Nevada's high technology crime task force

Dorinda A. Hollenbeck

University of Nevada Las Vegas
NEVADA'S HIGH TECHNOLOGY CRIME TASK FORCE

By
Dorinda A. Hollenbeck

A professional paper submitted in partial fulfillment of the requirements for the degree of

Master
In
Public Administration

Department of Public Administration
University of Nevada, Las Vegas
February, 1999
Acknowledgements

I wish to express my appreciation to the faculty of the Public Administration Department and especially to the members of my committee. The dedication they have for the students and the university have made this program most worthwhile and promises to be much more successful in the future.

Thank you to Attorney General Frankie Sue Del Papa who has provided me with opportunities to grow professionally as well as personally. I would also like to thank Gregory Smith and Ernesto Capiral of the Nevada Attorney General's Office who encouraged me to complete the program when office life became harried; and to my parents, Wong and Louise Mark, who have instilled in me a work ethic that I will always be proud to have.

Lastly, I want to thank my husband, David, who is a constant encouragement and supporter of me to be the best person that I can be and to push myself to the limits. Thank you for always being there for me.
Table of Contents

Abstract........................................................................ iv
Chapter I - Introduction............................................. 1
   A. State of Nevada vs. Ronald D. Harris.............. 1
   B. United States vs. Mary Ferris....................... 4
Chapter II - Computer Crime and Its Definition......... 8
Chapter III - Economic Impact................................. 13
Chapter IV - Methodology......................................... 21
Chapter V - Other jurisdictions are recognizing the need for specialized units................. 27
   A. Sacramento Valley High Tech Task Force........ 29
   B. Other Law Enforcement Agencies............... 31
   C. Federal Efforts........................................ 34
Chapter VI - Nevada's Accomplishments to Date....... 39
Chapter VII - Conclusions......................................... 42
Bibliography.......................................................... 48
Abstract

With the dramatic advances in computer technology in recent decades, the increase of crimes committed using high technology has skyrocketed. Losses to corporations and governmental agencies have totalled millions if not billions of dollars per year. Victims are beginning to speak out and ask for help. Law enforcement agencies throughout the country are teaming together to create specialized crime units and task forces in an attempt to successfully combat computer related crimes. Nevada is one of the many states which is in the infancy stages of developing such a task force. The Sacramento Valley High Tech Crime Task Force has actively supported the efforts of the Nevada Attorney General’s Office. What does the Nevada Attorney General’s Office need to do to launch a successful high technology crime task force as other jurisdictions have done? What is the best, most efficient, most productive method to investigate this type of white collar crime? This paper will examine such efforts.
Chapter I
Introduction

The dramatic increase in crime using high technology has caused losses to corporations and governmental agencies into millions of dollars per year. The figures will likely climb in the future. The reaction of law enforcement has resulted in the creation of specialized crime units and multijurisdiction task forces.

Nevada Attorney General Frankie Sue Del Papa referred to the following case as the state’s "wake up call" to the fact that a high technology crime task force was needed.

A. State of Nevada vs. Ronald D. Harris

In January 1995 Nevada State Gaming Control Board employee Ronald D. Harris travelled to Bally’s Hotel and Casino in Atlantic City, New Jersey. Accompanied by his companion, Reid McNeal, and packed with several pieces of high technology equipment, McNeal hit a $100,000 Keno jackpot on a video Keno game with the instruction of Harris.

After insisting on being paid cash instead of a cashier’s check, McNeal’s activity became suspect to hotel security and his room was subsequently searched.
The search uncovered items belonging to the Nevada Gaming Control Board (GCB) which were used to calculate and alter the element of chance in a game. Harris and McNeal were shortly arrested and an investigation began quickly in Nevada due to Harris’ position within the agency.

The Nevada Attorney General’s Office has the jurisdiction to investigate and prosecute state employees who during the course and scope of their duties misuse their authority and face possible criminal charges.

Harris was an engineer for the GCB in the Electronics Services Division. He had access to various computer programs submitted to the Board which are required by law to be provided by gaming licensees to the division for premarketing approval.

It was discovered that Harris used confidential information from his position at GCB to find a glitch in the random number generator used by a particular Keno program. He used this information to develop a computer program which would predict the outcomes of future games.

Harris not only figured the outcome of some Keno programs but also altered the element of chance on various slot machines within Nevada.

"Harris did . . . modify a proprietary computer
Crime Task Force

program of the GCB, known at the DEPROM, which was used by that agency’s field inspectors to test the proper functioning of gaming devices. The modification of the DEPROM program caused a cheating subroutine, or ‘gaff,’ to be inserted into computer chips in certain Universal slot machines -- equipment or devices associated with gaming -- which were being inspected by GCB employees. The gaff was activated by a predetermined sequence of coin bets, after which the gaffed gaming device would register and pay out its maximum award jackpot. The gaff affected the result of a wager by determining win or loss, and/or altered the normal criteria of random selection, affecting the operation or determining the outcome of the game." (Indictment filed in the Second Judicial District of the State of Nevada, case #CR96-1349)

Harris was also criminally charged with instructing his acquaintances in the use of a predetermined sequence of coin bets necessary to activate a cheating feature inserted into a computer chip contained within specific slot machines.

