*Harvard Journal of Law & Technology*
Volume 10, Number 3 Summer 1997

# WHY THE POLICE DON'T CARE ABOUT COMPUTER CRIME

*Marc D. Goodman*[*]

## TABLE OF CONTENTS



---

* M.P.A., John F. Kennedy School of Government, Harvard University, Class of 1997. Mr. Goodman is a Senior Sergeant/Investigator for the Los Angeles Police Department.

## I. WHY THE POLICE SHOULD CARE

*The world isn't run by weapons anymore, or energy, or money. It's run by ones and zeros — little bits of data. It's all electrons .... There's a war out there, a world war. It's not about who has the most bullets. It's about who controls the information — what we see and hear, how we work, what we think. It's all about information.*[1]

### *A. Nightmare Scenario*

A hacker breaks into the computer systems at Brigham & Women's Hospital at four o'clock on a Monday morning. Before most of the doctors arrive to treat their patients for the day, the malicious computer intruder changes a number of patient files on the hospital's central database system: surgeries slated to be performed on the right leg are now switched to the left leg; recorded blood types are altered from AB-negative to O-positive; warnings for known allergies to medicines such as penicillin are electronically erased from patients' charts; and laboratory records on HIV blood test results are insidiously switched from negative to positive just before patients are to receive their results. The computer intruder effectively covers up all electronic evidence of the crime, and though lives will be lost, the police are powerless to act.

This scenario is a real possibility with current technology. Police forces, however, are not prepared to investigate it. In the first section of this paper, I will discuss why police departments need to work to combat computer crimes. In the second section, I will lay out why this has not happened yet. Finally, I will propose some approaches for preparing departments to police the digital world.

### *B. Atoms, Bits, and Bytes*

The world has been accustomed to dealing with atom-based objects. Things made of atoms are those that we can see, touch, and feel, such as a collection of Shakespeare's plays or an Elvis Presley recording. In the middle of the twentieth century, however, something changed. With the advent of computer technology, electronic bits were born. As Nicholas Negroponte tells us, "[a] bit has no color, size, or weight, and it can travel at the speed of light. It is the smallest atomic element in the DNA of information."[2] Despite these physical properties, bits can be made to represent atom-based objects or analog forms of information. Speech,

---

1. As stated by Cosmos, the villain in the movie *Sneakers*. SNEAKERS (MCA/Universal 1992).

2. NICHOLAS NEGROPONTE, BEING DIGITAL 14 (1995).

text, music, photographs, and video can all be represented in a digital format.

As technology has improved over time, the amount of digital information that can be stored on a single chip has increased exponentially.[3] "Moore's Law" tells us that computer processing power doubles every eighteen months.[4] At the same time, costs of home computers have plummeted since they were introduced twenty years ago. The decreased costs to consumers and increased computational speed have encouraged more and more individuals to own powerful computer processors.[5]

Another trend that has pushed forward the digital revolution is the networking of home and business computers through the Internet. This interconnectivity ties computer users around the globe together in real time so that information retrieval is no more difficult in Johannesburg than in Jacksonville.[6] Those who doubt the success of the Internet need only look at the thirty-seven million-plus Americans who in 1995 had access to it, either directly or indirectly through a friend, co-worker, or commercial online service such as America Online.[7] "Metcalfe's Law" explains that the value of a network increases geometrically with the number of nodes or computers attached.[8] Given this and the clear trend toward more Internet use, it is likely that the number of computer systems connected to the Internet will continue to increase sharply in the years to come.[9]

Computers, like most other tools, can be used for either legitimate or criminal purposes. As the number of computers expands globally, there will be a concomitant rise in both the good and bad purposes for which they are put to use. Greater numbers of cheap, networked computers available to the general public also means greater numbers of cheap, networked computers available to the criminal elements in society.

Communities, individuals, governments, and businesses are legitimately availing themselves of the increasing sophistication and utility of information technology. Networked together, these computers

---

3. *See* Philip E. Ross, *Moore's Second Law*, FORBES MAG., Mar. 25, 1996, at 116.

4. *See* Christopher Anderson, *The Accidental Superhighway*, THE ECONOMIST, July 1, 1995, at S3, S4.

5. *See* THE WORLD ALMANAC & BOOK OF FACTS 1997 212 (Robert Famighetti ed., 1996).

6. *See generally* CLIFFORD STOLL, THE CUCKOO'S EGG: TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE (1989).

7. *See* Peter H. Lewis, *Another Survey of Internet Users is Out and This One Has Statistical Credibility*, N.Y. TIMES, Oct. 30, 1995, at D5.

8. *See* Anderson, *supra* note 4, at S4, S8.

9. *See id.* at S3, S8.

have created a digital infrastructure upon which society has come to depend heavily. This is important for law enforcement officers because computer networks used for legitimate purposes are subject to attack and disruption at the hands of computer-savvy criminals.

Publicly-switched telephone systems, air traffic control networks, police and fire dispatch centers, and utility companies all rely upon computers and information networks to provide their vital services to the public.[10] This National Information Infrastructure ("NII"), as it has come to be called,[11] is now fundamental to our way of life; both the government and the private sector have become increasingly dependent upon it.[12] As our national computer systems become more intertwined with other networks around the world, we will see the NII connect to the Global Information Infrastructure.[13] Since more and more critical information, such as military data, trade secrets, and hospital patient records, will be put into computer networks,[14] their protection will become more vital, yet at the same time more difficult. This increased difficulty will arise because the linking of computer systems means they can be attacked from anywhere in the world via a telephone line.

### *C. Definition of Computer Crime*

There is disagreement nationally and globally as to what exactly constitutes a computer crime.[15] The term "computer crime" covers such a wide range of offenses that unanimity has been an elusive goal. For example, if a commercial burglary takes place and a computer is stolen, does this constitute a computer crime, or is it merely another burglary? Does copying a friend's Microsoft Excel disks constitute a computer crime? What about sending obscene pictures over the Internet? The answers to each of these questions may depend entirely upon the jurisdiction in which one finds oneself.[16]

Computer crimes can be divided into three general categories: crimes where a computer is the target, crimes where a computer is a tool

---

10. *See* ROGER C. MOLANDER ET AL., STRATEGIC INFORMATION WARFARE: A NEW FACE OF WAR, xiii (1996), available at (visited Apr. 15, 1997) <http://www.rand.org/publications/MR/MR661/MR661.pdf>.

11. *See* Al Gore, *Bringing Information to the World: The Global Information Infrastructure*, 9 HARV. J.L. & TECH. 1, 1 (1996).

12. *See* Exec. Order No. 13010, 61 Fed. Reg. 37,345 (1996).

13. *See* Gore, *supra* note 11.

14. *See* MOLANDER ET AL., *supra* note 10.

15. *See* P.A. Collier & B.J. Spaul, *Problems in Policing Computer Crime*, 2 POLICING & SOC'Y 307 (1992).

16. *See* Jodi Mardesich, *Laws Across the Country Become Relevant in Connected World; Jurisdiction at Issue in Net Legal Cases*, SAN JOSE MERCURY NEWS, Oct. 8, 1996, at 1E.

of the crime, and crimes where a computer is incidental.[17] When a computer is the target of a crime, an innocent party's computer system is attacked by a criminal computer intruder. Some examples include trespass, vandalism, sabotage, theft of intellectual property, extortion based on threats to release information stolen from a target's computer system, and terrorist activities threatening parts of the NII for political purposes. If a computer is a tool of the crime, the computer is used to commit an old crime in a high-tech way. Examples of this include creation of counterfeit currency or official documents using computer scanners and graphics programs, embezzlement using a computer to skim very small sums of money from a large number of accounts, distribution of child pornography on the Internet, and theft of digital property. Other crimes can also be committed on the Internet: fraud, hate crimes, stalking, gambling, and money laundering. A computer is incidental to the crime if the computer itself is not required for the crime, but is used in some way connected to the criminal activity. Examples include a threatening letter that was written and stored on a computer, financial records on a drug dealer's machine, and an inculpatory bomb recipe discovered on a computer hard drive after an explosion in the neighboring town.

