

THE HIGH TECHNOLOGY INDUSTRY AND
LAW ENFORCEMENT – A CRITICAL PARTNERSHIP

Article

California Commission on
Peace Office Standards and Training

by

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

Command College Class XXXII

Sacramento, California

June 2002

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

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

As a senior manager for a San Francisco Bay Area law enforcement agency with over 20 years of police experience, I have seen how technology has affected my agency, as well as how law enforcement has responded to high technology crimes. I have spent a good portion of my law enforcement career as an investigator, supervisor and manager of investigative units and have witnessed law enforcement's slow response to high technology crimes.

In my opinion, the main reason for law enforcement's low response is that most law enforcement agencies are poorly equipped and lack the expertise to properly investigate and prosecute the wide variety of high technology crimes facing American law enforcement today, and certainly in the future. When you consider that there are 18,769 local law enforcement agencies in the United States, the vast majority being agencies of less than 50 sworn personnel, it becomes obvious that American law enforcement currently faces significant logistical, operational, communication and technological challenges.

Law enforcement has established various types of task forces to address specific community related problems in the past. Community Oriented Policing is the best example of the public and private sector coming together to address the causes of crime (i.e. broken window theory). Additionally, law enforcement has formed very successful multi-agency task forces to deal with organized crime, narcotics trafficking and vehicle theft. Most recently, task forces have been established to investigate terrorism and high technology crimes that use the private sector on a limited basis. In my opinion the time has come for the high technology industry to become more involved in computer and technology related crimes.

The high technology industry has the unique opportunity to protect its investment and at the same time provide expertise to enhance public safety and national security. Many believe that the success of the U.S. economy during the late 1990s and into the 21st century is attributable in part to the booming high technology industry, especially in the geographical region known as Silicon Valley, located in the San Francisco Bay Area.

The success of the high technology industry and the emergence of new technologies will forever change the way law enforcement views its relationship with the private sector.

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

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

Public/Private Partnerships – Then and Now

Beginning in 1940, the U.S. economy was flooded with new technologies that initially were kept clandestine due to the country’s involvement in the war effort. These technologies included mainframe computers, atomic energy, rockets, commercial aircraft, automobiles and television. Following World War II, these technologies were utilized for civilian use and coupled with the creation of the World Bank and the International Monetary Fund helped finance these new technologies. This public/private partnership resulted in a tremendous surge in the U.S. economy during the 1950s, which continued

into the 1960s. During the 1970s, the U.S. economy began to slow, which ultimately resulted in high inflation and later a world recession.³

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

Experts estimate that by 2005 the global population of Internet users will reach approximately 300 million. By 2010, 95 percent of people in the industrialized world and 50 percent of the developing countries will be online.⁵ This future forecasting of Internet expansion, wireless technology, and user expertise during the next ten years would create significant opportunities and as well as threats to the global economy, national security and individual privacy. For example, in June 2001 the Intel Corporation announced that it had created the world's fastest silicon transistor that turns on and off nearly 1,000 times more quickly than those that power today's microprocessors.⁶

Information technology is reshaping the logic of everything from business strategy to work to pop culture. It's also reshaping the logic of crime: what it looks like, how it takes place, and how we as a society choose to fight it. We're seeing more identity theft, illegally obtaining a credit-card number, a social security number, or other information. As we become a cash-less society, electronic banking will no doubt make our financial lives simpler, but it will also make it easier for criminals to access our bank accounts. The Willie Sutton Principle still applies, "Criminals go where the money is."⁷

The Internet for instance has made cyber crime easier to commit. In July 2001, a Russian programmer was indicted on charges of violating the Digital Millennium Copyright Act of 1998, which forbids software designed to thwart copyright. The Russian programmer, Dmitry Sklyarov, helped write a computer program for ElcomSoft that strips the copy protection from electronic books made by Adobe Systems of San Jose, making it possible to duplicate the books freely. FBI agents arrested Mr. Sklyarov when he arrived in Las Vegas to attend a hacker conference.⁸ Even though the charges against Mr. Sklyarov were eventually dropped, this case is a good example of how far reaching cyber crime can be.