An investigation by the Nevada Attorney General’s Office uncovered several jackpots won over the past years attributed to Harris and his colleagues who travelled statewide to win jackpots. Harris et. al. were criminally charged in Washoe and Clark Counties.
Harris was subsequently sentenced to serve 7 years in the Nevada Department of Prisons.

Another computer related case followed on the heels of the State of Nevada vs. Ronald D. Harris.

B. United States vs. Mary Ferris (AKA: Jane Treher)

In August 1996 L & H Administrators purchased Coresource, the State of Nevada's third party administrator of health claims.

Claims Manager Mary Ferris was hired to supervise a staff to process claims. She had previous claims processing experience in California and seemed to be a fine candidate for the position to which she was hired.

Eight months into her employment with L & H, Ferris planned and carried out a scheme which would net her $608,000 from the State of Nevada's account. These monies were the result of false claims paid which were created on the computer. These claims were made for services from fictitious providers which were also inputted into the computer.

An investigation was initiated when former employees of L & H brought an internal audit to the attention of authorities. L & H had known there was a problem with Ferris who was no longer with the company but when L & H was forced to close their doors due to poor business practices, they never advised the State
With Ferris’ knowledge of processing medical claims and access to the L & H claims computer, Ferris created false provider names and addresses which were found to be at various rented mail box locations. Ferris then processed false medical claims in an amount in excess of $600,000 to legitimate employees changing their addresses to the mail boxes rented by her. This would prevent any claims payment notification from being forwarded to the employees alerting them of payments made to fictitious providers who, of course, never rendered service.

Payments were generated by the computer for these false claims and checks sent to false providers at the mail boxes. Ferris collected the checks and deposited them in various accounts she had opened in the names of the false providers at a local bank.

Search warrants executed on the bank accounts resulted in the recovery of $471,000. Of the $471,000 recovered, the state’s share was $466,000 with the remaining going to Clark County. Ferris had performed similar acts with the Clark County account managed by L & H.

The Attorney General’s Office worked with the Federal Bureau of Investigation in this case that would recover much of the loss from Ferris and send Jane
Treher (AKA: Mary Ferris) to federal prison for over 4 years. Ferris had previous convictions for health care fraud in the State of California and was being sought by another private company in California for similar conduct.

With the sudden revelation that computer crime within the State of Nevada was becoming more prevalent, Attorney General Frankie Sue Del Papa sponsored the Nevada High Technology Crime Task Force. This task force is modeled after the Sacramento Valley High Tech Task Force which has been in place since 1995.

"The Nevada High Technology Crime Task Force was organized in July, 1997 at the direction of Attorney General Frankie Sue Del Papa and is comprised of representatives of state, local and federal law enforcement agencies and private industry. The task force was created for the purpose of forming high technology crime units to conduct multi-jurisdictional investigations; track and disrupt the illicit commerce in stolen high tech goods, investigate and prosecute suspects engaged in white collar crime, organized crime and fraud against the government and private industry."

(Executive Summary of the Strategic Plan, p.2)

While the Attorney General's Office has successfully brought computer crime to the attention of law enforcement officials and there is an increased
interest in pursuing such a task force, the specific dedication of resources by law enforcement agencies throughout Nevada has been nominal.

Why? Corporations and governments are losing millions of dollars per year. Why is there greater interest in the Sacramento Valley than in the Las Vegas Valley with all its casinos and computerized gaming devices? What did the Sacramento Valley law enforcement agencies do to create a successfully operating task force in a relatively short time? What can Nevada do to imitate the success in Sacramento and other parts of the country?

These are questions that need to be addressed in an attempt to make the Nevada High Tech Crime Task Force more efficient in their mission goals. (Much of the information contained in this paper was extracted from handouts distributed at an organizational meeting in July 1997 on the Nevada Computer Forensic Task Force.)

Additionally, what is the best, most efficient, most productive method to investigate such specialized, technically oriented white collar crime? This question will be answered by reviewing what other law enforcement agencies and jurisdictions are doing to address this ever increasing problem of computer crime.
Chapter II

Computer Crime and Its Definition

No single agency or reference can agree on exact verbiage to define computer crime. A broad definition which encompasses most of what is to be reviewed will define computer crime of a form of white-collar crime committed inside a computer system or the use of a computer as the instrument of a business crime. (Computer Crime, Criminal Justice Resource Manual, 2nd edition, p. 2)

This definition is a broad definition which covers a wide range of criminal activity. This activity can be further categorized and while various jurisdictions, authors, vendors, agencies, do categorize computer crime into several classifications, outlined below is a standard one that is generally acceptable.

The California High Technology Crime Task Force Committee, also modeled after the Sacramento Task Force, categorized high technology crime in 6 areas of interest.

1. Computer Component Theft. This includes burglary and robbery at manufacturing sites, storage facilities and retail stores. This also includes employee theft from manufacturers and theft of computers at non-
high technology businesses and institutions.

2. Telecommunications Fraud. This includes toll fraud, the theft of long distance telephone service. This can also include subscription fraud, the applying for telephone service in someone else's name. The cloning of cellular telephones would also be included in this category.

