COPING WITH CYBERCRIME
IN
THE TWENTY FIRST CENTURY

Article

By

Captain Edwin F. Flint
Sacramento County Sheriff’s Department

Sacramento, California

November 16, 2001
The year is 2006 and a new paradigm has emerged. The world is now considered a unified and peaceful global society, sophisticated and technologically advanced. Third world countries reap the benefits of lightening speed technology, elevating them to a new plateau in society. In this New World Order (NWO), traditional warfare is not politically correct. The United States, Russia and China still hold their titles as superpowers and continue to have significant nuclear capabilities. Together they have formed a Tri-Lateral Commission to prevent global proliferation of nuclear arms. The World Court established by the United Nations during the Clinton administration settles global conflicts and disputes between nations. But while the physical world appears at peace, the clueless society has been slumbering and a new frontier of war games has blossomed in epic proportions. This new breed of war is more machiavellian and destructive than history has ever seen, causing global conflict, vulnerability, security breeches, and terrorism in a new world called Cyberspace.

Sophisticated networks of international thugs, thieves and criminals emerge as a real and problematic national security threat. The year 2006 is marked by Russian, Chinese, Nigerian, Middle Eastern, and Italian gangs that have enthusiastically embraced globalization and technology to expand their criminal domains and elude police. In an emergency effort, the U.S. National Security Council calls for the world’s law enforcement agencies to begin treating Internet terrorism, cybercrimes and copyright violations committed by these perpetrators as crimes against the NWO and haggler over jurisdiction in the World Court by means of reciprocity, denying sovereignty of nations, and stirring the already heated debate of civil liberties.
In retaliation, the global underworld launches an all-out attack against NWO’s critical information infrastructures and declares war in the universe of cyberspace, holding the global society hostage. The 3-day attack cripples global computer networks to a near shutdown of medical services, telecommunications, electrical power grids, banking and financial institutions, and oil and gas production. Global terrorists capitalize on the confusion, bribing corporations and nations for millions of dollars in return for information security and reduction of the threat to completely destroy the electronic infrastructure.

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

Sound plausible? It is. You may be unaware, but the above scenario describes a future world by the year 2006 that will arguably be more real than fictional. The advent and popularity of the computer and its interconnectivity brought about by the Internet has given birth to a whole new species of white-collar criminals. The Internet provides clever hackers with a high degree of anonymity. Encryption is making investigations doubly hard, affording criminals protection from law enforcement intrusions. Since computer networks regularly cross city, county, state, and even national boundaries, figuring out who has jurisdiction is tricky. Extradition and
prosecution issues are often unclear. Many of the existing laws were written long before cybercrime was a problem. Jurisdictional boundaries and the confusing patchwork of laws make some types of behavior legal in one state and illegal in another. The Internet has an estimated fifteen to twenty-five million users in ninety-two countries and is growing at the rate of five to eight percent per month. The pace of change is relentless. Computer technology now surpasses itself with a new generation roughly every three years. As computer crimes become ever more audacious—and those who commit them ever more sophisticated—law enforcement must somehow keep up.

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

The current situation is that local law enforcement officers know how to handle a domestic violence call, and they are familiar with what to do when someone breaks into a home. But many do not know what to do if you make a purchase over the Internet that never arrives and the money you sent has disappeared. Law enforcement officers are confronted daily with new investigative and evidentiary issues that demand a high
level of technical knowledge about computers. To compound this situation, most state and local law enforcement agencies lack adequate training, equipment and staff to combat electronic crimes. Few officers are adept in investigating computer crime, and few prosecutors are adept at prosecuting computer crime. Those officers with the expertise to investigate cybercrime work for state or federal agencies, large police departments or a multi-jurisdictional task force. Officers in smaller departments often struggle to deal with a wide range of cybercrimes and training opportunities are limited.

It is imperative for law enforcement, especially in California, to prepare now for this rapidly impending future of Internet based white-collar crime. This futures study attempts to examine how California law enforcement should and will respond to the need for computer-based expertise in the identification, collection and preservation of electronic evidence in the year 2006. Futures research is concerned with the effects of social, technological, economic, environmental and political trends on alternative futures ten to twenty years from now. It is based on the premise that undesirable/desirable futures can be either avoided or created by intelligently made choices. The three principle goals of futures research are: 1) form perceptions about the future, 2) study possible alternative futures, and 3) make choices to influence desirable futures.

A variety of methodologies were employed to assist in achieving these three principle goals, such as scanning the social, technological, economic, environmental and political environments; conducting a comprehensive literature review of applicable books, magazines and newspaper articles, and periodical reports; several interviews with law enforcement and educators associated with computer crimes; and a type of brain-storming session, known as the Nominal Group Technique (NGT), with working
professionals from law enforcement, educational institutions, and the high technology industry.

Three major themes emerged from the research. First, high technology crime is on the rise and is proportionate to the rapid increase and change in technology. The use of the Internet to commit fraud, identity theft, auctions and information theft leads the way in high-tech crimes. Secondly, law enforcement is having a difficult time coping with the volume and complexity of high technology crimes. The criminals appear to have the upper hand. They are more sophisticated and knowledgeable about technology and use that knowledge to elude law enforcement. Finally, by all indications, law enforcement is ill prepared for the tremendous increase in cybercrime. There is a critical shortage of trained forensic specialists, high-tech investigators, as well as a lack of computer-based knowledge by field officers and investigators.

The research was used to develop three likely scenarios for the future—optimistic, pessimistic, and surprise free. The purpose of developing scenarios as a planning tool is to identify large-scale forces that impact and affect the future in different ways. It’s about making these forces visible, so that if they happen, the planners will at least recognize them. In a sense, the scenario is a tool that helps us study not only the possibilities of the future, but also our subjective involvement with those possibilities. Faced with the pessimistic future scenario, a strategic plan was designed to assist a mythical Turley Police Department response to the overwhelming demand for computer-based expertise within the organization by the year 2006.

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

There are many strategic planning models from which to choose; however, they all must address three basic questions: 1) Where are we going? 2) What is the environment? and 3) How do we get there? I selected the Applied Strategic Planning Model described in Leonard Goodstein, Timothy Nolan and J. William Pfeiffer’s book, “Applied Strategic Planning: How to Develop a Plan that Really Works,” because of its continual focus on application and implementation throughout the entire process and my familiarity with the planning process.

The outlook for curtailing cyberspace crime by technology or conventional law-enforcement methods is bleak. Most agencies do not have the personnel or the skills to cope with such offenses, and to date all high-tech approaches have been met by almost immediate turnabouts by hackers or crackers. In the future, many more users will possess skills far beyond those of today’s cyber criminals—a process termed by experts as “the democratization of computer crime.” Electronic crime will get more sophisticated as cyber criminals lead law enforcement toward higher technology. Cybercrime probably cannot be controlled by conventional methods. Technology is on the side of the cyberspace offender and motivation is high—it’s fun, exciting, challenging, and profitable. As individuals see and talk to each other over computers in the next few
years, and as nanotechnology makes computers even more portable, new technology will emerge to protect data. But simplifying systems to make them more universally acceptable and accessible will also make them more vulnerable to intruders.

There are those who predict that computer crime and crimes perpetrated across the Internet will be California law enforcement’s biggest problem in the future. And they say that this future is not far off. This futures study is meant to give us a serious look at where we are headed by the year 2006 in high technology crime, and for law enforcement to begin an appropriate course of action to be prepared for the coming generation of cyberspace wars.


2 Ibid., p. 4


BIBLIOGRAPHY


