

# California High-Tech Task Force Committee

## **Combating High-Tech Crime in California:**



## ***The Task Force Approach***



**This document is written for:**

- law enforcement and civilian agencies of city, county, and state government
- federal agencies
- the business community
- others interested in the problem of high-tech crime in California

**Produced June 1997 by Ohlhausen Research, Inc. (peter@ohlhausen.com or 703-978-7549) for the California High-Tech Task Force Committee under a grant from the Technology Theft Prevention Foundation (15 Mountain View Road, Warren, NJ 07059; 908-903-2561).**

**For more information on the task force approach to combating high-tech crime in California, contact Robert Morgester, Deputy District Attorney, Sacramento County District Attorney's Office, 901 G Street, Sacramento, CA 95814. Phone 916-440-6274.**

## Executive Summary

---

---

The high-technology industry is a vital part of California's economy, employing some three-quarters of a million Californians at an average wage that is substantially higher than the average for non-high tech jobs. The industry produces over half of the state's total export sales, and its electronics sector alone employs more Californians than any other manufacturing sector in the state.

But high tech is under serious attack. Crimes currently rage against innovators, developers, manufacturers, assemblers, and transporters of high technology; against businesses and homes that contain computers and other equipment; against anyone who makes cellular phone calls or uses a credit card. Criminals are forcibly taking over warehouses filled with computer components; hijacking trucks; stealing proprietary business information; perpetrating subscription fraud, cloning, and toll fraud against telecommunications companies and their customers; intruding into and disrupting corporate and government computers; pirating software; counterfeiting checks; and committing many other crimes *against high-tech targets or using high-tech means, or both.*

The scale of high-tech crime in California is remarkable. Targeted products are so compact and valuable that the dollar loss per incident is particularly costly. A shoebox full of the latest, hottest microprocessors could be worth \$50,000; a briefcase can conceal motherboards, hard drives, SIMMs, or invaluable plans for the industry's next great innovation. A truckload of notebook computers could be worth well over a million dollars. In one notorious building takeover, 10 armed robbers made off with over \$9 million in computer chips. At one point, component theft was running at \$1 million per week in Silicon Valley alone. These crimes occur throughout the state, affecting not just well-known high-tech areas but also any community through which goods are transported or in which telecommunications are used. In other words, these crimes strike everywhere.

The secondary impact of high-tech crime in California is possibly worse. Many high-tech crimes are also crimes of violence; people are getting kidnapped, injured, even killed. Businesses that have been hit particularly hard have laid off employees, and others have moved out of state. Such events have a ripple effect throughout the economy, harming even residents and businesses without direct ties to the high-tech industry. If companies shrink, close, or move, fewer dollars are spent and fewer are paid in taxes. Accentuating the potential impact of damage to the high tech industry is that sector's high multiplier effect. One study found that each new job at a certain software firm created 6.7 other jobs in the state, compared with a 3.8 multiplier for the local aircraft manufacturer. Thus, the loss of each job in high tech may cause the loss of several jobs in other sectors.

Worse still, high-tech crimes are unusually difficult for law enforcement agencies to prevent and investigate. There are several major reasons:

- The criminals—both individuals and gangs—move rapidly throughout the state and the country.
- The goods stolen are small, very valuable, easy to fence, and sometimes hard to identify and trace.
- Much theft is committed by company insiders who fit no particular criminal profile. Some of those insiders are placed there deliberately by gangs.
- Stolen high-tech goods are typically sold and resold up to a dozen times within two or three days and are often quickly shipped out of the country.
- Much component theft is practiced by ethnic gangs, which are difficult to penetrate. Language and other barriers greatly complicate investigations.
- Computer crimes (hacking incidents) are so complex and sophisticated that only law enforcement officers who specialize in investigating them can hope to understand what's going on. Evidence-handling requirements and investigation methods are much different than for traditional crimes.

What can be done? The most promising approach to combating high-tech crimes is the establishment of a statewide network of regional, specialized task forces. This approach has already been tested in some locales, formally and informally, with great success. The Sacramento Valley High-Tech Crime Task Force has coordinated the efforts of several law enforcement departments and federal agencies with the advice and support of local high-tech businesses. In 1996, the task force investigated over \$13 million in property losses, recovering more than two-thirds. (Those were just the reported crimes that listed dollar losses. The task force estimates actual losses at over \$30 million in components and \$20 million in information.) The task force performed 98 original investigations, assisted in 25 others, and conducted 53 forensic investigations. Those successes 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

A number of ad hoc operations also show the strength of the task force approach. For example, Operation Bytes Dust combined the efforts of the Oakland, Stockton, and Alameda police departments, the FBI, DEA, Customs,

INS, and the California Department of Justice. The investigation resulted in simultaneous coast-to-coast arrests of some 40 gangsters involved in heroin trafficking and armed robberies of high-tech businesses. Their criminal activity ranged throughout California and stretched to Minnesota, New York, and Virginia. In Operation West Chips, the FBI, IRS, and San Jose Police Department set up a storefront to accept stolen chips and arrested 128 persons. Those operations could not have been done by any single agency—they succeeded because of multi-agency collaboration in which each agency contributed its strengths to the effort.

A statewide task force would strengthen and speed those collaborative relationships, attract the best high-tech law enforcement talent, greatly improve information-sharing among agencies, and provide a central point of contact between government and the high-tech industry, which is eager to lend its assistance.

The goal of a statewide network of regional high-tech crime task forces is this: to break the high-tech criminal network, not merely to catch crooks climbing out the back window of a store. By disabling fencing operations and gangs and intercepting those who steal U.S. technological information, the network would have the greatest chance of quashing high-tech crime.