3. Theft of Proprietary Information. This includes trade secret theft.

4. Computer Intrusion. This includes committing fraud by altering or destroying records.

5. Counterfeiting and Software Piracy.

6. Related Crimes, i.e. child pornography.


The Criminal Justice Resource Manual on Computer Crime (1989) says the technical definitions in the state laws also vary. Many states have followed the definitions proposed in early federal bills. (Those bills referencing the Federal Computer Systems Protection Act of 1977.) These definitions have been heavily criticized by the technical community in Congressional hearings as ranging from being too dependent on current technology to being inaccurate or irrelevant. However, they prevailed and are found in

In Nevada there are existing statutes which address computer crimes, namely in Chapter 205 of the Nevada Revised Code. Definitions of access, computer, data, network, etc. are defined specifically in NRS 205.473. This chapter also addresses the prohibitions of modification, damage, destruction, concealing, copying, gaining access, etc.

While these statutes exist in the Nevada Revised Codes, neither Ron Harris nor Jane Treher were criminally charged with computer crimes. Harris was charged with gaming offenses and Treher was charged federally with theft offenses.

The Department of Justice broadly defines computer crimes as "any violations of criminal law that involve a knowledge of computer technology for their perpetration, investigation, or prosecution." (Dillon, Groene, Hayward, 1998)

The May 1995 issue of The CPA Journal defines computer fraud and categorizes it in yet another way.

1. Altering Input. Increasing salaries, creating fictitious employees, collecting salaries of terminated employees can be easily done by perpetrators.

2. Theft of Computer Time. Theft of time means using a computer system for unauthorized
purposes.

3. Software Theft and Modifications. Making unauthorized or illegal copies, modifying software, or using software in an unauthorized manner, all constitute computer fraud. This might also include developing software to carry on unauthorized activities.

4. Altering or Stealing Data Files. In numerous cases, data files have been scrambled, altered, or destroyed by disgruntled employees. Employees can also steal company data selling this insider information to securities buyers.

5. Theft or Misuse of Systems Output. Many people share printers, and this output can be subject to unauthorized copying.

(Romney, 1995)

No matter which journal article, text, agency, or organizational definition is used to define computer crime and no matter how many different categories each author can place them in, the bottom line remains the same. Computer crime results when a computer has been illegally used to commit a crime.

The overall definition will always be broad in its general reference. It is not until the matter is addressed in a court of law that the definition needs
to be specific. With different courts of law come different definitions of criminal violations.

Those states without specific computer crime statutes and even states with computer crime statutes may and usually do prosecute under general fraud/theft statutes as were the cases of Harris and Treher. Prosecutors find it easier to explain to a judge and jury that a financial crime has been committed by using statutes that are more familiar and easier to understand by the general public.
Chapter III
Economic Impact

Can the economic impact of computer crime be determined? Several articles were reviewed for statistics on what kind of losses companies and governments are facing.

Dillon, Groene, and Hayward (1998) state that accurate statistics on the extent of high technology computer crime are impossible to determine because of the difficulty in adequately defining computing crimes. The statistics are also untrustworthy due to failure to report incidents for fear of losing customer confidence and the inability to detect computer crime. However, the aggregate annual losses to businesses and governments are estimated to be in the billions of dollars.

There is no one, single source of reporting computer crime. It becomes more difficult if not impossible to track losses when prosecutors do not charge under computer crime statutes or end up plea bargaining cases to include criminal charges which do not relate to computer crime. For example, an individual may be criminally charged with a computer crime but in court, the defendant pleas to a reduced charge of theft. If a statistician were to attempt to
compile figures based on final court dispositions, the theft case would not reflect a computer related crime.

"The resulting economic losses are staggering. An American Bar Association study found that half of the businesses and government institutions uncovered at least one fraud in the year of the study. The National Center for Computer Crime Data concluded that the cost of computer crime exceeds $555,000,000 a year and that the average computer loss is $109,000. According to another study, up to 90% of companies have lost money to computer fraud. The Bank Administration Institute calculates that U.S. banks lose over a billion dollars a year because of information systems abuse.

Many computer frauds go undetected and unreported. The FBI estimates that only one percent of all computer crime is detected. Also, an estimated 80% to 90% of the frauds uncovered are not reported. The most common reason for not reporting computer fraud is that companies fear they will lose more money from the adverse publicity surrounding the disclosure than from the fraud itself." (Romney, 1995)

Another article in Risk Management in April 1995 estimated computer losses:

* Computer losses range from $500 million to $8 billion a year.

* Computer losses are projected to cost $200
billion by the year 2000.

* Computer crime has increased by 260% since 1985.

* Average computer crime nets $450,000.

* Computerworld (April 15, 1996) reported of a survey of 325 corporations by the American Society for Industrial Security (ASIS) which revealed that losses by U.S. firms from theft of proprietary data are increasing rapidly, rising 323% since 1992. The figure includes losses attributed to bribery, hacking and numerous kinds of industrial espionage. The average loss per incident amounted to $26 million, and overall industry losses in the U.S. per month come to around $2 billion. Over 60% of the financial losses are related to loss of research and development, strategic plans and manufacturing process data.

It [computer crime] is also an economic threat. Estimates of the financial impact of computer crime have risen with the number of cracker incidents. In 1995, the FBI estimated that digital criminals cost U.S. businesses $7.5 billion a year, with the criminal charges ranging from outright industrial espionage and willful destruction of files and data to the simple cost of forcing system administrators to plug holes. That year, according to an annual survey conducted by the Computer Security Institute in San Francisco, about
one out of every five networks on the Internet was penetrated.

