sup> Global Business Dialogue on Electronic Commerce (GBDe). "Cyber Security and Cyber Crime." Web-site. <http://www.gbde.org/nn/2000/cybersecurity.html>. Internet accessed: September 22, 2001.

<sup>12</sup> Grassley, Chuck. "Cyber-Security and Critical Infrastructure Protection." Web-site <http://www.senate.gov/~grassley/releases/2001/p01r7-25b.html>. Internet access: November 3, 2001

<sup>13</sup> Atomic Tangerine. "Information Technology Crime, a Growing Challenge to law enforcement." <http://www.interpol-assembly2000.com/atomic Tangerine.html>. Internet accessed: September 30, 2001.

<sup>14</sup> Heiman, Bruce J. "At Risk: A Secure Net." Legal Times August 14, 2000.

<sup>15</sup> High Technology Crime Investigation Association (HTCIA). Web-site. <http://www.htcia.org/membership.html>. Internet access: November 1, 2001

<sup>16</sup> Command College handout

---

## BIBLIOGRAPHY

Mintz, Howard. "Reno Urges Teamwork on Battling Cybercrime." San Jose Mercury News. April 5, 2000. Online. Silicon Valley News. Accessed: September 22, 2001.

Schwartz, Peter and Leyden, Peter. "The Long Boom: A History of the Future, 1980-2020." WIRED. July 1997. Accessed: June 15, 2001.

Police Futurist, "Scanning, Trends & Events" Spring 2001. Volume 9, Number 1

The Argus, Associated Press: "Intel Unveils the "Worlds Fastest" Transistors. June 10, 2001.

Futurist, Cyber Crime. Gene Stephens. Class handout December 6, 2000.

Kirby, Carrie. The San Jose Mercury News: "Charges dropped in copyright case." December 14, 2001.

Staedter, Tracy. Technology Review. "Face Recognition." November 2001.

Geewax, Marilyn. San Francisco Chronicle. "The Cost of Cyber Crime." December 1, 2001.

Global Business Dialogue on Electronic Commerce (GBDe). "Cyber Security and Cyber Crime." Web-site. <http://www.gbde.org/nn/2000/cybersecurity.html>. Internet accessed: September 22, 2001.

Grassley, Chuck. "Cyber-Security and Critical Infrastructure Protection." Web-site <http://www.senate.gov/~grassley/releases/2001/p01r7-25b.html>.

High Technology Crime Investigation Association (HTCIA). Web-site. <http://www.htcia.org/membership.html>.

Atomic Tangerine. "Information Technology Crime, a Growing Challenge to law enforcement." <http://www.interpol-assembly2000.com/atomic Tangerine.html>.

Heiman, Bruce J. "At Risk: A Secure Net." Legal Times August 14, 2000.