# Contents

---

---

- 1. Introduction ..... 1
- 2. Size and Significance of the High-Tech Industry ..... 2
- 3. Scale and Impact of High-Tech Crime ..... 3
- 4. Types of High-Tech Crimes ..... 8
- 5. Challenges for Law Enforcement and Industry ..... 14
- 6. Solution: Statewide Task Force ..... 17
- 7. Matrix of Resources ..... 21
- 8. What Next? ..... 23

# 1. Introduction

---

Without a doubt, the California high technology industry is a major driver of the state's economy, and California is by far the leading high-tech state in the nation.

But high tech is under serious attack. High-tech crime is now sky-high, with half-million-dollar losses now commonplace. Criminals are busy targeting innovators, developers, manufacturers, assemblers, and transporters; businesses and homes that contain computers and other equipment; and anyone who makes cellular phone calls or uses a credit card. Organized gangs are forcibly taking over warehouses filled with computer components; hijacking trucks; stealing proprietary business information; perpetrating subscription fraud, cloning, and toll fraud against telecommunications companies and their customers; intruding into and disrupting corporate and government computers; pirating software; counterfeiting checks; and committing many other crimes.

**Definition.** High-tech crime, as defined in this paper, means both *crime against high-tech targets* (for example, theft of computer components or high-tech intellectual property) and *crime using high-tech means* (for example, computer hacking to facilitate telecommunications theft). High-tech crime often involves violence, and high-tech criminals are often also involved in low-tech crimes, such as drug trafficking.

In the sections that follow, this paper will lay out the background of the high-tech crime problem and describe the recommended solution. The paper will show the following:

- The high-technology industry is vital to California's economy.
- That industry is under serious attack by formidable criminals.
- High-tech crime is particularly challenging for law enforcement agencies to investigate and prevent.
- The most promising approach to combating high-tech crime is a statewide network of regional, multi-agency task forces composed of city, county, state, and federal law enforcement agencies, assisted by the high-tech industry itself.

## 2. Size and Significance of the High-Tech Industry

---

---

By any economic measure, *high technology matters*.

The California high-tech industry is one of the largest and best-paying employers in the state. In 1996, high-tech firms employed 724,181 Californians, up 8.2 percent from 1995. They received an average wage of \$55,160, which is 84 percent higher than that paid for non-high tech jobs. The 21,349 high-tech establishments produce \$58.8 billion in export sales (1995)—61 percent of the state's total—and high tech's electronics sector alone employs more Californians than any other manufacturing sector in the state. In fact, California's high-tech employment is double that of the next highest state.

Nationwide, the high-tech industry is one of the great engines of the U.S. economy. Its 149,873 establishments employ 4,253,767 workers at wages 75 percent above the non-high tech average. The national high-tech payroll runs to \$203.3 billion, and 1996 U.S. spending on high technology totaled some \$420 billion.

But there is more significance to the high-tech industry than size alone. What happens to the high-tech sector happens to the rest of the economy, only more so. A recent *Business Week* cover story (3/31/97) argued that the national business cycle is now tied to the health of the high-tech sector: "In the past three years, the high-tech sector has contributed 27 percent of the growth in gross domestic product, compared with 14 percent for residential housing and only 4 percent for the auto sector. Over the past year, a stunning 33 percent of GDP growth has come from information-technology industries, propelled by everything from the Internet boom to the rise of direct-broadcast satellite television." The article pointed to growing evidence that high tech has a larger multiplier effect on the economy than do traditional manufacturing industries. For example, while heavy manufacturing growth often involves substantial outsourcing to other countries with lower labor costs, "creating a new chip design or a new software program is a labor-intensive effort that relies almost exclusively on well-paid domestic workers." A study that compared the economic influence of a software firm with that of an aircraft manufacturer found that the addition of one job at the software firm created 6.7 other new jobs in the state, while the addition of a job at the aircraft manufacturer created only 3.8 other jobs.

The flip side of that positive news about high tech is this: When crime against high-tech businesses causes those businesses to lay off employees or fold altogether, will that same multiplier effect hold? Will the loss of one high-tech job

cause the loss of 6.8 other jobs in the local economy? One thing is certain: the high-tech industry is worth protecting.

### **3. Scale and Impact of High-Tech Crime**

---

---

The size of the high-tech industry may be impressive, but the scale of crime against it is truly astonishing. Losses from component theft, cellular phone and long-distance toll fraud, theft of company proprietary information, and other high-tech crimes tend to be larger than losses caused by crimes in non-high tech environments. Plenty of giant, dramatic crime incidents stand out and show just how costly a single high-tech crime can be, but high-tech crime isn't an episodic, isolated problem. These crimes take place day after day after day—\$300,000 here, \$1.2 million there—in cities throughout the state.

The impact of high-tech crime can be examined at two levels. First, it causes a tremendous, direct monetary loss. Second, it creates consequential losses and effects.

#### **Direct Impact of High-Tech Crime**

Just how much money is being lost to high-tech crime? No crime loss statistics can ever be perfect, as not every crime is detected and not every crime is reported, but a collage of figures paints a general picture.

- Worldwide sales of electronic products in 1995 were close to \$800 billion dollars. It is certainly reasonable to estimate theft loss in the billions of dollars.
- The FBI found that the average high-tech theft loss costs the victimized company almost half a million dollars.
- In 1994, component theft losses in Silicon Valley were totalling about \$1 million per week; many individual incidents caused losses over \$1 million.
- One estimate places the total annual crime loss to the U.S. high-tech industry at \$8 billion, with a potential rise to \$200 billion by the year 2000.
- One California hard-drive manufacturer reports cargo theft amounting to more than \$12 million in just the last 12 months. In one incident alone, \$2.2 million worth of product was stolen.
- In 1995, 10 armed robbers in suits and ties robbed an Irvine electronics firm of some \$9 million worth of computer chips and memory boards.