In mid-1996, the Computer Security Institute and the FBI announced the results of a joint survey of 428 U.S. corporations, government agencies, financial institutions, and universities. Forty-two percent had discovered electronic malfeasance on site in the previous year, with many of the companies believing that the intrusions were performed by crackers for foreign competitors. More than half the incidents came from outside intrusions (the rest, from insiders who abused their access). Fearing negative publicity to their corporations and stockholders, fewer than 17 percent of the institutions reported these incidents to law enforcement. The survey suggests that computer criminals are costing private businesses billions of dollars. (Freedman, Mann, 1997)

Electronic News (1997) reported that according to the American Electronics Association (AEA) high-tech thefts averaged about $500,000, the record being $12 million in chips and memory boards stolen in 1995 from Centron Electronics in Irvine, California.

"Early this year (1997) the FBI commissioned a nationwide survey of U.S. companies of all sizes on the subject of computer security. The survey was conducted for the FBI by the Computer Security Institute (CSI), a
security-research organization in San Francisco.

Among the survey's findings:

* Seventy-five percent of the 563 companies that responded said they had been victimized by computer related crime in the preceding year.

* Fifty-nine percent of the victimized companies could place a dollar figure on their losses; the average per company was $401,600.

* Forty-nine percent of the respondents reported unauthorized use of their computer systems.

Safeware, a computer-insurance firm in Columbus, Ohio, estimates that in 1996, U.S. businesses lost $1.4 billion to thefts of computers alone." (McCollum, 1997)

A 1997 issue of American Banker reported that U.S. financial firms are losing up to $2.4 billion a year to computer theft, according to a report issued Thursday by Rep. Henry Gonzalez, the House Banking Committee's ranking Democrat. The report stated that financial institutions, despite increasing use of Internet transactions, have not installed software necessary to fight off computer fraud.

Computerworld (Feb. 2, 1998) again reported that
the Business Software Alliance (BSA) expects software piracy to rise in Asia this year, partly due to the financial crisis hitting the region. More than half of the software in use today in Asia is pirated, according to figures released by BSA. Officials for the Washington group said they expect piracy will rise in both corporate and consumer markets. BSA plans to lobby for stricter international copyright laws. BSA estimated piracy losses in Asia at $3.74 billion in 1996.

Three weeks later Computerworld (Feb. 23, 1998) featured a story of a fired engineer doubling as his company’s network administrator and acted out corporate America’s worst security nightmare when he allegedly launched a logic bomb that wiped out all of the firm’s software, inflicting $10 million in damages.

Computer crime and information security breaches are increasing, costing U.S. corporations and government agencies millions of dollars, according to the Computer Security Institute (CSI), a San Francisco-based association of information security professionals.

The "1998 Computer Crime and Security Survey," conducted by CSI in conjunction with the FBI’s International Computer Crime Squad San Francisco, California office, uncovered a wide range of serious
intrusions. The figures were based on responses from 520 security practitioners in U.S. corporations, government agencies, financial institutions and universities.

Computer security breaches increased dramatically in only one year. Sixty-four percent of respondents reported such breaches within the last twelve month -- 16 percent more than the "1997 CSI/FBI, Computer Crime and Security Survey" results. In 1997 48 percent reported unauthorized use, a 22 percent increase over the initial 1996 survey. If the report were to also include those reporting only incidents of computer virus or laptop theft, the number increased to 88 percent of those responding to the survey.

Although 72 percent of respondents acknowledged suffering financial losses from such security breaches, only 46 percent were able to put a specific dollar figure to their losses. The total financial losses for the 241 organizations that could compute dollar figures totaled $136.8 million. This represented a 36 percent increase in reported losses over 1997 losses of $100 million. (Electric Light & Power, 1998)

In light of all the incidents reported of computer crimes and whichever survey is reviewed on the economic impact, the results are staggering and numbers are overwhelming. Computer crimes result in losses of
millions of dollars a year to various victims and the losses will likely increase significantly in future years.

It is obvious from whichever figures are examined that high technology crime needs immediate investigative and prosecutorial attention from all law enforcement agencies.
Chapter IV
Methodology

It has been determined from Chapter III's literature review that the losses caused by computer crimes are staggering and increasing exponentially. The need for investigative attention is immediate. What is the best, most efficient, most productive, method to investigate such white collar crimes?

Meyer and Short (1998) reported that results of a survey of law enforcement agencies revealed that they are inadequately equipped to investigate computer crimes. The study showed that criminals tend to be more computer literate than the police officers who investigate their activities. The most common problem cited by respondents was the lack of sufficient training in computer crime, which means that only a few officers can be involved in investigating computer crimes. Other obstacles noted were the lack of needed equipment, inadequate laws governing computer crimes and time constraints.

It is agreed that investigating computer crime is more complex than the standard crimes of homicide, burglary, robbery, and rape. Computer crime involves software and hardware that most individuals, including law enforcement officers, are unwilling to spend the
time to learn. Smaller agencies and jurisdictions will have to turn to others for assistance as their resources are even more scarce.