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

The tragic events of September 11, 2001 may be the catalyst that ignites the sense of urgency in both law enforcement and the high technology industry to forge closer working relationships. For example, the recent tightening of security at U.S. airports in response to the terrorists attacks has unleashed a flood of technology designed to

intercept potential terrorists before they act. This type of technology has the ability to offer security at the expense of constant surveillance. Whether society is willing to pay that cost is yet to be determined.⁹

In a 2000 survey of 276 private sector organizations, the FBI discovered that 95 percent of them suffered a computer intrusion and many of those reported that each incident cost an average of 1 million dollars.¹⁰ Generally, the high technology industry has the lead responsibility in operating the global information infrastructure, security requirements, standards, design and implementation. It is of vital economic interest for businesses worldwide to cooperate with stakeholders, public and private, to provide for a secure infrastructure.¹¹

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

The high technology industry must do its part in the war against cyber crime. The high technology industry must share information while still protecting the privacy of

others. Each high technology company should be encouraged to share non-proprietary information concerning threats, vulnerabilities, protective measures and effective information security practices. The industry should also cooperate with law enforcement in reporting incidents of cyber crime, while respecting laws or other agreements regulating the collection, processing and disclosure of personal data.

However, there will be instances in which the high technology industry will need to provide law enforcement with access to proprietary information that each company restricts to its highest corporate officers. Of course, this information needs to be protected by law enforcement to ensure future cooperation from the high technology industry. This will require that state and federal evidence codes be amended to protect the proprietary information from disclosure during court proceedings.

The California Evidence Code for example allows law enforcement officers to invoke a privilege that is designed to protect informants or certain information from being disclosed to the defense. This procedure allows the trial judge (neutral party) to review the information and weigh the consequences of non-disclosure versus the right of a defendant to cross-examine evidence and witnesses used against him in court. This process should be extended to all proprietary and sensitive company information that may be disclosed during a normal trial or as a matter of public record.

The high technology industry should also provide training and expertise to law enforcement agencies concerning the latest developments in technology. This recommendation challenges any high technology company with a new business idea that radically changes the market. These companies need to weigh the public benefits of

allowing law enforcement access to the inner workings of the new technology versus their desire for increased profit margins and market share.

An Alternative for the Future

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

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

enforcement information. The private sector investigators and technicians/analysts would provide logistical, technological and high technology security assistance.

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

The task force would also accept cases directly from the high technology industry, thus making it easier for victim companies to report high technology crimes that will forge closer working relationships with the high technology industry. Since prosecutorial resources are limited on both the state and federal levels, each high technology case would be evaluated to determine which court system would give the best probability for a successful prosecution.

Steering Committee

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

large enough to represent the participants involved in the task force, but small enough to conduct normal business.

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

Personnel

The personnel that will comprise this task force would consist of full and part time local and state law enforcement officers from the two contiguous counties that would work side by side with their federal and private sector counterparts. These investigators should have a good understanding of computer technology, Internet capabilities, network security and criminal investigation procedures. The investigative team would confer with the prosecuting attorney who would be handling the case for assistance with legal advice and case strategy.

The private sector investigators would provide their unique perspective and expertise to the task force that can only come from having inside knowledge of the latest advances in industry hardware and software. The private sector investigators and technicians would become the backbone of the high technology investigative task force.

Unlike the law enforcement investigators who may transfer back to their respective agency every 2-3 years (promotions, normal transfers etc.), the private sector investigators and technicians will most likely stay with the task force for longer periods of time. These individuals would provide the institutional knowledge and stability that any task force or organization needs to continually be successful.

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

Funding Sources

Every successful program has several critical elements that can be attributed to its continued success. One of those elements is identifying and receiving adequate funding sources. The high technology investigative task force will need to identify and secure funding from several governmental sources. There are several avenues for the task force to obtain the funding they will need to investigate complex high technology crimes effectively.

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

Transition Management

A Transition Management Plan is imperative to the success of a new program, particularly one such as what is being proposed which can spread over many years and encumber a significant amount of personnel and financial resources. Commitment to the program from the stakeholders and the identification of relevant issues impacting the program are critical to developing an effective program.

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

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

Conclusion

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

We need not wait until 2007 to see the results of these consequences. High technology crimes are increasing and these are only the ones that are reported to law enforcement. Many high technology investigations either lack proper investigative follow up or are not investigated at all. Communities, such as in the San Francisco Bay Area, that have dedicated high technology investigative units, continue to have success, but they could be even more successful if private industry is allowed to play a greater but supervised role in the investigation of high technology crimes.

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

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

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

ENDNOTES

¹ Mintz, Howard. "Reno Urges Teamwork on Battling Cyber crime." San Jose Mercury News. April 5, 2000. Online. Silicon Valley News. Accessed: September 22, 2001.

² Ibid.

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

⁴ Ibid.

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

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

⁷ Futurist, Cyber Crime. Gene Stephens. Class handout December 6, 2000.

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

⁹ Staedter, Tracy. Technology Review. "Face Recognition." November 2001.

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

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

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

BIBLIOGRAPHY

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

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

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

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

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

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

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

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

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

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