### *D. Computer Criminals*

For computer crime, as with most crimes, it is valuable for law enforcement to have a "profile" of the average offender in order to investigate and solve a given offense. Since most police officers have yet to encounter a computer crime case, their sense of a high-tech criminal's profile has come not from the police training academy, but from the media. Many police executives still believe the prevalent myth of the neighborhood hacker[18] envisioned in the 1983 film *War Games*.[19] In the movie, actor Matthew Broderick innocently breaks into the computer systems of the United States Strategic Air Command and accidentally launches a countdown to nuclear war. Though the aforementioned stereotype of a hacker as an innocent, maladjusted,

---

17. *See* David Carter, *Computer Crime Categories: How Techno-Criminals Operate*, 64 FBI L. ENFORCEMENT BULL., July 1995, at 21; Scott Charney, *Computer Crime: Law Enforcement's Shift From a Corporeal Environment to the Intangible, Electronic World of Cyberspace*, 41 FED. B. NEWS & J. 489, 489 (1994).

18. *See generally* BRUCE STERLING, THE HACKER CRACKDOWN: LAW AND DISORDER ON THE ELECTRONIC FRONTIER (1992).

19. WAR GAMES (Metro-Goldwyn-Mayer 1983).

teenage nerd might have been true in the early- and mid-1980s, such is not the case today.[20]

Although there are some relatively innocent hackers left, many of the computer intruders today are malicious and often motivated by greed.[21] Skilled computer hackers today are in great demand, often finding employment with organizations such as the Italian Mafia, Colombian drug cartels, Chinese Triads, or Russian organized crime.[22] Their motives range from greed to intellectual challenge, and the profile of each must be considered when investigating high-tech violations.[23] Of course the greatest threat from computer crime will continue to come from the "insider."[24] Law enforcement officers familiar with the problem of retail theft know that most losses occur from employees, not from shoplifters or robbers.[25] Armed with inside knowledge and access to their employers' computer networks, employees may pose new security risks for all types of organizations.

### *E. Why the Police Should Be Concerned About Computer Crime*

According to Kenneth Rosenblatt, Deputy District Attorney for Santa Clara County, California, "our society is about to feel the impact of the first generation of children who have grown up using computers. The increasing sophistication of hackers suggests that computer crime will soar as members of this new generation are tempted to commit more serious offenses."[26] Furthermore, ever-increasing numbers of people today have the ability to learn computer skills and thus have the opportunity to use them for nefarious purposes. Colleges, universities, and technical schools graduate large numbers of computer experts each year, many of whom have the ability to exploit their knowledge for illegal purposes.[27] One expert at the United States Department of Justice has gone so far as to suggest that by the year 2000, nearly 90% of

---

20. *See* Wade Roush, *Hackers: Taking a Bite Out of Computer Crime*, TECH. REV., Apr. 1995, at 32, 34; *see generally* STERLING, *supra* note 18.

21. *See* Roush, *supra* note 20, at 36.

22. *See* Joshua Cooper Ramo, *Crime Online: Mobsters Around the World are Wiring for the Future*, TIME DIGITAL, Sept. 23, 1996, at 32.

23. *See* STERLING, *supra* note 18, at 58-59, 177-78, 185-86.

24. *See* Rory J. O'Connor, *Computers Vulnerable to Insiders*, SAN JOSE MERCURY NEWS, Mar. 6, 1997, at 3C.

25. *See* Mary Guthrie, *Firms Target Employee Thefts*, L.A. TIMES, Jan. 7, 1993, at D7.

26. Larry E. Coutorie, *The Future of High-Technology Crime: A Parallel Delphi Study*, 23 J. OF CRIM. JUST. 13, 14 (1995).

27. *See generally* STAFF OF SENATE COMM. ON GOV'T AFFAIRS, PERMANENT SUBCOMM. ON INVESTIGATIONS, 104TH CONG., SECURITY IN CYBERSPACE (Comm. Print 1996) [hereinafter SECURITY IN CYBERSPACE].

criminals might be computer-literate.[28] Even if that number seems inflated, it should certainly cause some alarm in the world of law enforcement.

In addition, traditional barriers to crime faced by former generations of thieves, thugs, and convicts are being obliterated by digital technologies. In a digital world, there are no state or international borders; customs agents do not exist. Bits of information (contraband and otherwise) flow effortlessly around the globe, rendering the traditional concept of distance meaningless. In the past, the culprit had to be physically present to commit a crime. Now, however, thanks to the digital revolution, a thief can steal millions of dollars from anywhere on the planet simply by moving bits of electronic ones and zeros into his own bank account.[29] Cybercrimes can be committed from anywhere in the world as bits are transmitted over wires, by radio waves, or via satellite. Today, a theft in Los Angeles could just as easily be committed by a criminal in Minsk as one in Malibu.

Information stored in computers may also be more vulnerable to attack than data stored in paper format. Traditionally, companies protected their secrets and bank funds in locked file cabinets and vaults.[30] These locked boxes were located in offices, which themselves were locked in buildings surrounded by electronic fences and armed guards.[31] In the digital world, all of a company's proprietary information may be located on one computer server that is connected to dozens, hundreds or even thousands of other computer systems around the world.[32] Any one of these networks or even a phone line into a company's main computer is a transnational invitation to crime. The person on the other end of the remote computer login session could be a legitimate student user, a business person, or a computer enthusiast. But, she could also be a member of an organized crime group, a saboteur, or even a foreign intelligence agent.

Crime in the digital world has another advantage for crooks over "atom-based" crime: electrons and bits have no effective mass or weight. If one were to rob a bank or an armored car of two million dollars in cash, transportation and storage of the stolen goods would pose a problem. A thousand pounds of U.S. currency is hard to carry away from the bank and even more difficult to hide under one's mattress. In

---

28. *See* Richard S. Groover, *Overcoming Obstacles: Preparing for Computer-Related Crime*, FBI L. ENFORCEMENT BULL., Aug. 1996, at 8.

29. *See* Saul Hansell, *Citibank Fraud Case Raises Computer Security Questions*, N.Y. TIMES, Aug. 19, 1995, at 31.

30. *See* SECURITY IN CYBERSPACE, *supra* note 27, at 14-15.

31. *See id.*

32. *See id.*

the digital world, however, money has no weight.[33] The theft, transportation, and storage of electron-based money, or other digital goods for that matter, is greatly facilitated by the fact that they are without mass. A billion dollars of electrons weighs no more than, and is just as easy to transport as, ten dollars of electrons. Thus, the potential to steal large amounts of cash and other goods without detection is enormous.

### *F. Computer Crime Is on the Rise*

Given the advantages of digital crime over its analog counterparts and the growing number of computer-literate thieves, it is undoubtedly in the interest of police agencies to learn as much as possible about computer crime now, while there still remains a possibility of catching up with these criminals.[34] The trends in digital crime grow more alarming each year. According to a 1995 study by Ernst & Young, at least twenty companies responding to an annual security survey had suffered losses exceeding $1 million as a result of computer break-ins.[35] The Business Software Alliance estimates the lost revenue resulting from software piracy alone amounts to $2.8 billion per year.[36] Cellular phone companies lost an estimated $650 million last year to fraud committed by crooks who altered the software in wireless phones to make free calls.[37] A recently-closed "electro-bookie" gambling operation run by the mob in New York City was found to be processing thousands of "marks" each day, netting members of the Gambino, Genovese, and Colombo crime families nearly $65 million per year.[38] Over $2 trillion in international wire transfers happen every day.[39] As Citibank recently found out when its computer network was compromised by a crime group in Russia, even the paltry sum of $10 million can be quite enticing.[40]

---

33. *See infra* notes 41-45 and accompanying text.

34. *See* David L. Carter & Andra J. Katz, *Computer Crime: An Emerging Trend for Law Enforcement*, FBI L. ENFORCEMENT BULL., Dec. 1996, at 1.