"Because of increases in reporting, investigators and prosecutors will have to develop ways to address these offenses [computer crimes]. Large agencies may establish full-time computer crime units. Other agencies will probably designate an investigator or prosecutor to specialize in these offenses. Many other arrangements are possible. Police departments may borrow investigators from other departments to conduct and assist in investigations. Another arrangement is the development of associations of investigators in a state or region. These associations can then call upon each other for investigations of computer crimes. Regardless of agency size, police departments and prosecutors' offices will receive more training on computer crimes." (McEwen, 1990)

Clark and Diliberto (1996) agree that law enforcement resources are stretched to the limit almost everywhere, and management does not want to deal with any crime that requires still more resources. One major problem in selling the need for training and equipment is the fact that most of these crimes go unreported. Studies show that about a quarter of all businesses that use computers have a significant loss
due to computer crime. Most are not reported because of the lack of confidence in the ability of law enforcement to investigate and reluctance by the company to admit the loss and take the blame from its shareholders.

Clark and Diliberto go on to say there is a need in computer-related investigations for both technical and investigative abilities. No single individual knows all there is to know about computer hardware, software, criminal investigations, and the law. In these investigations, even when seizing and evaluating a single computer, the job is much faster and effectively completed when two or more trained persons are involved. Good working teams of experienced, computer-literate investigators working with computer professionals who understand the techniques and purposes of preserving the chain of evidence and are qualified in the forensic evaluation of the evidence make the most successful seizure and forensic examination teams. (p. 1)

Icove, Seger and Vonstorch (1995) also agree that computer crimes call for knowledge beyond the expertise of most investigators. For this reason, it is almost always a good idea to form an investigative team to carry out every computer crime investigation. The team approach is not unique to computer crime investigation;
it is used in all major investigations. But it is more important in computer crime cases than in many types of investigations because computer crime investigations do demand special skills and expertise beyond that available to most untrained investigators. (p. 176)

Further support for specialized units is cited from Computer Crime: Expert Witness Manual (1980) which said in recent years law enforcement agencies have increased, with notable successes, the use of multi-disciplinary teams in major crime investigations. Even more than is the case for other complex white collar crime investigations, computer related crimes can be expected to require the assistance of technical experts in addition to investigative and prosecutorial resources. The interdisciplinary team approach is advocated for the effective investigation and prosecution of such cases. (p. 15)

In the August 1996 issue of the FBI Law Enforcement Bulletin, Richard Groover points out that several states have established computer crime support units, but these have not developed sufficiently to make a significant dent in the problem. The high cost of creating and maintaining such a unit makes it virtually impossible to establish a full support capability.

If departments overcome the funding and personnel
obstacles, the usual approach to law enforcement careers might need to be reexamined. Normally, police and sheriff’s departments rotate staff among the different disciplines in their departments. Such a practice might create well-rounded officers, but it would damage the departments’ computer expertise.

Computer technological knowledge and training must be comprehensive and continual. Every year, a person’s knowledge potentially becomes outdated because the technology changes so quickly. New knowledge builds on old knowledge, and personnel rotation forfeits the continuum of skill needed to deal successfully with computer-related crime.

Local law enforcement agencies also must work together to address the problems associated with computer-related crime. As mentioned, the computer field is too large in scope for most single law enforcement agencies to handle. Divide-and-conquer tactics offer the only efficient and productive solution.

One jurisdiction can become the expert on one type of hardware and certain software, while a neighboring jurisdiction can specialize in another type. Then, when a computer and its software become evidence, a team can work together to uncover the information critical to the investigation. It took teamwork to
make a dent in the drug war; the computer war will be very similar.

In a letter dated July 14, 1997 to Nevada Chief Deputy Attorney General Kevin Higgins from Sacramento County Deputy District Attorney Robert Morgester, he writes the task force concept allows the sharing and pooling of scarce resources between large and small agencies to combat high technology crime. The task force also introduced vertical prosecution to the area of high technology crime. Each participating jurisdiction has assigned a prosecutor to handle all cases from their inception to trial. Vertical prosecution allows prosecutors to learn and understand case issues in this advanced and consistently changing area.

Several law enforcement agencies throughout the country have formed high technology crime units within their jurisdictions. Whether their crime units are constructed within their own agencies or part of a multi-jurisdictional task force, computer crime is, indeed, slowly getting the attention it needs.

Law enforcement agencies are recognizing the need for specially trained professionals who will know what to look for at a crime scene. The professional will know how to deal with the crime scene in terms of obtaining the information off the computer, analyzing
the information and storing it as to not lose any vital evidence which will be necessary for a successful prosecution. The professional will also know what information is required to be included in a search warrant.
Other jurisdictions are recognizing the need for specialized units

In a brief review of various jurisdictions tackling the computer crime problem, the task force approach appeared to be the most successful, the most efficient, and the most reasonable.

"California law enforcement agencies found that the most promising approach so far is a task force in which high-tech specialists from city, county, state, and federal law enforcement agencies work together and accept assistance from industry. A statewide task force consisting of a network of regional high-tech task forces will provide several benefits to strengthen law enforcement efforts to suppress high-tech crime. By sharing and centralizing information, a task force will greatly improve the intelligence capability of each participating agency. The task force will also be a highly visible clearinghouse for information from all sources. A task force will also improve communication between law enforcement and industry. When business people are familiar with law enforcement agents, they are more likely to report crimes. A further benefit of the cooperation brought about by a task force is deconfliction, or the process of making sure multiple
agencies don’t trip over each other while investigating the same crime or criminals." (Combatting High-Tech Crime in California: the Task Force Approach, 1997)

The Nevada Attorney General’s Office turned to the Sacramento Valley High Tech Crimes Task Force as a model which has produced excellent results in recent years.