- In 1996, two delivery trucks containing \$2.7 million worth of notebook computers were hijacked from a California warehouse.
- In just two cases of remarking (changing the labeling of a component to exaggerate its specifications or claim a more prestigious manufacturer), a two-person team of California law enforcement investigators proved \$8 million worth of remarking losses.
- Nationwide theft of long-distance service is estimated at \$3.7 billion for 1996, up 12 percent from 1995. The average loss due to hacking into a company's PBX (private branch exchange) is estimated at \$90,000 per incident.
- In 1996, the Sacramento Valley High-Tech Crime Task Force investigated \$13.3 million in property loss and recovered \$9.1 million through 98 original investigations, 25 assisted investigations, and 53 forensic investigations.
- Employees of high-tech firms are being tied up and threatened during takeover robberies and have been kidnapped and taken to their place of work to let the robbers in. Truck drivers are being pulled from their trucks, beaten, and kidnapped. Informants helping law enforcement agencies investigate high-tech crimes have been murdered.

These figures are just the tip of the iceberg. Even less dramatic high-tech crimes can run up big losses fast. High-tech components' high ratio of value to size makes it especially easy to steal large dollar amounts. For example, a 20-pack box of hard drives can run \$4,000 to \$12,000; a single pallet load can be worth \$200,000. A sophisticated motherboard can be spirited away from a company in a pizza box. A briefcase could easily contain tens of thousands of dollars' worth of high-tech product. A single truck could be carrying more than \$2 million worth of high-tech goods.

### **Consequential impact of high-tech crime**

High-tech crime does more than cause companies to suffer direct dollar losses. It also imposes secondary or consequential costs on businesses, law enforcement agencies, and California communities in general.

***Business impact.*** In response to the current crime wave, insurers are raising many high-tech companies' deductibles to such high levels that the companies end up practically insuring themselves. Businesses report deductibles, per incident, as high as \$10 million. Larger companies pass those and other costs of theft along to consumers in the form of higher prices. In the case of desktop computers, theft-related costs may add as much as \$150 to the price of each unit. Smaller companies simply close their doors for good.

Some high-tech companies report difficulties in hiring new employees—in some areas people are becoming afraid to work for high-tech businesses because of the risk of armed takeover robberies, kidnapping, and threats against their families. Moreover, after a significant high-tech crime, current employees are typically too distracted or worried to work well for some time. Some even suffer stress disabilities after such incidents.

Theft of high-tech components from offices—a major problem in many areas—results in a whole range of losses. The stolen components must be replaced; the information contained on hard drives may have to be recreated at substantial cost; corporate proprietary information (customer lists, business plans, information on products in development) may be compromised; business may be idled for some time while the company gets its information systems up and running again; and the company may lose customers by being temporarily unable to serve them.

When thieves steal components (such as hard drives) and finished goods (such as notebook computers), legitimate manufacturers are injured in several ways. To preserve consumer confidence, some manufacturers choose to support stolen merchandise—even to the extent of replacing defective items with new ones. After all, in most cases the end user had no idea the item was stolen when he or she bought it. But that customer support is completely uncompensated by sales. Other companies decline to support stolen merchandise, but they pay the price in ill will among innocent buyers, and their reputation may suffer.

Several other consequential losses can affect victims of high-tech crime:

- When inferior products are remarked as coming from a better manufacturer, the poor product performance hurts the company's reputation for quality.
- When stolen goods are sold, the manufacturer loses not only the original product but also the subsequent opportunity to make sales, because at least some customers have been satisfied, having already bought what they need.
- Sometimes stolen goods are recovered. However, the short product life cycle in the high-tech industry causes the value of high-tech goods to drop precipitously after they age even a few months. Faster, smaller, and better goods constantly enter the market, so even if stolen goods are recovered, they may have lost a substantial portion of their value.
- When a manufacturer's goods are stolen, if it can't very quickly produce replacement goods, then it can't provide those goods to its customers, who may need to assemble them into their own products and may be unable to wait. The customers then have

to go elsewhere. Thus, the original victim company has lost its goods and its customers. This is not a minor problem. Companies report that high-tech crimes have caused them to lose business deals as large as \$15 million.

- Some companies are diligent about placing serial numbers and other identifiers on their products as theft countermeasures. Unfortunately, just taking those precautions is an automatic loss, as the cost of maintaining complex product tracking systems is expensive. In fact, all forms of heightened security (including physical security measures, company time spent investigating losses, and security consulting fees) are expensive. One manufacturer laments having had to spend an extra \$1 million for security in just the last year as a result of high-tech crime.

***Community impact.*** When high-tech crime flourishes and companies feel that local government doesn't take their concerns seriously, they sometime move away. When they do, they take jobs out of state; they tell other companies why they moved; newspapers pick up the story; and a city, county, or state's reputation as a place to do business can suffer. Even rampant theft of notebook computers from businesspeople who come to a city for conferences can damage that city's reputation. These secondary effects of high-tech crime are not speculation; they have already happened and have received press coverage.

Does it really matter if companies or businesspeople leave town? A look at communities limping along after the departure of the local auto plant can answer that question.

Of course, a company doesn't have to leave town for jobs to be lost. When high-tech crime hurts a business badly enough, it has to lay off workers or even close up shop. Aside from the harm to the company and employees, the community suffers the loss of tax revenue from the decrease in company and employee income.

High-tech crime has other spillover effects on a community. When cellular phone fraud is rampant, criminals work hard to obtain residents' social security numbers, credit card numbers, and other personal data. In the type of toll fraud known as call-sell operations, the potential for community violence increases as competing groups of criminals get into territorial fights over banks of phones in public places.

More ominous threats from high-tech crime must also be acknowledged. There is definitely the potential for high-tech crime to disrupt an entire community, city, or state. Cellular phone sites can be shut down by sabotage; electronic banking can be disrupted; all types of businesses (not just high-tech ones) are interrupted by the loss of computing ability; criminals snoop on people's medical and financial records; public services can be disrupted by hackers.