35. *See* Peter H. Lewis, *Losses From Computer Breaches Are on the Rise, a Study Finds*, N.Y. TIMES, Nov. 20, 1995, at D2.

36. *See* Elizabeth Corcoran, *In Hot Pursuit of Software Pirates: Industry Sends Out Private Investigators to Fight $15 Billion Trade in Illicit Copying*, WASH. POST, Aug. 23, 1995, at F1.

37. *See* Ruth Larson, *Secret Service Nabs 259 on Cellular-Phone Fraud: "Cloned" Phones Seized*, WASH. TIMES, June 18, 1996, at A4.

38. *See* Ramo, *supra* note 22.

39. *See* SECURITY IN CYBERSPACE, *supra* note 27, at 34.

40. *See* Hansell, *supra* note 29.

### G. Other Trends of Concern to Law Enforcement

A number of recent technological developments will significantly frustrate police in their search for cybercriminals. The introduction of budding technologies such as digital cash and sophisticated encryption programs may render it impossible to track future generations of digital wrongdoers. Digital cash technology has existed for several years. For example, DigiCash is a plastic card with a small microprocessor chip that can be used instead of atom-based cash.[41] The introduction of digital cash may eventually mean the decline of real currency as legal tender.[42] These cards have cash values encoded on them but contain no information linking the DigiCash card to its user.[43] Any transaction paid for by DigiCash will be completely anonymous.[44] While possibly a boon to Internet commerce and to those who wish to keep their names and personal shopping habits hidden from credit card companies, electronic payment systems like DigiCash will make it possible for criminals to transfer large sums of money for illegal purposes in a manner that is completely undetectable by law enforcement.[45] Indeed, DigiCash may make today's problems with money laundering seem like child's play.

As if the difficulties in policing a world with digital cash were not daunting enough, the introduction of widely available, highly sophisticated, computer-based encryption programs may mean the demise of incriminating evidence in many cases.[46] Encryption uses mathematical algorithms to convert digital information into a different format so it cannot be decoded without a password.[47]

Of course, there are legitimate uses for encryption. Sent over the Internet, e-mail and other computer files often pass through dozens of computers between sender and recipient. The contents can be copied and viewed anywhere along their path. Encryption prevents unautho-

---

41. *See DigiCash — Numbers That Are Money* (visited Mar. 16, 1997) <http://www.digicash.com/publish/digibro.html>.

42. *See* Kelley Holland & Amy Cortese, *The Future of Money*, BUS. WK., June 12, 1995, at 66; *see generally* Joshua B. Konvisser, Note, *Coins, Notes, and Bits: The Case for Legal Tender on the Internet*, 10 HARV. J.L. & TECH. 321 (1997).

43. *See Digicash — Numbers That Are Money*, *supra* note 41.

44. *See* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 462 (1996).

45. *See Money in CyberSpace* (last modified Feb. 3, 1997) <http://www.ustreas.gov/treasury/bureaus/fincen/cybpage.html>; Vanessa Houlder, *Cash Versus Cashless — Electronic Money Is Becoming a Reality but Questions Remain Over Privacy and Fraud*, FIN. TIMES, Feb. 20, 1996, at 11.

46. *See* Julian Dibbell, *Keys to the Kingdom: Cryptography, the Black Art of Spies and Diplomats*, TIME DIGITAL, Nov. 11, 1996, at 38.

47. *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 714 (1995).

rized reading of the files. The military, government, banking institutions, and other businesses and individuals all have legitimate reasons for wanting to use encryption. But, just as bad guys today wear gloves to cover up their fingerprints, the techno-criminals of the future will use encryption to cover up their electronic tracks.[48] Police agencies must come to grips with these changes taking place in the world of evidence collection and preservation. Officers must be trained to follow the digital equivalent of a "blood trail" if they wish to be able to investigate and prosecute the growing number of criminal offenders in the digital world.

### *H. Technology-Based Attacks Against Law Enforcement Will Increase*

Not only is technology being used by criminals to further their illegal enterprises, but computers, cellular phones, and other sophisticated electronic devices are being used to gather counterintelligence on police operations.[49] When agents of the United States Drug Enforcement Administration recently conducted a raid at the Cali drug cartel headquarters in Colombia, they discovered two large IBM mainframe computers.[50] The computers were hooked into the national telephone service of Colombia and stored the phone records of millions of Cali residents.[51] These phone records were routinely cross-checked against calls made to the United States Embassy in Colombia and the Colombian Ministry of Defense in an effort to identify Colombians who were cooperating with government drug enforcement efforts.[52]

Federal, state, and local law enforcement agencies and officers can expect to come under increasing attack as digital criminals increase in sophistication. When notorious hacker Kevin Mitnick was targeted by specific law enforcement officers, he would routinely change the police agent's voice-mail greeting at work, cancel or re-route an officer's home telephone service, and even add lines of negative annotations to credit reports of judges and probation officers with whom Mitnick had disagreements.[53] Police agencies may find their 911 systems interrupted, their encoded radio transmissions intercepted, their proprietary databases altered, and intelligence relating to impending drug raids pilfered by

---

48. *See* Vic Sussman, *Policing Cyberspace: Cops Want More Power to Fight Cybercriminals*, U.S. NEWS & WORLD REP., Jan. 23, 1995, at 54.

49. *See* Ramo, *supra* note 22.

50. *See id.*

51. *See id.*

52. *See id.*

53. *See* TSUTOMU SHIMOMURA & JOHN MARKOFF, TAKEDOWN 238 (1996).

cybercriminals who attack at the heart of police command, control, and communications systems.[54] If police agencies cannot appreciate the importance of preparing for technology-based attacks against others, surely they can see the wisdom of self-preservation.

### *I. Computer Systems Remain Vulnerable*

The Computer Emergency Response Team ("CERT") was founded by the Defense Advanced Research Projects Agency ("DARPA") in 1988 to coordinate responses to computer crises and emergencies such as those described earlier.[55] Although police agencies might prefer to leave the investigation of computer crime to specialists such as CERT, they cannot. CERT provides advice and serves as a repository of information for victims of computer crime, but it has no power to conduct any type of criminal investigations. This means that police agencies will be called upon to handle the escalating number of computer crimes.

A study recently completed by the Defense Information Systems Agency ("DISA") demonstrates how vulnerable even "secure" information systems are to attack.[56] DISA has been performing proactive computer hacking on behalf of the government for the past three years.[57] These computer specialists attempt to break into Department of Defense ("DOD") computer systems using only those tools commonly available on the Internet to all other hackers.[58] Based upon an estimated 30,000 attempted electronic penetrations performed as of May 1996, DISA has been able to break into 65% of the systems in under one week.[59] DISA estimated that given more time, it could break into 95-98% of the DOD's unclassified computer systems.[60] The DOD computer network managers affected by the penetrations only detected these intrusions 4% of the time and only reported 27% of those to the appropriate security or law enforcement personnel. Thus, the intrusions by DISA were not reported 98.92% of the time! If there is a 98.92% failure rate in detection and reporting on the military's computer systems, what is the corresponding rate in the civilian world?

---

54. *See* SECURITY IN CYBERSPACE, *supra* note 27, at 153-55.
55. *See* Carnegie Mellon University, *CERT Coordination Center* (visited Mar. 14, 1997) <http://www.cert.org/>.
56. *See* SECURITY IN CYBERSPACE, *supra* note 27, at 37.
57. *See id.*
58. *See id.*
59. *See id.*
60. *See id.*

### *J. Cyberspace Laws Are Expanding*

Whether or not criminal justice agencies want to deal with computer crime may become a moot point in the very near future. Legislators around the nation are passing a flurry of new laws relating to cyberspace.[61] Currently, every state except Vermont has enacted some form of computer-crime statute.[62] At both the federal and local levels, police organizations are being tasked by legislative bodies to assume the responsibility of digital crime enforcement.[63] Thus, law enforcement agencies are being required to update their tactics and techniques for the twenty-first century. Those police departments that earnestly rise to the occasion may be able to make the case for increased funding and training to meet the demands imposed by these new laws. In contrast, those police chiefs who fail to prepare for these new responsibilities may find themselves in conflict with the mayors and city councils who have appointed them.