A. Sacramento Valley High Tech Crimes Task Force

The Sacramento Task Force consists of twelve state, local and federal agencies with dedicated personnel and resources administered by the Sacramento County Sheriffs Office. The Sacramento Task Force has seven investigators who work high tech crimes on a full time basis. Additional investigators also participate part time on one to two shifts per week. The task force was created with the assistance of five computer manufacturers and two cellular companies. Supporting businesses also provided furniture, office equipment, safety equipment, cash for informant fees, training and miscellaneous expenses. The Sacramento Task Force works closely with the security departments of private companies, and cases are often directly forwarded from company security investigators to the task force. In 1996 the Sacramento Valley Task Force investigated property loss of more than $14 million and recovered
more than $9 million. One hundred fifty six suspects were arrested for illicit commerce in components, burglaries, on line crimes, telecommunications fraud, financial fraud, gambling, robberies, narcotics and other offenses. (Combatting High-Tech Crime in California: the Task Force Approach, 1997)

Those successes by Sacramento Valley Task Force were largely due to several strengths of the task force approach:

* improved cooperation among different agencies
* use of investigators who specialize in high technology
* a focus on long-term investigations
* development of intelligence networks

Relationships are the linchpin to interagency cooperation. Attempting to understand and maneuver through another organization's complex rules is easier if you can work with people you know [within the task force]. These would be the same colleagues who are dedicated to the same mission. Further, it is simply more efficient to build those relationships in a structure that lasts for numerous investigations instead of rebuilding another relationship for each case that is assigned. Fortunately, technology is an ally to a far-flung task force. Long-term interagency relationships within a task force can be developed even
in such a large state as California partly through periodic meetings and partly through telephone, e-mail, and videoconferencing. (Combating High-Tech Crime in California: the Task Force Approach)

B. Other Law Enforcement Agencies

David Plotnikoff wrote in the San Jose Mercury News (March 8, 1998) that in 1986, when the San Jose Police Department became the first local law enforcement agency in the nation to add a high-tech crimes detail, fewer than 10,000 computers -- most of them government and university mainframes -- were connected to the Internet. In the beginning, the unit consisted of just one sergeant and one officer, and the focus was on the millions of dollars worth of components disappearing off the loading docks of the city's high-tech manufacturers. The unit now consists of a sergeant and four investigators who are all veteran cops, with lengthy experience in other details.

Further, he wrote, of the approximately 25 cases the team has open at any given time, between 50 percent and 70 percent are component thefts and related fraud. The team's second largest responsibility is supporting other parts of the department -- from burglary to homicide. (Whenever a computer is believed to be involved in a crime, it is the team's job to do the
seizure and the forensic search for evidence.)

Thomas Weber wrote in the Wall Street Journal (Dec. 8, 1997) of Michael T. Geraghty, a New Jersey State Police detective, who heads the agency's High Technology Crime and Investigations Support Unit. He is responsible for policing the Internet, not only for its role in crimes but also for new techniques for investigating cases. Geraghty says that while his unit handles every type of high-tech crime, the Internet now figures in about 80% to 90% of the total. Geraghty and his staff face new challenges in investigations, including the anonymity of Internet use. Internet investigations also cross many jurisdictions creating additional issues that will need to be addressed.

It is unknown exactly how many specialized high technology computer crime units have been created in recent years. However, it appears that as computer crime begins to get officials' attention (that is, officials who have the inclination to react to increasing problems and to public demands), the recognition for the need of the crime units also increases.

The Austin, Texas Police Department created a unit in February of 1995 and modeled its unit after San Jose's. The Massachusetts Attorney General's Office created a unit in April of 1997. The Illinois Attorney

Again referring to the report from California on Combatting High-Tech Crime and aside from the Sacramento Valley Task Force, California's solution is a proposal for five (5) regional task forces throughout the state. These regional task forces would model after the Sacramento Valley Task Force. Those jurisdictions with high tech crime units created within individual police departments would be converted into the formal regional task forces.

The task force approach has been tried successfully on a local and regional basis.

As in San Jose Police Department, New Jersey State Police Department, and various attorney general offices other jurisdictions have found that a special high technology crime unit is becoming essential in the fight against computer crime. Traditional units such as burglary, homicide, forgery and the fraud units cannot each dedicate their already limited resources to a computer specialist alone. Thus, police departments are beginning to realize the need for not only specialized high technology units but also that these units must also be available to regional task forces when called upon in an effort to better utilize
resources, pool efforts and avoid duplication of services.

C. Federal Efforts

The National Infrastructure Protection Center (NIPC) addresses risks and threats to critical infrastructures which would have a debilitating impact on the defense or economic security of the United States.

The NIPC is composed of 85 FBI agents and 40 governmental and private sector organizations.

