
Defending Against Cybercrime and Terrorism

A New Role for Universities

By TONY AEILTS



With the growth of technological access, systems, and resources, cyber-related crimes are on the rise in many communities. How will local law enforcement agencies address the growth of high-tech crime in the future? What impact will terrorism have on the nation's

technological infrastructure, and how do we protect against it?

The high-tech industry is vital to the nation's economy and its future. Industries, businesses, government agencies, and private households all benefit from a healthy and well-protected technological environment. And, everyone

wants reassurance that communications, financial operations, and technological infrastructure are closely guarded. The rising fear of cyber-related crime not only inhibits the use of developing technology but adversely affects national economic conditions. The FBI estimates that the average loss for a

technology-oriented crime is nearly \$500,000, and, further, the added cost to the consumer is \$100 to \$150 per computer sale.¹ Other estimates indicate that losses related to high-tech crimes in the United States are \$10 billion to \$15 billion per year.² Further, 10 million Americans were victimized by identity theft in one year, with estimated losses exceeding \$50 billion,³ and the Federal Trade Commission reported that of the 516,740 complaints received in 2003, over 41 percent regarded identity theft.⁴

Beyond the implications of cybercriminal activity, a new technological threat exists pertaining to terrorism. Since September 11, 2001, the nation has focused more on the issue of cyberterrorism because although terrorists typically have used traditional methods of physical attack (explosives, kidnappings, and hijackings), their attention may move, with increasing frequency, toward cyberterrorism. Various forms of technological infrastructure may be vulnerable to such attack; pipelines, power plants, transportation, and other hard assets rely on cybertechnology. Further, communication systems used for financial, military, police, and corporate purposes suffer from the same vulnerability. This not only includes threats against physical

facilities and tangible equipment but remote cyberattacks that could disable national infrastructure as well.

DEFINING THE SCOPE OF THE PROBLEM

Headlines regarding the threat of high-tech crime have become commonplace. Cyberstalking of children, child pornography, identity theft, financial fraud, computer hacking, computer viruses, and theft of proprietary business information and intellectual property have become the prominent crime for those with even modest amounts of technological sophistication.⁵ Statistics related to the prevalence of high-tech crime remain unclear. Many law enforcement agencies do not clearly identify occurrences of high-tech crime.

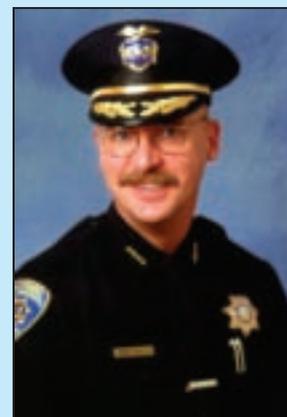
For example, a high-tech related theft of money or resources statistically is identified as a theft based upon historical definitions; the high-tech component of the crime may not be identified at all. To address this issue, the FBI and the National White Collar Crime Center implemented the Internet Fraud Complaint Center (IFCC) in 2000.⁶ The IFCC tracks complaints it receives and coordinates with local law enforcement agencies regarding appropriate investigative jurisdiction; however, this process still does not provide consistent measurements of cybercrime.

From January 1, 2002, to December 31, 2002, the IFCC Web site received 75,063 complaints.⁷ Additionally, the IFCC points out “that Internet usage passed the 200 million

“

This virtual crime world demands cooperation and sharing of resources among agencies....

”



Chief Aeilts heads the California State University Police Department in San Luis Obispo.

mark...from just 65 million in 1998.”⁸ This dramatic threefold increase in Internet usage in just a few years could indicate the possibility of a corresponding increase in cybercrime. Some experts argue that many “...victims may have serious doubts about the capacity of the police to handle computer crime incidents in an efficient, timely, and confidential manner.”⁹ Businesses or other institutions may not report such crimes due to concerns of loss of prestige, customers, and financial status. Consequently, agencies may not adequately capture cyber-related crime statistics, and the gross impact of this type of crime, generally, may appear understated.

COORDINATING JURISDICTIONS AND SHARING RESOURCES

The difficulty of identifying the impact of cybercrime is not the only significant concern—jurisdictional issues also are problematic. When a high-tech crime occurs, it is not always clear which law enforcement jurisdiction is responsible for its investigation and prosecution. Cyberincidents can cross regional, state, and even international jurisdictional boundaries. Crime has expanded into a virtual geographic world and traditional jurisdictions and boundaries do not apply. This virtual crime world demands

cooperation and sharing of resources among agencies: “...although sharing information among the courts, the police, and other justice agencies at every level of government has been a goal of dedicated individuals and organizations for the past several years, the September 11 terrorist attacks have given the issue a renewed national scope.... The attacks, they say, highlighted the lack of information exchange and underscored the importance of improved coordination among agencies....”¹⁰

“

Together, all stakeholders should explore the various dynamics of the high-tech crime problem.