All these crimes are facilitated by a general climate of high-tech crime. The Internet now provides a potential pipeline into a large percentage of businesses throughout the state. That vulnerability raises the potential for information attacks by foreign powers or hackers, with drastic consequences for telecommunications systems, power grids, public utilities, and financial networks, to name only a few.

High-tech crime definitely can injure the general population's quality of life.

*Law enforcement concerns.* Of course, local law enforcement agencies have to respond first to the crimes that scare citizens the most. A report of an intruder in someone's home or an assault in progress trumps a call to investigate an open door at a computer warehouse. On the other hand, because high-tech crime has a serious impact on the community as a whole, it merits serious attention.

Responding to the scenes of high-tech crimes has become increasingly dangerous for law enforcement officers. Many high-tech burglars come prepared to turn their burglary into a robbery or even a hostage situation, bringing along tape for tying up their victims and automatic weapons for attacking the police. When responding to a call from a high-tech establishment, law enforcement officers now have to take precautions similar to those required when they respond to a bank robbery.

Another law enforcement concern is that if high-tech crime continues to flourish, the criminal organizations involved will grow larger, stronger, and richer. They will be able to invest in resources to facilitate even more crime: weapons, communications systems, storage locations, bail funds, safe houses, money to support the families of their comrades in jail, etc. Then high-tech crime will become even harder to combat.

## 4. Types of High-Tech Crimes

---

The term “high-tech crime” covers a wide range of activity. Here’s a look at what’s happening in the major categories of high-tech crime:

### **Computer Component Theft**

The high worldwide demand for computer components fuels a huge market in stolen goods. Criminals steal large quantities of the latest, most desired micro-processors, memory modules, and hard drives, along with notebook computers, printers, monitors, PCMCIA cards, and other items. Some of those goods are sold to U.S. computer dealers or consumers. Others are shipped out of the country to be built into foreign computers, which may be used overseas or exported back to the United States. The stolen property typically changes hands anywhere from three to 12 times within the first 72 hours. In fact, it’s not uncommon for the property to find its way to another part of the state (say, from Silicon Valley to Los Angeles) or offshore within hours.

The major methods of component theft are these:

#### ***Burglary and robbery at manufacturing sites, storage facilities, and retail stores.***

Some component thieves are simple burglars who let themselves into a retail store through the back window. But more criminals who burglarize and rob high-tech sites are serious, large-scale operators who do their homework. They perform careful site surveillance, collect information by sifting through company trash, plant fellow gang members inside as temporary or permanent employees, sometimes obtain blueprints of a company’s security system, and kidnap workers who have the keys to the plant. Once inside, these criminals often tie up and terrorize employees and threaten to harm their families. They also arm themselves well and have shown themselves willing to take on the police if necessary.

***Cargo theft.*** As high-tech businesses have improved the security of their buildings, thieves have turned increasingly to cargo theft. Enormous amounts of high-tech product are now disappearing in transit as thieves realize it is easier to take over one truck and one driver, for example, than a whole warehouse and its staff.

Trucks are being attacked in several ways. Criminal groups come to learn which products leave from which loading docks at a manufacturing site. They keep the freight area under surveillance, and when they notice a truck leaving from the desired dock, they notify fellow gang members, who tail the truck as it leaves town. They might block or ram the truck with their own van, steal the whole truck, and beat and kidnap the driver. Alternatively, they might wait until the driver stops to eat, then break into the back of the trailer and empty it

out. In just a minute and a half, they can relieve the truck of \$100,000 to \$150,000 worth of goods. Cargo thieves are often very bold: Truck drivers report that these criminals sometimes carry automatic weapons, and they have even been known to steal repeatedly from a truck en route as it stopped at red lights. Now even trains are sometimes hit, with containers showing up empty at their destinations.

Cargo is also stolen from freight forwarding sites at airports and shipping ports. One hard drive manufacturer reports repeatedly losing whole pallets of product—\$200,000 to \$300,000 worth—through collusion at the airport from which it ships. Even courier services are being hit: not long ago, a box containing \$150,000 in computer chips was stolen from the back of a Federal Express truck.

Cargo theft is one type of high-tech crime that can occur literally anywhere, even in parts of the state that contain no high-tech businesses at all.

***Employee theft from manufacturers.*** Employees and other insiders (such as vendors and service people) have always had the best access to company products. In the high-tech industry, because the products are typically small, many employees have been busy stuffing components into their pockets and briefcases or concealing them in the trash for later retrieval outside. If an employee steals just a single item each week, the company's loss can add up fast: One \$500 chip or hard drive multiplied by 50 weeks a year equals a \$25,000 loss.

Other employees use cleverer methods, changing company paperwork to make good product look like scrap (which they then steal instead of destroying) or stealing genuine scrap (which is typically less well secured) and selling it as first-quality product on the gray or black market.

***Theft of components from computers at non-high tech businesses and institutions.*** A quick burglary or smash-and-grab from a typical office can yield thousands of dollars' worth of computer components. Newspapers are full of reports of corporate, government, university, and other buildings being burgled out of their microprocessors, SIMMs, hard drives, monitors, and printers. In one notorious case, a Romanian national flew up and down the West Coast stealing computer components from universities, including at least four in California. He took advantage of the open university atmosphere to steal tens of thousands of dollars' worth of SIMMs. When nabbed, he had some \$20,000 worth right in his backpack.

***Fraud.*** Another way thieves steal components is simply by ordering them from the manufacturer. These fraudsters set up phony businesses, order products, pay with stolen credit cards or arrange credit via fraudulent references, and skip town as soon as they receive the goods. Such crooks work their way through the state, moving from city to city.