Its mission is:

* to detect, deter, prevent, assess, warn of, investigate, and respond to attacks on critical infrastructures
* program manage computer intrusion investigations
* fully support the FBI's law enforcement, counter terrorism, and foreign counterintelligence missions
** support other agencies and state & local governments
* encourage sharing of information, technical expertise, and technological developments
* provide training for FBI, state and local cyber investigators, and other government
organizations
(FBI Special Agent in Charge Bobby Siller, Las Vegas field office, personal communication, April, 1998)

_Electric Light and Power_ (1998) explained the efforts of the FBI. The FBI, in response to an expanding number of cases in which criminals have targeted major components of information and economic infrastructure systems, has established International Computer Crime Squads in selected offices throughout the United States. The mission of these squads is to investigate violations of the Computer Fraud and Abuse Act of 1986, including intrusions to public switched networks, major computer network intrusions, privacy violations, industrial espionage, pirated computer software and other crimes where the computer is a major factor in committing the criminal offense.

DiDio (1998) further explained efforts by the federal government to fight computer crime. In the six years since its inception in 1992, the FBI's National Computer Crime Squad (NCCS), which is run by the bureau's National Infrastructure Protection Agency, also has broken up securities and investment fraud schemes and online gambling in addition to child pornography rings. It also investigates violations of the Federal Computer Fraud and Abuse Act of 1996 and probes electronic crimes that cross international
borders. Those include intrusions into financial, medical and government computers and networks.

Holmes (1996) wrote the national squad (NCCS) was created in 1992. Its success led to the creation of the San Francisco unit, as well as a branch in New York. The Computer Crime Squad investigates such crimes as computer network intrusions, privacy violations, and the cases of pirated computer software. In fact, the squad basically investigates any crimes in which the computer is a major factor in committing the criminal offense. If investigators find that a crime has been committed, federal charges are brought up and the party is prosecuted just as in other investigations in which the FBI has jurisdiction.

Holmes went on by explaining that part of the reason the units have been so engaged is because they each cater to areas larger than their immediate vicinity. Not only does the San Francisco unit handle California, it also deals with crimes of an international scope. The Washington, D.C. office covers computer crimes that take place in the Southeast and much of the western United States. The New York branch covers the Northeast.

Holmes continued to say that although the FBI has only three offices fully devoted to computer crimes, each of the bureau's 56 field offices has one or two
people on staff who are also equipped to deal with crimes of that nature. In fact, field offices actually handle many intrastate computer crimes, while the three units tend to stick primarily with interstate computer offenses.

Other agencies within the federal government besides the FBI are realizing the need for computer crime units.

An article in *Security Management* (1995) explained the Department of Justice’s Computer Crime Unit has recently expanded its program to help expedite investigations. The Justice Department has established a network of computer coordinators. Every U.S. attorney’s office in each of the ninety-four districts will appoint one person to keep abreast of computer legality issues. These computer coordinators will form a support network for computer crime investigations.

So many agencies are realizing the necessity to address high technology crime. However, the complexity of the technology has forced the specialization of individuals and has placed a tremendous burden on budgets. Again, the task force approach would allow agencies to share resources and avoid the duplicating of efforts. These are efforts that are often cost prohibitive to some small agencies if they did not have the option of the task force approach and make
justifying their efforts more convincing.
Nevada's Accomplishments to Date

The Nevada Attorney General's Office has developed a "Strategic Plan to Combat High Technology Crime in Nevada." For the most part, this strategic plan can be found on the Attorney General's web site at www.state.nv.us/ag.

The Nevada High Tech Task Force was organized in July 1997 at the direction of Attorney General Frankie Sue Del Papa.

The major goals of the task force are to:

* Investigate crimes involving computers and computer components, such as financial crimes, child pornography, network intrusions, consumer fraud, and theft of proprietary technology.

* Investigate computer thefts from businesses, agencies and manufacturers, including burglaries, robberies, hijacking, sales of stolen goods, etc.

* Investigate telecommunications fraud such as cell phone cloning, and theft of long-distance service.

* Provide technical forensic expertise and assistance in seizing, analyzing or copying computers and data, including expertise in
defeating passwords, cloning hard drives, burning CD ROMS, and examination of files systems or data.

* Provide prosecution assistance for all high technology crimes.

* Develop and provide training for all law enforcement officers, prosecutors and judges in the investigation and prosecution of high technology crimes; develop a cadre of certified computer forensic investigators.

* Develop and provide education and training for businesses and the general public in ways to defend against high technology crimes.

* Propose necessary legislative changes to enhance the investigation and prosecution of high technology crimes.

* Develop and provide resources and funding for high technology crime units and other goals of the Nevada High Technology Crime Task Force.

Numerous law enforcement agencies and private sector businesses throughout the State of Nevada have expressed an interest in being a part of the task force.

At this time, resources are scarce as agencies cannot dedicate individuals to a long term task force.
due to budget restrictions.

The Attorney General’s Office is seeking funds from the 1999 legislative session for seed money for the task force. The money would provide for two support positions (one for the north and one for the south) as well as money for two computer forensic specialists and equipment. Investigators would, hopefully, come from the various law enforcement agencies which are willing to support the task force on a case by case basis.

Federal grants are also being sought for additional funding as well as resources from private industry.