### *K. The Most Important Reason Why Police Departments Should Be Concerned About Computer Crime*

Law enforcement officers should be concerned about high-technology crime because society has placed the burden upon them to do so. The people have entrusted the police to protect them and their property. The prevention of crime and the apprehension of offenders are duties that the law places on the police. The fact that the nature of crime may change over time and make their role more difficult does not relieve law enforcement agencies of their fundamental responsibility to protect all citizens from crime. The Law Enforcement Code of Ethics reminds all police officers:

> As a Law Enforcement Officer, my fundamental duty is to serve mankind; to safeguard lives and property; to protect the innocent against deception, the weak against oppression or intimidation and the peaceful against violence or disorder; and to respect the Constitutional rights of all men to liberty, equality and

---

61. *See* Xan Raskin & Jeannie Schaldach-Paiva, *Eleventh Survey of White Collar Crime: Computer Crimes*, 33 AM. CRIM. L. REV. 541, 562 (1996).

62. *See id.* at 563.

63. *See, e.g.*, 18 U.S.C. § 1029 (1996) (high-tech fraud and counterfeiting); Communications Decency Act, Pub. L. No. 104-104, 110 Stat. 56 (1996) (codified in scattered sections of 42 U.S.C.); ARK. CODE ANN. § 5-41-103 (Michie 1993) (computer fraud); CAL. PENAL CODE § 502 (Deering 1996) (computer trespass).

> justice . . . . I recognize the badge of my office as a symbol of public faith, and I accept it as a public trust to be held so long as I am true to the ethics of the police service. I will constantly strive to achieve these objectives and ideals, dedicating myself before God to my chosen profession . . . law enforcement.[64]

Although the concept of "digital crime" may be difficult for many police executives to accept and understand, they must ensure that their departments are ready and able to handle such offenses when they occur. Law enforcement practices and policies have changed in response to changes in society before. Although high-technology crime may be more difficult to comprehend than other events demanding change, the police have a moral obligation to prepare well for the future digital crime wave.

Given the previously enumerated, significant trends in computer crime, one might expect that police departments would be scrambling to improve their ability to investigate high-technology crime. Unfortunately, this is not the case. For a variety of fiscal, cultural, and political reasons, computer crime is not a high priority for the vast majority of law enforcement agencies. The impediments to changing this situation are described in the next section of this Article.

## II. WHY THE POLICE DON'T CARE

"*I think it is going to take a lot of people dying, unfortunately, before anything will be done about computer crime.*"[65]

Simply stated, computer crime is not a priority for police departments around the world. In a time when greater and greater emphasis is being placed on issues like violent crime reduction and community-based policing,[66] the detection and investigation of computer-related offenses remains an elusive goal. When asked about the lack of serious progress in the fight against computer crime, police executives almost unanimously cite "money, money, money" as the principal impediment.[67] However, the true reasons for law enforcement's lackadaisical approach to handling digital crime are much more complex and enigmatic.

---

64. SANTA CLARA POLICE DEPARTMENT CODE OF ETHICS (1960).

65. Glenn D. Baker, *Trespassers Will be Prosecuted: Computer Crime in the 1990s*, 12 COMPUTER L.J. 61, 63 (quoting Kenneth Rosenblatt, Deputy District Attorney for Santa Clara, California).

66. *See generally, e.g.*, Barbara A. Webster & J. Thomas McEwen, *Assessing Criminal Justice Needs*, NAT'L INST. OF JUST. RES. IN BRIEF, Aug. 1992.

67. *See* Groover, *supra* note 28.

Computer crime has been recognized as an enforcement dilemma for at least two decades,[68] yet the majority of police agencies seem unconcerned with its presence or effects. Although some strides to investigate and prosecute such crimes have been made recently,[69] the challenges facing the police in their struggle to catch up with the hackers, crackers, and crypto-anarchists of the digital world remain formidable. Despite the recent increase of technology-related crime, 72% of police departments and 88% of sheriff's departments do not have units that specialize in the area.[70] In this section of the paper, I will examine why law enforcement agencies have been slow to recognize and deal with these acts of criminal misconduct, despite the increasing threat they pose to society.

Before the public, the business world, and policymakers can begin to change the current state of affairs, they must first understand why the police do not seem to care about digital crime. Some of the reasons include: police culture itself, the invisibility of digital crime, the difficulty in investigating high-tech crime, an abundance of "real crime," a lack of public outcry on the subject, and the high cost of computer training and specialized units.

### *A. That's Not Why I Became a Cop!*

When rookie police officers are asked why they chose a career in law enforcement, most cite reasons such as "I wanted to help people" or "I wanted to arrest bad guys." Many officers developed their sense of job description well before they joined the police force. Television shows such as *Dragnet*, *Adam-12*, *Starsky & Hutch*, *S.W.A.T.*, *Hawaii Five-0*, *Hill Street Blues*, *Cagney & Lacey*, and *T.J. Hooker* influenced generations of young men and women to consider a career in law enforcement. However, the newest members of the police service find out quickly that they do not get into blazing gun battles every day of the week. There are no daily vehicle pursuits and not all crimes are solved in sixty-minute episodes.

Yet many officers still long to be heroes. The culture of law enforcement is one in which machismo and physical bravery are greatly rewarded. Indeed, the highest honor most police departments bestow upon their own is the "medal of valor," an award given only to a select few crime-fighters who risk their lives in order to save others. Rescuing people from burning buildings, arresting gang members who are armed

---

68. *See* Bill D. Colvin, *Computer Crime Investigators: A New Training Field*, FBI L. ENFORCEMENT BULL., July 1979, at 9.

69. *See* Webster & McEwen, *supra* note 66, at 4.

70. *See id.* at 4-5.

with AK-47s, and pursuing neighborhood rapists in long foot chases over backyard fences are the types of activities that garner officers the accolades of their peers and promotions from the police brass. Uniformed patrol officers and personnel assigned to high-risk duties such as the Special Weapons and Tactics ("SWAT") team see themselves as the "thin blue line" between anarchy and a peaceful society. These officers are perceived to be the *real* cops.

Of course, there are other cops — police officers who work mostly inside as detectives, desk officers, and administrative officers. The functions assigned to this group of individuals are not accorded the same level of respect given to *real* cops. There is an omnipresent undercurrent of social stigma against those who fulfill less dangerous duties in law enforcement, and derisive names are commonplace: "desk jockey," "station queen," "house mouse," "pogue," and "squint" are among those most frequently heard. When investigating computer crime, life-and-death emergencies are rare; thus far, no medals of valor have been awarded for "cybersleuths." Since the internal culture of police departments places a lower value on catching non-violent offenders,[71] it should come as no surprise that officers are not clamoring to investigate computer crimes.

At a time when most police departments cannot keep up with the hectic pace of constant 911 emergency calls,[72] the thought of dedicating scarce resources to the "fuzzy" concept of computer crime is very hard to sell to most police chiefs. Rapes, murders, drive-by shootings, auto theft, and drugs are all higher on the priority list than computer crime.[73] While many people call the precinct captain to complain about drug dealers in their neighborhood, few, if any, call to complain about "those darn hackers!" Indeed, as I will discuss later, the invisibility of digital crime is one of the major reasons why most police executives can afford not to care about the problem, *for now*.

Other reasons why police departments have been very slow to respond to digital crime issues include lack of computer savvy and the fear of technology, or "technophobia."[74] Technophobia is a serious problem for both police officers and the public at large. According to a recent survey by the Dell Computer Corporation, 55% of the population

---

71. *See* Collier & Spaul, *supra* note 15, at 311.

72. *See* MALCOLM K. SPARROW ET AL., BEYOND 911: A NEW ERA FOR POLICING 105 (1990); Gordon Witkin & Monika Guttman, *This is 911 . . . Please Hold*, U.S. NEWS & WORLD REP., June 17, 1996, at 30, 31.