Component thieves are highly adaptable, altering their methods and targets to match trends. For example, as security increased at high-tech sites, they shifted from burglaries to plant invasions to kidnapping of company executives and other employees to establishing fictitious businesses to cargo theft. Similarly, as the price of computer memory dropped, thieves turned their attention to disk drives and other components instead.

## **Telecommunications Fraud**

The major types of telecommunications fraud are toll fraud, cloning, and subscription fraud.

***Toll fraud.*** This refers to theft of long-distance telephone service. Criminals use many techniques, both high-tech and low-tech, to commit these crimes. Computer hackers break into companies' PBX, voice-mail, call-forwarding, and 800-number systems to make free long-distance calls. They steal access codes and calling card numbers by searching through companies' trash, shoulder surfing (looking over the shoulder of callers at pay phones in public places), tapping into networks that transmit credit card and calling card data, bribing telecommunication company workers to hand over whole boxes of calling cards, or using ruses to trick businesses and individuals into divulging usable numbers. After they break into a company's phone system, they often steal only a little long-distance service at first, then more and more. Companies that don't analyze their bills carefully might be subsidizing hackers to the tune of \$30,000 to \$40,000 per month without realizing it, thinking only that their own use of long-distance service has gone up over time.

***Subscription fraud.*** In this scam, criminals typically commit identity theft (using stolen information to pose as someone else) to apply for cellular or land-line telephone service. They do so for several purposes: to commit toll fraud for their own communication; to run a call-sell operations, in which they charge customers a below-market rate to make calls overseas; to have an untraceable communication means to facilitate their other illegal activities; or simply to obtain free cellular telephone service. Through subscription fraud a criminal can often get away with the free use of a phone for up to 90 days before service is cancelled.

***Cloning.*** Cloning is the process of programming one cellular phone to have the same electronic security number and mobile identification number (phone number) as another. The holder of the cloned phone then makes calls on the legitimate customer's account. Cloners sit on overpasses, in train stations, and at other places where many activated cell phones pass by. There they use electronic scanners to capture phones' numbers, then program those numbers into other phones. A cloned phone is typically usable for about 30 days before being shut off. Use of cloned phones is most successful in roaming areas. Thus, it is a crime that almost always spans jurisdictions.

Observers expect 1998 and 1999 to see substantial growth in all forms of telecommunications fraud.

### **Theft of Proprietary Information**

This crime has long been a problem for high-tech businesses. Several aspects of high tech tempt competitors, both foreign and domestic, to steal proprietary information. Competition in the industry is intense; the product life cycle tends to be short, and advance knowledge of a competitor's plans can give one company an edge; production costs tend to tumble through economies of scale, but development costs run high, making it desirable to obtain new product designs without actually having to develop them; and some foreign businesses and governments are so far behind in developing technology that they feel the only way to catch up with the United States is to steal our technology.

What has gotten worse, however, is the ease with which proprietary information can now be stolen. Companies are wrestling with technological developments that jeopardize their own technology. Until recently, data had to be removed from a plant physically on a diskette; now that data can be transmitted to a buyer instantly and discreetly as an e-mail file attachment. In some companies, sensitive information held on computers can only be viewed on a monitor, not copied onto a diskette or printed out. However, with the advent of affordable compact video camcorders, thieves can now surreptitiously videotape a monitor displaying sensitive information and spirit the videotape out.

Trade secret theft is probably the greatest criminal threat to American business.

### **Computer Intrusion**

Stories of hackers and the damage they can cause are familiar to most people. Hackers break into business and government computers for several reasons: to commit fraud, to destroy or alter records, to create havoc, or simply to demonstrate that they can hack their way in at will. Stealing by means of a computer is easier than other methods and typically presents the criminal with less risk of detection and capture.

Unfortunately, hackers are altering their methods and targets to keep up with trends in the high-tech industry. In one new twist on hacking, hackers have broken into the computers of Internet service providers. They threaten to crash the companies' servers, delete customers' e-mail, and compromise the ISPs' customer databases unless the owners pay tens of thousands of dollars in blackmail.

### **Counterfeiting and Piracy**

Scanners, color printers, and other high-tech items have become so good and so affordable that criminals are using them to counterfeit checks and currency.

In the past, a counterfeiter needed some rare artistic talent. That is no longer true; all he or she needs now is the right gear.

Software piracy has also been made easier by the increasing speed and affordability of equipment that writes to compact discs. Counterfeiters race neck-and-neck with legitimate manufacturers to replicate the latest anti-counterfeiting devices: holographic stickers, printed frangible tape, etc. High tech provides both the method and the target of much counterfeiting and piracy.

## **Related Crimes**

Criminals rarely stick to one type of crime. Law enforcement agencies have found that criminals who use cloned phones are often also involved in narcotics trafficking, burglary, robbery, hacking, and other crimes. Not long ago, a kilo of cocaine was traded for a trailer full of computer components. Component thieves, when arrested, have often turned out to be wanted already on serious drug or other charges, including attempted murder.

Moreover, many other types of criminals now use computers to help organize their criminal activity. Computers often contain evidence of their owners' involvement in fraud, gambling, prostitution, stalking, and trading in stolen property and child pornography.

High-tech law enforcement units in Silicon and Sacramento valleys have noted narcotics involvement along with computer crimes they investigated. In fact, intelligence gathered from Operation West Chips, described earlier, revealed that some of the profits made from chip theft were being used to fund drug operations.

High technology—in particular, the Internet—is also facilitating more and more activity in the gray area of legality. Gray area activities include providing instructions on the manufacture or cultivation of illegal drugs, advocating anarchy, distributing hate literature, giving out bomb construction advice, and selling items that are illegal in California but not in other states or countries.