The Attorney General’s Office has produced 2 pamphlets for distribution to the public. "High Tech Crime: Tips for Businesses to Fight High Tech Crime" and "Keeping Your Child Safe on the Information Superhighway: A Parent’s Guide." These have been distributed to businesses and schools in the state’s effort to be proactive on this issue.
Chapter VII
Conclusions

Carter and Katz (1996) write that computer crime poses a real threat. The massive losses and setbacks experienced by companies worldwide, both private and public, have gotten the attention of administrators. The economic impact of computer crime is overwhelming. As new technologies emerge and another generation of people becomes not only computer literate but also network literate, the problems will only multiply. Just as law enforcement agencies have developed specialized criminal investigative units and prevention programs for crimes of violence and drug abuse, they must initiate similar programs for computer crime.

Computer crime units are being created throughout the country as administrators are recognizing the need to address this problem which in many areas of the world has already become out of hand.

The options of combating computer crime are limited. The option of "doing nothing" would be allowing general field detectives to attempt to prevent and solve computer crimes. This would be in addition to their already overburdened case load of burglaries, robberies, homicides, etc. Of course, the priority would lie in solving the violent and more traditional
crimes. The success rate of computer crime investigation would be measured with a zero without the specialization necessary in technical training and expertise. This is no longer an option in many areas such as Silicon Valley.

In an October, 1998 telephone interview with Deputy District Attorney Alberto Roldan who is the chief prosecutor for the Sacramento Valley High Tech Crimes Task Force, he attributed much of the success of the task force to the funding which the private sector was willing to provide.

The need for the task force was determined by a high number of thefts being experienced by the Silicon Valley companies which produce computer components. When one single company loses computer components at the rate of $1 million per week, the need for assistance is immediate. The companies were not satisfied with the law enforcement response they were being provided and agreed to assist in the funding of a high technology crimes task force. They were willing and able to provide hardware, software and training to law enforcement officers on their individual programs and systems.

Roldan stated that the Sacramento Sheriff’s Office took the lead and created the task force with 13 other agencies involved to this date. All the agencies had
an interest in the task force involvement for their jurisdictions were responsible for the computer companies in their areas. The computer manufacturers are looking to the law enforcement agencies in their area to not only express an interest and but also an ability to assist them in their positions as victims of crime. Law enforcement officials recognize the need to try to keep these large companies satisfied. It is the companies which provide jobs and profits to the community and support to them is crucial.

Compare this with Nevada.

One of Nevada’s main sources of revenue is gaming. While it has already been determined in Chapter 1 that computer crime can have an impact on gaming, it can also have a major impact on the perceived integrity by the public. Knowing this, most casinos would prefer to deny any large losses caused by a system breakdown. Casinos have shareholders to satisfy and a world-wide customer base to attract. Casinos, like many private, profit generating companies, would prefer to not acknowledge to the public that they have experienced a significant loss and would rather write it off than to expose the company to financial problems or admit system vulnerabilities.

Dillon, Groene, and Hayward (1998) wrote that owners of statutorily protected computers often prefer
to handle security problems themselves, avoiding the embarrassment of publicity focused on the vulnerability of their computers.

While there remains a large demand for computer crime units in California where the manufacturers are, the demand and desire in Nevada does not appear to be as great. However, it is in the state’s best interest to pursue a task force with the expertise necessary to handle major computer crimes. More importantly, Nevada needs all the major law enforcement agencies to make a dedicated commitment to this state task force for it to be successful.

Efforts by the Attorney General’s Office to certify computer forensic specialists have been less than successful. Four individuals have been sent to the two week course offered by the International Association of Computer Investigative Specialists (IACIS). This association offers agencies throughout the world with training for the forensic computer specialist and upon completion of the program, the specialist is then recognized as "certified." This certification allows the specialist to be called as an expert witness during a court proceeding.

After the two week classroom course, the student is expected to complete a series of tests over the course of the following year and submit their
projects/assignments to their assigned instructor.

Of the four individuals, only one has successfully completed the program which certifies an individual to be a computer forensic specialist. Two individuals, for whatever personal or professional reasons, have neglected to complete the program and their time allowed to do so has expired. The last one still may complete the requirements.

If the Attorney General’s Office is sponsoring the task force and asking other agencies to contribute time and other resources to this task force, the office should also be willing to contribute resources. This would include assuring that individuals who are sent by the office to certification training complete the commitment of the program with the full support of the office. That is, to allow the employees the time to complete their projects and to purchase the equipment necessary to do so.

Without the completed certification, the training has become useless and valuable training dollars have been wasted. (It is doubtful that the attorney general, herself, knows the certification status of the staff.)

As cited throughout this paper, numerous references have supported the need for specialized crime units or task forces. While assistance and
support from the National Infrastructure Protection Center and the local FBI office has always been available (as stated on p. 32) on a case by case basis, funding remains a number one problem.

The vision of seed money funding still has a hope, however minute, that the 1999 legislative session will provide a budget for the Nevada High Technology Crime Task Force. The 1999 legislature will soon determine the level of priority high technology crime has in the State of Nevada.
Bibliography


DiDio, Laura, (1998, April 27), Special FBI unit targets online fraud, gambling, (the FBI’s National Computer Crime Squad), Computerworld, v32.


Freedman, David H. & Mann, Charles C., (1997, June 2), Cracker: this computer geek could have taken down the networks of military sites, nuclear-weapon labs, Fortune 100 companies and scores of other institutions, U.S. News & World Report, v122.