73. *See Reno Attacks House Budget Plan to Cut Crime Funds*, Reuters World Service, Mar. 17, 1995, *available in* LEXIS, News Library, Wires File.

74. *Cf.* Raoul Vincent, *Police Hope to Nab Criminals in Their Own World Wide Web*, CHI. TRIB., May 19, 1996 (Evening Update), at 2; STERLING, *supra* note 18, at 194.

suffers from some fear of or hesitation about technology.[75] Compounding the problem is the insufficient training law enforcement personnel receive on either computer usage or computer crime. Very few, if any, departments train recruits on high-technology issues. Any computer training that does occur is generally only on how to use proprietary law enforcement and criminal database systems for the purposes of checking for warrants and stolen vehicles. At best, these are rudimentary skills that do not prepare police officers to combat computer-related crime.[76] According to a 1995 University of California study, 40% of police professionals receive no formal training on computers.[77] An additional 20% of police professionals receive no more than two hours of computer instruction.[78] This by no means suggests that police officers as a whole are incapable of learning these skills; rather, it illustrates how far they have to go before they will be prepared to tackle sophisticated computer crime. Since police officers, like other human beings, do not like doing things they are not good at or do not understand, they will continue to ignore high-technology crime until it becomes impossible to do so any longer.

Rank-and-file officers are not alone in their lack of understanding of high-technology issues. The problem also affects higher ranking officers. The majority of senior law enforcement officials have been neither formally nor informally trained in the use of computers.[79] When today's police managers first joined the force in the 1960s, computers were almost unheard of. All a good beat cop needed then was a baton, the ability to fight well, and a "nose" for finding criminals. Police work today, however, is more complicated. New tools are required to meet the challenges posed to law enforcement officers in the twenty-first century. Unfortunately, however, many police chiefs think they can "get by" without having to dedicate additional resources to the issue of high-technology crime because that is what has been done in the past.

Thus, many agencies have tried to "fake it" or "make do" when it comes to handling computer crime. A police chief might designate the most proficient WordPerfect user as the department's "computer expert." To the uninformed, it might make sense that the same officer who is capable of creating the precinct newsletter might be capable of conducting a forensic examination of a UNIX mainframe computer. Nevertheless, this is certainly not the case. Police departments that look internally

---

75. *See* Kevin Hogan, *Technophobia*, FORBES MAG., Feb. 28, 1994, at 116.

76. *Cf.* Alana Northrop et al., *Police Use of Computers*, 23 J. CRIM. JUST. 259, 262 (1995).

77. *See id.* at 270.

78. *See id.*

79. *See id.*

to their own computer hobbyists to solve sophisticated computer crime cases may find they have made a grave error in judgment. After all, who would expect their department's most avid reader of Agatha Christie to be their best homicide investigator?[80] Failure to recognize this critical difference is undoubtedly a pivotal factor in law enforcement's inattention to digital crime.

Any attempt to understand why police are behind in the fight against computer crime must consider the larger historical context of law enforcement's relationship with technology. The police have always been slow to adopt technology; the same cannot be said for criminals.[81] Indeed, criminal organizations have been quick to draw on new technologies which might aid in furthering their illegal enterprises. For example, in the 1930s, members of Chicago's brutal organized crime syndicates had more sophisticated weapons technology than most police officers. Similarly, in the 1980s, well before pagers were common in society, drug dealers availed themselves of these digital communications tools in an effort to avoid detection and wire-tapping by law enforcement.[82] As soon as the technology advanced, organized criminals turned to fax machines and cellular phones to conduct their criminal enterprises.[83]

What makes law enforcement's slow technological progress with regard to computer crime particularly troublesome is the fact that modern stand-alone and networked computer systems are vastly more complicated than machine guns, pagers, or cellular phones, and they are becoming more so all the time. Therefore, the longer police agencies wait to begin their study of computers and computer-related crime, the more difficult the process will be.

Learning about the issues involved in policing computer crime is as difficult as learning about the technology itself. Commonly-held ideas of crime and criminality must be substantially updated as digital technology continues to reshape the world in which we live. Basic crimes like theft have always meant that one person took something belonging to another without permission; the result was that the first party no longer had possession of the property which was taken. Economic value has always been placed on tangible, visible, and atom-based assets. Yet in an electron-based universe, it is quite possible for

---

80. *See* Coutorie, *supra* note 26, at 27.

81. *See* Michael R. Zimmerman, *Drug Dealers Find Haven in Online Services*, PC WK, Mar. 4, 1991, at 43.

82. *See* Jonathan M. Moses, *Message Is Out on Beepers: Police, Industry Fight Use by Drug Dealers*, WASH. POST, July 11, 1988, at A1.

83. *See* Terry E. Johnson, *Crime: Dialing For Dollars*, NEWSWK., Sept. 14, 1987, at 42.

one person to have taken something that belongs to another without permission and make a perfect copy of the item.[84] The result is that the original owner still has the property even though the thief has taken a version as well. Can a theft truly occur when the victim of the crime has not been deprived of the original copy of the property? The answer is generally yes. Changes like this are difficult for traditionalists in the criminal justice system to comprehend because they represent a fundamental shift in the way law is constructed and enforced.

Not only are criminal laws being reconstructed, but so are traditional concepts of evidence and forensics.[85] As Dan Duncan, senior instructor at the Federal Law Enforcement Training Center, recently stated, "This is a new world for law enforcement [because] cops have always followed a paper trail, and now there may not be one."[86] A shift from an environment where items are stored in tangible forms to an electronic environment means that computer crimes and the methods used to investigate them are no longer restricted by many traditional rules and constraints.[87] Generations of police officers accustomed to following evidentiary "paper trails" may find chasing electronic "data trails" very difficult. Electronic crime investigations require special expertise and training. Since most officers lack this training, they are reluctant or unable to pursue computer criminals. A future that lacks printed or atom-based evidence will continue to thwart most police agencies for some time to come, thereby increasing their reluctance and inability to investigate these crimes.

### *B. It is Difficult to Police the Internet*

Because of the distributed essence of the Internet, many legal difficulties confront law enforcement professionals who attempt to police cyberspace. The Internet was originally created as a project of the DoD's Advanced Research Project Agency ("ARPA")[88] in 1968.[89] The Defense Department's goal was to establish an open and accommodating

---

84. *See* Todd H. Flaming, *The National Stolen Property Act and Computer Files: A New Form of Property, A New Form of Theft*, 1993 U. CHI. L. SCH. ROUNDTABLE 255, 255 (1993).

85. *See* Sussman, *supra* note 48.

86. *Id.* at 59.

87. *See* Charney, *supra* note 17, at 940.

88. ARPA was the original name for the agency currently known as DARPA. The name was changed in 1972. *See* Scott Ruthfield, *The Internet's History and Development: From Wartime Tool to the Fish-Cam*, CROSSROADS, Sept. 1995, at ¶ 4 <http://info.acm.org/crossroads/xrds2-1/inet-history.html>.

89. *See generally Public Broadcasting Service, Life on the Internet: Net History* (visited Apr. 3, 1997) <http://www.pbs.org/Internet/history>.

global communications network of trusted hosts, including military installations, university researchers, and defense contractors.[90] The Internet was designed to survive a nuclear war and provided innumerable pathways for messages to be sent; if one route had been destroyed, the message had to be able to "react" and find a new path to its intended destination.[91] Although this network architecture is well-suited for military command and control operations, it presents a major headache for those who would attempt to limit the access and activities of computer criminals.

Hackers on the Internet often cover their tracks by "looping and weaving" in and out of dozens of computer systems around the world, masquerading as legitimate users on the co-opted system.[92] This can raise serious law enforcement jurisdictional issues for police personnel who attempt to follow the digital evidence trail to the true location of the computer criminal. Under current law, the only way to trace the individual may be with a court-ordered wiretap for each system on which the criminal has traveled.[93] Since hackers often take a different path each time, obtaining the wiretap order in advance poses unique challenges to police.[94] These challenges are further complicated by the fact that wiretap orders may be necessary for different cities, states, and nations — each with its own concept of computer crime.