## **Victims**

In some quarters, law enforcement efforts to suppress high-tech crime have been hampered by the impression that victims of such crimes are primarily wealthy corporations or well-to-do individuals. That might have been true long ago, but now the victims or potential victims of high-tech crime include anyone who uses a telephone or credit card; any community through which trucks pass; any community that is home to small computer shops or mail-order computer businesses; large high-tech companies, which often have to raise their prices because of crime; small high-tech companies, which sometimes go out of business because of high-tech crime and which tend to be less tuned into security measures than large businesses; and any institution that uses

computers (because of component theft from non-high tech sites). It is hard to think of any type of community, business, or person not affected by high-tech crime.

## 5. Challenges for Law Enforcement and Industry

---

---

The preceding sections have shown that the high-tech industry is important, that high-tech crime is occurring on a large scale and in many forms, and that some high-tech criminals are formidable. Still, very little that law enforcement agencies do can be called easy. What makes high-tech crime such a special challenge for law enforcement?

### Unfamiliarity

It is easy to forget that much about high tech is quite new. As a group, law enforcement officers have fallen behind in the computer age and have a lot to learn, including such basic matters as what the various components of computers look like and are called; how to preserve evidence discovered on a computer; how to handle high-tech items; and how to prevent suspects from destroying evidence before their very eyes.

If high-tech items are unfamiliar, it's hard for officers to know just what they're looking at in, say, a traffic stop. A shoebox full of microprocessors could be worth tens of thousands of dollars, yet to officers unfamiliar with high technology, the contents might appear to be just a pile of little gizmos. One major California computer manufacturer worked to support the development of a high-tech task force in its area because of inadequate law enforcement response to its crime problems: Officers often wouldn't come when the security manager first called for help; when they did come, they came slowly; they didn't seem to know what computer parts were; and they didn't do anything beyond taking a report. That unenergetic type of response generally is a result of unfamiliarity with the subject matter of the crime.

### Complexity

Of course, some criminal justice professionals are familiar with high technology. However, even for them it is especially complicated to investigate and prosecute high-tech crimes. How does one investigate an intrusion into a mainframe computer? What must be done so the evidence will stand up in court? How would one know whether a suspect has stolen trade secrets?

Some police investigators simply don't go near high-tech crimes because they are too complicated, too involved, and too time-consuming. An officer handling computer crime needs a much lower caseload than other officers. In addition, if a high-tech crime investigation is handled poorly, law enforcement agencies can end up being embarrassed or even sued (for interfering with electronic bulletin board service operators who claim they're publishers, or for damaging a computer network or e-mail system). An experienced high-tech

prosecutor put it this way: When working high-tech crime, police are walking on eggshells.

## **Other Difficulty Factors**

***Geographic stretch.*** High-tech crime is almost always transjurisdictional. Not only do component thieves move their goods out of a jurisdiction quickly, but they also move themselves around the state and country. Crimes committed electronically (via modem) may originate anywhere in the world. In fact, a single act of high-tech crime may contain steps in several countries. For example, in toll fraud, because some crooks know that calls to Haiti are monitored closely, they first call Canada and then loop their stolen calls to Haiti.

***Language and cultural barriers.*** Much high-tech crime is committed by ethnic gangs, which are notoriously difficult to investigate. Gang members typically share a culture and language that an officer in the local police department does not possess and cannot imitate. Language and cultural barriers also separate police from some victims of high-tech crime. After a takeover robbery, terrorized employees might not have much to tell the police, in part because they don't speak English and in part because their families have been threatened.

***Small size, high value.*** It's been said before, but many high-tech items (especially microprocessors and proprietary information) are worth more than their weight in gold. However, they are not protected nearly as well as gold typically is. Anytime something small and valuable is the target of theft, it's a challenge for police, who have to work against the ease of concealment and criminals' high level of temptation.

***Ease of fencing.*** If there were only a few places to fence stolen high-tech goods, police would know where to focus. However, in high tech, the demand for goods is so high that fences are numerous. For both small-time and big-time thieves, components are very easy to sell. Also, thieves can get a high price for high-tech goods—up to 50 percent of the item's value, as opposed to the more common 10 percent for other goods. Small-time thieves can sell to component dealers that advertise in computer publications; big-time thieves satisfy demand worldwide.

***Insider aspect.*** Estimates suggest that as much as 75 percent of theft from businesses may be by insiders, and insider theft is always difficult for police to investigate. Employees, vendors, and others who are allowed access to a company's site are in an especially good position to cover their tracks.

***Untraceability.*** High-tech components have been called the dope of the '90s. That is true in some ways, but in other ways high-tech crime is even more complicated to combat. For instance, to any officer encountering stolen product, it may not be obvious that it's stolen; it's not illegal for someone to pos-

sess high-tech items, so just spotting them doesn't point to a crime. A quick analytical test or sniff by a dog could tell an officer whether a discovered substance was an illegal drug. By contrast, it's hard to identify some high-tech products and determine whether they were stolen. The situation is made more difficult by poor product marking (lack of manufacturers' names and serial numbers on products).

***Lack of reporting.*** It's especially difficult to investigate high-tech crime that isn't reported. Some companies have been reluctant to let large thefts become public knowledge. Why? They fear their stock prices will be affected; they don't want to advertise their vulnerability to other criminals; and some lack confidence in law enforcement's ability to respond. One study suggests that only 18 percent of trade-secret thefts are referred to law enforcement for prosecution.

## **6. Solution: Statewide Task Force**

---

To address high-tech crime adequately, California law enforcement agencies need a high level of computer knowledge; foreign language resources; assistance in tracking criminals to distant locales; a rapid flow of intelligence; and certain financial and equipment resources. 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.