Complicating any effort to police computer crime is the difficulty in obtaining digital evidence. Not only can incriminating clues be hidden, encrypted, and virus-laden, but they can be strewn anywhere around the world. The current laws regarding the search and seizure of digital evidence are ambiguous at best, and most of these laws remain to be tested. Furthermore, privacy rights asserted by various parties make the search and seizure of computer evidence very difficult.[95] The level of privacy and other rights accorded to an item or place to be searched depends on its actual and intended use. For example, is the computer to be seized acting as a simple storage and communications device or is it also fulfilling some type of publishing function? Legally, a personal computer used by a single individual is easier to search than a thousand-user bulletin board system ("BBS").[96] By seizing the BBS, the police may stop the illegal distribution of contraband, but they may also interfere with the publication of the BBS's newsletter and distribution of

---

90. *See id.*
91. *See id.*
92. *See* SECURITY IN CYBERSPACE, *supra* note 27, at 13.
93. *See id.* at 167.
94. *See id.* at 13.
95. *See* Raphael Winick, *Searches and Seizures of Computers and Computer Data*, 8 HARV. J.L. & TECH. 75, 81-89.
96. *See* SECURITY IN CYBERSPACE, *supra* note 27, at 102-09, 114-25.

e-mail to persons who have no connection to the illegal activity.[97] Because computer crime presents so many unique obstacles to investigation and prosecution, most police agencies would rather avoid the matter altogether. Thus, officers pursue the "low-hanging fruit" — those criminals such as street corner prostitutes and drug dealers — who require fewer resources and less complicated investigations in order to sustain an arrest and conviction.

### *C. The Lack of Resources*

Compared to violent street crime, white collar crime in general, and computer crime in particular, is vastly underreported.[98] Underreporting is significant because law enforcement resources are allocated based upon the number of *reported* crimes.[99] If a particular precinct has a 50% increase in the number of 911 emergency calls for service in a six-month period, it is likely to see additional patrol officers allocated to deal with that problem. Similarly, if a precinct commander notices a 75% increase in commercial burglaries, he or she is likely to ask for more burglary detectives to help abate the problem. Since police agencies receive few complaints about computer crime, there appears to be no problem. In fact, many senior law enforcement administrators state that computer crime simply has not become a problem in their particular jurisdiction.[100] As a result, police chiefs allocate few resources to the problem.[101] A wiser police manager, however, would not confuse invisibility with nonexistence.

Law enforcement executives attuned to the issue of computer crime still face financial challenges. Training police officers to investigate digital crime is an expensive proposition. In these times of public fiscal constraint, police chiefs are loath to spend their limited resources on anything that will not provide a sure and noticeable return. A properly trained computer crime investigator may require extensive ongoing professional education to maintain up-to-date skills.[102] Because computer companies introduce many new hardware and software products each year, staying ahead of the educational curve can be a monumental task. Furthermore, no single investigator can know how to

---

97. *See* Charney, *supra* note 17, at 941-42.

98. *See* SECURITY IN CYBERSPACE, *supra* note 27, at 243-45; Michael G. Noblett, *The Computer: High-Tech Instrument of Crime*, FBI L.ENFORCEMENT BULL., June 1993, at 7, 7-9.

99. *See* Collier & Spaul, *supra* note 15, at 308.

100. *See id.* at 307.

101. *See id.*

102. *See* Groover, *supra* note 28.

operate every system.[103] A number of officers must be trained to specialize in a variety of platforms.

As if training costs were not enough to discourage the average police chief from investigating digital crime, there is always the cost of equipment to be considered as well.[104] The specialized hardware and software required for the forensic examination of computers can easily run to tens of thousands of dollars.[105] Digital evidence storage rooms, spaces without magnetic interference, must be established to prevent the break down and destruction of digital evidence.[106] A police department serious about the investigation of high-tech crime must prepare for any eventuality: thousands of dollars could be spent on forensic IBM PC software only to discover the system that must be examined is an Apple Macintosh. In such a case, none of the PC cables or disks would work with the Macintosh, requiring additional funding in order to adequately equip digital crime investigators with the tools they need.

Training and equipment are not the only financial impediments to conducting high-technology crime investigations: the physical distance between perpetrator and victim also poses special problems for those investigating computer crimes. A New York City police detective working on a traditional burglary in lower Manhattan might have to drive to Brooklyn to interview suspects, execute a search warrant, and seize physical evidence, but rarely will her cases take her very far. In the world of digital crime, however, the Manhattan detective is much more likely to be confronted with a suspect who lives outside of the New York City area, in Los Angeles for example. Not only might this necessitate a trip to California, but it would also require significant coordination between the New York City Police Department and the Los Angeles Police Department. This coordination takes not just precious time, but also lots of money. Needless to say, this scenario is more complicated when the suspect and evidence are located outside of the United States.

A suspect who dials into the Oxford University computer system in England and illegally uses that system to break into the University of San Marcos in Peru for the purpose of illegally accessing a NASA computer at Cape Canaveral may commit a crime in three countries. At the very least, the evidence will have traveled, and therefore will need to be traced, through all three countries. Since computer hackers often erase any digital evidence of their illegal presence, monitoring access must be done in real-time at multiple sites in different countries, involving

---

103. *See id.*

104. *See id.*

105. *See generally* Michael Noblett, *Computer Analysis and Response Team (CART): The Microcomputer as Evidence*, 19 CRIME LABORATORY DIG. 11 (1992).

106. *See generally* CLARK & DILBERTO, INVESTIGATING COMPUTER CRIME (1996).

federal, state, and local governments, twenty-four hours a day. Not only does coordination in the above scenario prove to be a nightmare, but the costs involved in such work are often prohibitive. When international cases are pursued, the mechanics of cooperation, such as the execution of mutual legal assistance treaties or the involvement of the State Department, can add substantial delays and expense to an already burdensome and difficult operation. Because computer crime is underreported and relatively expensive to prepare for, many police agencies prefer to ignore the situation and spend their limited resources in other areas, such as purchasing newer police cars, police officer overtime pay, and community policing programs.

The lack of tangible, conspicuous evidence is another factor in the underreporting of computer crime. When a homicide occurs, a body almost always appears and is reported to the authorities. Crimes like homicide are easily defined and quantified and, by law, must be reported to the Federal Bureau of Investigation ("FBI") and the Federal Bureau of Justice Statistics.[107] As mentioned earlier, the definition of a computer crime remains ambiguous.[108] The lack of a standard definition makes it harder for the police to understand and track such crimes. The overwhelming majority of law enforcement organizations do not keep statistics on computer crime.[109]

Each year when the FBI's *Uniform Crime Reports* comes out, the public pays considerable attention to a given community's homicide and auto theft rates. Nowhere in the *Uniform Crime Reports*, however, is there any mention of computer crime statistics.[110] Because the Department of Justice does not mandate their collection, police agencies do not feel compelled to count the number of these crimes.[111] Since computer crime statistics remain invisible to the police department, the police feel no particular compunction to dedicate limited resources to high-tech crimes that nobody bothers to count.

Complicating the invisibility problem, most victims of computer crime and intrusions fail to report their victimization.[112] Individuals often do not know that the violation committed against them actually constitutes a criminal offense. Businesses have different reasons not to report computer crime incidents: mistrust of the police, the fear of

---

107. *See generally* FEDERAL BUREAU OF INVESTIGATION, UNIFORM CRIME REPORTS FOR THE UNITED STATES 1995 (1996) [hereinafter UNIFORM CRIME REPORTS]; U.S. DEPARTMENT OF JUSTICE, SOURCEBOOK OF CRIMINAL JUSTICE STATISTICS — 1995 (Kathleen Maguire & Ann L. Pastore eds., 1996).

108. *See supra* text accompanying notes 15-17.

109. *See* Collier & Spaul, *supra* note 15, at 308.

110. *See generally* UNIFORM CRIME REPORTS, *supra* note 107.

111. *Cf.* SECURITY IN CYBERSPACE, *supra* note 27, at 242-43.