### **Interagency Communication and Information-Sharing**

The sophistication of high-tech criminal organizations, such as the South American Connection and various Asian gangs, makes it impossible for a single local agency to track enough data to stop them. Such a group's stolen goods network extends over many, many jurisdictions. By sharing and to some extent 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. In other words, agencies throughout California, the United States, and potentially the world will know to whom they should send high-tech crime information (on names and activities of suspects, modus operandi in specific crimes, and crime trends) and from whom they can get it. Analysis of those trends will help the task force focus its investigations on the most urgent areas and work to prevent emerging problems.

A task force will also improve communication between law enforcement and industry. When businesspeople are familiar with law enforcement agents, they are more likely to report crimes—it's a matter of knowing who to contact. Also among the benefits of increased reporting are increased leads into other high-tech crimes. For example, when a cellular phone company learns of a cloning case and turns it over to police, it typically turns into something even bigger, since cloners are often engaged in theft, hacking, narcotics, counterfeiting, and fraud and may even be involved with international crime rings.

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.

### **Relationships and Resource-Sharing**

The rapid exchange and transport of stolen high-tech components and information creates problems for agencies that are used to dealing primarily with

crimes within their own jurisdictions. Interagency cooperation can be difficult, particularly between local and federal agencies, because each agency has its own rules, procedures, and chain of command. Sorting out the conflicts takes time, and high-tech crime moves too fast for that.

Because a task force operates with a single set of policies and procedures, it can act much faster. In addition, the unique resources of each agency represented (both local and federal) can be brought to bear on a particular investigation as needs arise. Those resources, explained more fully in Section 7 below, include geographic reach, application of different laws, different capabilities to search, and strengths in investigating different types of crimes.

Relationships are the linchpin of interagency cooperation. Navigating another organization's complex rules is easier if you can work with people you know. Further, it is simply more efficient to build those relationships in a structure that lasts for numerous investigations instead of constructing a new relationship for each case that comes along. 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.

## **Expertise**

Technological expertise is essential if law enforcement is to make any dent in high-tech crime. In many agencies, there is no high-tech unit and the only expertise available comes from officers who happen to be personally interested in computers.

A task force will make a big difference in the level of expertise that California can employ against high-tech crime. First, a task force will attract talented people—it will look like a desirable assignment, not a position that puts one's career on hold. Second, by allowing for a longer assignment period, it will hang onto knowledgeable people. The learning curve for a computer-crime investigator is so steep that most officers are just becoming valuable when they are transferred. Third, it will help its members improve their knowledge. It's easier to obtain organized training from industry for an identified group like a task force than for dozens of separate agencies. Task force members will be better able to keep up-to-date with the latest techniques in high-tech investigation. (Those techniques are constantly evolving. For example, at an arrest, police may not always want to unplug a suspect's computer; useful evidence might be coming in by modem.) Federal law enforcement agencies bring with them additional training opportunities.

The desktop computer is the smoking gun of the '90s, and the expertise the task force develops will help it with forensic analysis of the computers it seizes. The task force will also become an identifiable source of expertise for other

law enforcement agencies and industry and be able to direct them in developing their own forensic capabilities.

Also, whereas some local law enforcement agencies have shied away from taking on particularly complex high-tech cases, they will now have somewhere to send those cases: the task force.

### **The Big Picture**

The California statewide high-tech task force will not be about quashing minor thefts or stopping someone from making an extra copy of his software. Its goal is to disrupt the high-tech crime network, to suppress fencing operations—simply to make it less attractive to steal high-tech goods and information. The task force will be big enough and sophisticated enough to undertake the necessary enforcement measures: long-term surveillance and intelligence gathering, especially on organized criminal groups; undercover purchases; use of confidential informants; reverse stings; storefront operations; and other techniques suited to preventing crime, not just reacting to it.

### **Financial Benefits**

The high-tech industry—both individual corporations and associations—will be more likely to provide financial and other resources to a centralized task force than to dozens of separate agencies. In addition, giving funds or equipment to a task force is a way that the industry can support the effort to fight high-tech crime without putting any individual law enforcement agencies in the appearance of a conflict of interest.

•••••

There's more to the task force approach than just benefits—there's a real urgency to get going. Temporary task forces and one permanent one have succeeded in reducing losses in a few sectors of high-tech crime. But criminals don't stay down for long. It takes time and effort to set up a task force, and now's the time to make that effort. A new, hotly sought high-tech product will appear, or prices for one component or another will rise, and the criminals will be back in businesses.

In fact, with the shutting down of the particularly successful Operation West Chips (in which the FBI, IRS, and San Jose Police Department set up a storefront to accept stolen chips and arrested 128 persons), California's ability to gather timely and valuable intelligence on high-tech crime has been weakened, opening the door for organized crime groups to reestablish themselves. Criminals have always had the flexibility to recover from setbacks, and in fact police have identified several individuals and businesses that are expected to fill the void left by the arrests of their associates.

By going active now, while some criminal organizations are gravely disabled, authorities stand a better chance of developing deep access to the criminal organizations, which is needed to provide the intelligence necessary to keep those groups down. In addition, before the relationships and methods developed in Operation West Chips go stale, they should be made permanent through the institution of a California high-tech task force.

A further reason to move fast toward developing a California high-tech task force is this: A task force is one of the best ways for law enforcement agencies and prosecutors' offices to develop and maintain high-tech expertise. Over time, without such expertise, there will be a whole range of crimes—high-tech and low-tech—that they simply won't be able to deal with. High-tech crimes will continue to present all the investigative challenges described earlier, and much of the evidence of low-tech crimes (gambling, prostitution, etc.) will be stored on criminals' computers and will require special handling to be usable in court.