112. *See id.* at 242-45.

negative publicity, and potential loss of future revenues. It is for these reasons that the private security industry attracts billions of dollars each year.[113] Last year alone, corporate America alone spent $6 billion for private computer security services.[114]

The business community clearly believes that police officers cannot handle computer-related crimes and security problems because they think cops will not understand the issues.[115] Corporate managers "believe that police agencies are at best ineffective, and at worst, that their use is counter-productive in prosecuting or restricting computer crime."[116] Perhaps the greatest obstacle to businesses reporting computer crime is the deeply-held fear of losing customer and shareholder confidence.[117] 65% of those who participated in a survey by the San Francisco-based Computer Security Institute ("CSI") cited a fear of negative publicity resulting from disclosure of a break-in.[118] In CSI's survey, 83% of the respondents stated they did not advise the police when they had been victimized by computer crime.[119]

Even the smallest business owner knows that customer confidence is an essential element for financial viability; corporations who lose the confidence of the public can face bankruptcy. For example, a hospital whose patient records system was hacked by computer intruders, as in the nightmare scenario with which I began this Article, would surely lose customers. A major airline that had its flight maintenance database destroyed would rightly be concerned about passengers choosing another carrier. Perhaps no organizations are as susceptible to public perceptions of safety as financial institutions. In 1995, when Citibank lost $10 million to a group of hackers operating out of St. Petersburg, Russia, its top twenty customers were immediately targeted by six of Citibank's competitors who argued that their banks were more secure.[120]

Another problem that contributes to underreporting is that law enforcement agencies and corporations have different goals in mind vis-à-vis computer crime: the police want to prove a crime has occurred and bring the culprits to justice;[121] a corporation is more interested in stopping the intrusion, minimizing losses, and avoiding publicity at all

---

113. *See* Andrew Leckey, *Investing for the 21st Century*, THE FUTURIST, July-Aug. 1995, at 31, 34 (estimating the figure at $65 billion per year).

114. *See* Richard Behar, *Who's Reading Your E-Mail*, FORTUNE, Feb. 3, 1997, at 57, 58.

115. *See* Collier & Spaul, *supra* note 15, at 310.

116. *Id.*

117. *See* SECURITY IN CYBERSPACE, *supra* note 27, at 27.

118. *See id.*

119. *See id.*

120. *See id.* at 51.

121. *See id.*

costs.[122] To this end, many computer crime investigations are conducted through the corporation's general counsel's office so as to provide a veil of secrecy that flows from the attorney-client privilege.[123] According to the FBI, as little as 11% of computer crime is actually reported to law enforcement officials.[124] A few security firm executives recently admitted that their goal is to catch and notify the hacker to stop his attack against the security company's client.[125] Once that particular assault has stopped, businesses do not mind throwing the hacker back into the marketplace, hopefully to attack their competition down the street.[126] Since the goal of the average company is to stop its own financial losses due to computer malfeasance, there is little consideration of the greater public good of getting the computer criminal behind bars.

As long as private computer security firms continue to handle most high-tech crime investigations, businesses will continue to believe that the police are incapable of protecting their corporate and economic interests. This situation can rapidly become a vicious cycle, with businesses balking at future tax increases for police given the little value they derive from such public services. More importantly, however, businesses are integral parts of most communities. Police agencies that neglect their criminal enforcement and investigative obligations to members of the community fail in their publicly chartered mission.

### *D. The Police Cannot Do It Alone*

Even if police agencies properly understood the importance of digital crime, law enforcement does not operate in a vacuum. Mayors, district attorneys, city council members, and judges are among some of the most important participants in the battle against high-technology crime. These public officials must be convinced of the need to expand into the poorly understood arena of digital law enforcement, a difficult sell with many competing political interests at stake. In a time when most police departments are "getting back to the basics" of patrol and community-based policing, creating another specialized unit seems anathema to larger organizational goals.[127]

---

122. *See id.*

123. *See id.* at 52.

124. *See* Noblett, *supra* note 98.

125. *See* SECURITY IN CYBERSPACE, *supra* note 27, at 51.

126. *See id.*

127. *See generally* David Kocieniewske, *Safir Shifts 500 Detectives to Aid Precincts*, N.Y. TIMES, Feb. 2, 1997, at 34 (reporting the reassignment of police investigators from specialized central units to non-specialized precinct units); *The Police Reform That Must Not Die; Community Policing Push Affirms City Hall Commitment*, L.A. TIMES, Jan. 9, 1994, at M4.

Those police departments that choose to pursue computer criminals must therefore include prosecutors and elected officials as an integral part of their overall anti-crime strategy. What is the point of detecting and investigating computer crime if the district attorney's office lacks the expertise or refuses to prosecute these matters? In addition, penalties for conviction in digital crime cases vary enormously, often yielding no more than a mere "slap on the wrist" for the offender.[128] Why expend limited resources on cases that have questionable results? Despite the best efforts of the police department, political authorizers may still not see the value in policing high-technology crime, instead pushing officers to concentrate on crimes which people "care about."[129]

### *E. Lack of Public Outcry*

Most police chiefs have yet to hear any significant complaint about computer crime. Since neither the business community nor citizen groups seem to be upset about these crimes, law enforcement executives are free to put all their resources into something people *are* upset about, violent crime.[130] The public outcry against violence pushes municipal and law enforcement leaders to find a few extra dollars in the budget. There has not yet been such an outcry against cybercrime.

Complicating the lack of general public concern about computer crime is a strong reaction from some against law enforcement entering the world of "digital policing." Policing the Internet will unquestionably put pressures on American notions of privacy, property, and free speech.[131] A number of organizations have legitimate concerns regarding law enforcement's intrusion into cyberspace. Groups such as the American Civil Liberties Union,[132] the Electronic Frontier Foundation,[133] and the Electronic Privacy Information Center[134] are willing to wage

---

128. *See* Collier & Spaul, *supra* note 15.

129. *See supra* text accompanying notes 72-73.

130. *See id.*

131. *See* Sussman, *supra* note 48, at 55.

132. The American Civil Liberties Union ("ACLU") is a public interest organization created in 1920 to protect individual rights through litigation, legislation, and education. *See American Civil Liberties Union* (last updated Mar. 25, 1997) <http://www.aclu.org/>.

133. The Electronic Frontier Foundation ("EFF") is a non-profit, public interest, civil liberties organization working to protect privacy, free expression, and access to public resources and information online, as well as to promote responsibility in new media. *See Electronic Frontier Foundation* (visited Mar. 25, 1997) <http://www.eff.org/>.

134. The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. *See Electronic Privacy Information Center* (visited Mar. 25, 1997) <http://www.epic.org/>.

long, drawn-out battles in court when they perceive that police officers have overstepped their constitutional boundaries in enforcing cybercrime.

Thus, the sluggishness with which police agencies are pursuing digital criminals can be attributed to a lack of public outcry combined with significant political pressure warning politicians and police executives to proceed with great caution into this new arena of criminal law. Moreover, mayors have not yet found it necessary to push their police chiefs into doing anything about high-technology crime. In the ever-changing world of law enforcement, it is hard to plan for next week, let alone for ten years from now. Events like high-profile homicides, civil unrest, publicized incidents of police misconduct, and officers killed in the line of duty lead police chiefs to manage from one crisis to the next. Thus, at least for the present time, police departments are willing to turn a blind eye to those crimes taking place in cyberspace.

As we have seen, there are many reasons why police do not yet care about high-technology crime. These impediments include police culture, limited police resources, the invisibility of digital crime, and other high priority concerns like violent crime. Yet, like it or not, law enforcement agencies around the globe have to confront a rapidly changing world in which ever-evolving technologies will fundamentally change society as we know it. The digital revolution has begun. The longer police departments wait to patrol the information superhighway, the more daunting their task will eventually be.

## III. How Do We Get To Where We Need to Be?

While computer crime is on the rise, significant cultural, financial, and educational challenges may stymie police agencies who wish to combat high-tech offenses. Yet, something must be done by law enforcement officers to combat computer crime. The race is on and the bad guys have a significant head-start. To turn around police departments will require a paradigm shift in the way policing is done.

Although the information revolution is upon us and changing the way in which criminal activity is taking place, very little attention has been given to the information and computer literacy skills of police professionals. If police agencies are to be considered competent, there must be greater resources dedicated to training officers to understand and investigate computer crime. Many police departments might like to ignore problems of high-technology crime and leave the work to federal agencies. This tactic, however, would be ill-advised.

Police managers who assume they can just call in their federal law enforcement counterparts any time a local high-tech crime takes place are making a serious error. Although organizations like the FBI will

likely become involved in any case of computer crime that threatens national security, they do not have the resources to assist with the investigation of local gamblers, child pornographers, or even murderers who had inculpatory evidence stored on their hard drives. The resources simply do not exist for federal law enforcement agencies to handle the bulk of high-technology crimes at the local and municipal levels.

Local and state police agencies will thus have to build mechanisms to deal with these types of crimes. The approach must be two-pronged: both long- and short-term responses are needed. In the short run, most agencies will have to "play catch-up." That is, there will be a need for some rapid growth in the amount of equipment and personnel dedicated to the problem of computer crime. Some officers will have to be trained elsewhere, perhaps by organizations in the private sector that offer basic computer classes. Of course, a small percentage of officers will need advanced training, particularly in computer forensics. On the equipment front, it may make sense for police agencies with limited budgets, particularly those in suburban and rural areas, to form regional task forces to deal with the rising workload in computer crime. Several police agencies could pool their resources and each could purchase smaller amounts of equipment to share among the members of the group.

For the long-term, police executives have to think strategically about computer crime and must be prepared to allocate the appropriate resources for the recruitment, education, and training of personnel capable of investigating these crimes. Departments that have not yet computerized their operations should do so. Not only will this lead to increases in overall efficiency, it will begin to familiarize officers with computing. Employees should be encouraged to think about how technology might help them improve department operations. Furthermore, serious consideration should be given to encouraging young, college-educated computer science majors to join the police force.

Departments also need to find funding for these endeavors. Many agencies, especially smaller police departments, do not have the resources to train personnel for the effective investigation of computer crime. Although some of the necessary equipment can be acquired through donations, police departments should not be put in the position of holding bake sales to pay for necessary and justifiable training. Given the numerous interests competing for each tax dollar, most local and state law enforcement organizations will encounter resistance from their political authorizers as they attempt to expnad their use and understanding of computers. A major funding source for these endeavors must be identified.

In 1968, President Johnson signed the Omnibus Crime Control and Safe Streets Act.[135] Among the Act's provisions was the creation of the Law Enforcement Assistance Administration ("LEAA"),[136] to provide technical assistance to local government law enforcement agencies. Funding for LEAA was withdrawn in 1982, but in the fourteen years of its existence, LEAA provided local agencies with nearly $50 million in funds for police officer training and technology assistance to local criminal justice organizations.[137] It is time to bring back a version of LEAA to help police departments gear up to fight computer crime.

The police officers of today and tomorrow will require certain attitudes, training, and education to effectively control crime in a digital world. Current theories in criminal justice administration have been critical of law enforcement's traditionally reactive responses to crime. Community members and police executives have been calling for a more proactive approach to all facets of law enforcement. This clamor for proactive policing must extend into the world of digital crime.

### *A. Building a Computer-Competent Police Force*

For the bulk of the police force, the levels of computer literacy necessary to function are relatively low. It is certainly not necessary for every police officer to have a Ph.D. in computer science in order to be effective in the twenty-first century. However, a basic level of computer literacy must be mandated so that officers can ask the basic questions about the crimes they will be investigating.

Patrol officers must be trained to recognize a high-technology crime when it occurs. Furthermore, these "first responders" must understand the importance of calling in an expert to deal with such situations. A lack of attention or willingness to call in a computer crime specialist can have negative consequences for police departments attempting to preserve evidence, arrest a perpetrator, or successfully pursue a prosecution in court. If a computer examination is not conducted properly, valuable evidence may be lost, and the police department involved may be liable for any damage caused to the computer.

These days, criminals can install degaussing loops around the door jambs of their apartments. The magnetic field created will erase any magnetic media carried through the door. Specialists responding to handle the investigation would be attuned to the potential presence of such a device and could respond appropriately. An inexperienced

---

135. Pub. L. No. 90-351, 82 Stat. 197 (1968).

136. *See* SUE T. REID, CRIMINAL JUSTICE PROCEDURES AND ISSUES 130 (1987); *see generally* ENCYCLOPEDIA OF POLICE SCIENCE 409 (William G. Bailey ed., 2d ed. 1995)

137. *See* REID, *supra* note 136.

officer, however, might carry the computer out of the house unaware that the magnetic field was destroying all the recordings on the disk. A computer criminal could also alter his computer so that any police officer who turned on the machine without using the appropriate bypass switch would unknowingly cause the hard drive to format itself, thereby destroying any possible evidence contained in the machine. To avoid such catastrophes, the basic rule of thumb for patrol officers and detectives when a computer is found at a crime scene should be: "Don't touch it!"

Although not all police officers need to become computer specialists, all first responders do need basic training to handle crimes and crime scenes involving computers. Even common police calls can take on different dimensions in the world of high-technology. For example, police officers already have an understanding of what it means to stalk somebody, but, the idea of stalking by computer may be a new concept for most officers. Nevertheless, it does not take a specialist to ask a victim to print out copies of the harassing e-mail so they can be attached to a police report and forwarded to the district attorney for prosecution. If an officer has no idea what e-mail is, or even that electronic records of e-mail are kept and can be found, then the chances for a successful prosecution will be severely limited. In this scenario, an officer only needs a minimal amount of computer savvy. Basic guidelines and procedures for handling the preliminary investigation of computer crime should be established. These procedures should include a method for determining when a computer crime expert should be summoned.

Thus, although all officers will require basic literacy in information technology, some police personnel will require in-depth training in order to effectively police the digital world. Seizing electronic material is highly specialized work. Just as every police department in the country has a bomb squad or a SWAT unit, or contracts for such services, they must do the same for computer crime. Delicate protocols have to be followed in order to preserve critical and perishable evidence. Having this work done by those who lack expertise could hurt the agency's reputation, be harmful to the victim, embolden criminals for future acts, and jeopardize prosecutions. If there is any doubt about the competency of an agency to handle more a particular crime, the case should be referred to an expert.

### *B. Training Officers for Computer Literacy*

One of the roles of the specialist division should be to provide training to other members of the police department. Patrol officers need to know how to handle computers found during investigations. Detectives need to include electronic media in the standard repertoire of

items included in their search warrants. All officers need to receive more training and more exposure to computers. Such a focus on training could begin by requiring basic computing skills of all academy recruits. Students in the academy need to be trained in the advantages to law enforcement of using information technology as well as the threats posed by computer crime.

Officers who are already on the force need to be encouraged to learn about computers. Departments should offer general computer training to familiarize officers with how word processing, spreadsheets for crime statistics, and databases can be useful in their daily work. They should also be introduced to the Internet. Many departments may not have the resources for in-house training, but they can hire outside consultants to do such training. More advanced training should be provided when possible. This could include comprehensive reimbursement programs for officers who wish to take computer classes at local schools and universities.

## IV. CONCLUSION

Society has placed the burden of investigating computer crimes on police departments. Unfortunately, many institutional factors have led police departments to shy away from pursuing these crimes. Programs to address the problem of computer crime need to address the social, cultural, and political factors that are currently stopping police departments from developing teams to combat these crimes. Unless police departments start planning and training now, it may be impossible to keep up with the criminal elements of society as they plan their future misdeeds. In order to protect society from these new cybercrimes, it is necessary for law enforcement agencies not merely to meet the expertise of their criminal counterparts, but rather to exceed their knowledge and skills. Training and equipment must be acquired soon. If not, the U.S. criminal justice system will fall perpetually behind in its efforts to enforce and prosecute a whole new class of criminal activities.