A California statewide high-tech task force will benefit all those involved:

- Businesses, regardless of whether they help support the task force, will get their problems investigated better. They will be more willing to report problems because they will see that law enforcement has become organized, funded, and committed to fighting high-tech crime. Companies that support the task force can show that they're helping the community at large by combating fraud, child pornography, and other crimes that harm a community. A task force also provides a neutral setting in which competing companies can get together to share information. And by helping to dismantle the network of fences, the task force will help even those companies that are experiencing mainly internal, not external, theft.
- Law enforcement will obtain and develop both experts and the leads needed to solve high-tech crimes.
- The whole community will benefit—this approach is not going to be just an industry police force. A good task force can be one of the factors that influences where a company builds a new plant or office. The government response to the high-tech theft problem can either draw or repel businesses, jobs, and taxes.

## 7. Matrix of Resources

In a statewide high-tech task force, each participating agency has something special to offer. Here's a list of a few of the key resources that could be contributed by each envisioned member of the task force or its steering committee. Note: the following are not necessarily all the bodies that should be represented on the task force or steering committee, and the strengths and resources listed are just a sample.

<b>Task Force Members</b>	<b>Strengths and Resources Offered</b>
City and county law enforcement agencies (police and sheriffs' departments)	<ul style="list-style-type: none"> <li>• best knowledge of local conditions</li> <li>• ability to move quickly</li> <li>• close relations with high-tech companies for sharing information and giving advice</li> <li>• fast, local decision-making</li> </ul>
Prosecutors (district attorneys' offices)	<ul style="list-style-type: none"> <li>• ability to carry out vertical prosecution (useful in complicated high-tech cases)</li> <li>• ability to provide legal advice for search warrants in high-tech investigations (to help law enforcement avoid legal traps)</li> </ul>
State agencies (California Department of Justice, Office of Criminal Justice Planning, and California Highway Patrol)	<ul style="list-style-type: none"> <li>• management of task force funds</li> <li>• intelligence repository</li> <li>• elimination of local jurisdiction problems</li> </ul>
Federal agencies	
– Customs Service	<ul style="list-style-type: none"> <li>• broad authority to search inbound and outbound cargo</li> <li>• experience in financial investigations</li> </ul>
– FBI	<ul style="list-style-type: none"> <li>• ability to enforce different statutes than state agencies can</li> <li>• ability to work wiretaps, long-term investigations, and confidential informants</li> <li>• agents in place throughout country and world</li> <li>• elimination of jurisdiction problems in multi-state investigations</li> </ul>
– INS	<ul style="list-style-type: none"> <li>• ability to track and deport criminals who are in U.S. illegally</li> </ul>
– IRS	<ul style="list-style-type: none"> <li>• experience in financial investigations</li> <li>• ability to prosecute for money laundering and tax evasion</li> <li>• ability to discover criminals' identities by following the flow of funds</li> </ul>
– Secret Service	<ul style="list-style-type: none"> <li>• experience in NY high-tech task force</li> <li>• specialized training and equipment for investigating telecommunications fraud</li> </ul>

	<ul style="list-style-type: none"> <li>• major focus on computer-related crimes</li> </ul>
--	--

<b>Steering Committee Members</b>	<b>Strengths and Resources Offered</b>
High-tech businesses	<ul style="list-style-type: none"> <li>• high level of interest and enthusiasm</li> <li>• ability to teach task force members about latest targets of theft</li> </ul>
Trade and professional organizations	<ul style="list-style-type: none"> <li>• ability to train and educate law enforcement officers and the public</li> <li>• ability to analyze some recovered products</li> <li>• experience at conducting and funding research</li> </ul>
Insurers	<ul style="list-style-type: none"> <li>• central point for collection of information on losses</li> <li>• experience at conducting and funding research</li> </ul>

## 8. What Next?

---

One proposal calls for the California statewide high-tech task force to start with five regional task forces. They would contain the following counties: (1) Sacramento, Placer, Yolo, and El Dorado; (2) Santa Clara, Alameda, and San Mateo; (3) Orange and Los Angeles; (4) San Diego and Imperial; and (5) Riverside and San Bernardino.

The task forces would be staffed with detectives from municipal, state, and federal agencies. Each county would provide a deputy district attorney to handle vertical prosecutions of offenders. Each regional task force would be guided and assisted by a regional steering committee, which would include representatives of nearby high-tech companies. A statewide steering committee, also including corporate representatives, would work with the Office of Criminal Justice Planning to decide how funds should be allocated to the local task forces based on performance and need and would require progress reports. The Sacramento Valley High-Tech Crime Task Force, already in place, is very close to the type of regional task force envisioned. Santa Clara and Irvine already have relationships in place that could quickly be converted into formal regional task forces.

The high-tech industry originated in Silicon Valley, and high-tech crime was a natural outgrowth. As technology has developed and the industry has spread, so has the crime problem. Coordinated, dedicated high-tech task forces are a natural answer to the unique problems associated with investigating and prosecuting those crimes. The task force approach has been tried successfully on a local and regional scale. At this point, the only remaining question is that of funding.

To put costs in perspective, a single successful high-tech task force operation can save high-tech firms and the people who work for them tens of millions of dollars and put away many dozens of criminals. When that kind of money is put back into the taxable stream, government will receive more revenue.

This paper noted earlier that high-tech businesses may move if they feel neglected by local government. The flip side is that high-tech companies are more likely to stay in areas where they feel they are being taken care of. A major computer component manufacturer in Irvine recently reported that it was considering building a new facility out of town. That decision would have had a negative economic impact on the city and possibly the state. However, the company decided to stay in Irvine in part because it felt it received good cooperation from the Irvine Police Department on high-tech crime matters.

There is some urgency to setting up a statewide task force. High-tech crime is growing and spreading; criminals and criminal organizations are getting

stronger, richer, better equipped, and better organized. Independent, small-scale defensive measures aren't good enough in the high-stakes fight against high-tech crime. As one victim of multimillion-dollar high-tech crimes put it, "You don't fight a war by constantly building bigger and stronger bomb shelters. You have to devise a strategy and then attack." A statewide network of regional high-tech task forces *is* that strategy.