”

Most law enforcement agencies simply do not have the resources to adequately deal with the myriad of potential cybercrimes.¹¹ The ability to track criminals in multiple jurisdictions, as well as specialized knowledge of vast varieties of hardware, software, applications, foreign languages, and other related issues, requires regional, state, and national

multiagency cooperation. “The most promising approach so far is a task force in which high-tech specialists from city, county, state, and federal law enforcement agencies work together and accept assistance from industry.”¹² However, one critical component is missing from that formula—the effort can and should bring high-tech resources from higher-education institutions to the forefront to assist law enforcement and national defense. “The White House’s top computer security official...called on colleges and universities to help develop a national strategy for securing computer networks. ‘I think this effort—this framework—is extremely important because it demonstrates that the issue of network security is a major concern of colleges and universities around the country,’ said...[the] president of the American Council on Education in a statement. ‘Policy makers and corporate leaders should know that the higher-education community is working together constructively to address this challenge.’”¹³

LINKING WITH HIGHER-EDUCATION INSTITUTIONS

Higher-education resources are abundant within the realm of technology, but law enforcement agencies fundamentally underuse them. Frequently,

these resources are in close proximity to many agencies but simply remain overlooked.

Specific Strategies

University High-Tech Faculty and Staff

Law enforcement administrators should identify university faculty and staff as a significant training resource, as well as one in support of high-tech criminal investigations. Faculty members routinely conduct high-tech research, including the development and implementation of cutting-edge innovations. Their positions enable them to recognize the implications of emerging technology issues and understand potential social impacts. Their research and development often address how individuals can abuse and compromise technology, as well as find ways to protect it. "University research is crucial to developing ways to protect computer networks, in part, because businesses can't afford to spend money on long-term, high-risk research."¹⁴ Further, universities typically have well-developed information technology support services with cadres of highly trained staff who routinely install, repair, modify, and protect information systems. Part of their expertise comes from daily exposure to these systems on a functional level.

Few local law enforcement agencies have this well-developed resource.

Additionally, institutions of higher education have high-tech classroom facilities with numerous monitors, computers, interfaces, remote projection, automated lectures, and other related capabilities, providing substantial opportunity to train multiple students, provide quality high-tech instruction, and enhance student interaction. These training resources commonly are available during academic breaks throughout the year.



An Investigative and Multiagency Protocol

Many colleges and universities employ state-certified law enforcement agencies to protect assets of the institution. These educationally based departments can provide a critical conduit for allied law enforcement agencies and their access

to university high-tech resources and personnel and serve as a mechanism to ensure investigative integrity. University police departments can monitor such issues as search and seizures, due process, and investigative protocol and provide liaison with member agencies and the district attorney. This expertise proves helpful when identifying and using nonsworn university resources in support of cybercrime investigations, and it can smooth the way toward a successful investigation.

Using a multiagency, high-tech investigation protocol can reduce potential misunderstandings about resources (departments should use personnel and other resources based upon prior agreement), protect the integrity of the investigations, and provide a system of easy reference that allows member agencies to follow a consistent and predictable process. Agencies should consider a number of factors in their protocol, including the personnel-sharing process, technological equipment and programs purchases, and grant-funding distribution.

Financial Opportunities

Many high-tech task forces compete for a variety of state and federal grants. However, most grants require an accomplishment record indicating the importance of financial support

to continue efforts to address the problem. Because many high-tech businesses have a strong interest in guarding against high-tech crime, collaborating with these organizations may produce additional financial resources. Many companies offer a variety of funding opportunities via foundations—corporate efforts to support their community. Agencies should pursue corporate high-tech support, as well as government grants.

A high-tech crime investigation partnership, in and of itself, provides a generally self-supporting mechanism. Equipment and people cost money, but the sum contribution of partnered agencies constitutes the initial formula that best would support the beginning steps of this effort. In fact, if each agency provides some limited support, such as personnel, resources, training expertise, and computer equipment, the high-tech group likely can be self-supporting. Additional funding based upon grants, foundations, and allied organizations then becomes a resource to enhance an already existing and functional program.

Stakeholders

Together, all stakeholders should explore the various dynamics of the high-tech crime problem. Each will have

a perspective unique to their needs, concerns, resources, and customers. Until such collaborative meetings occur, stakeholders will lack full awareness of their own resources and expertise. Most important, participants must gain their organization's support. Long-term approval for partnerships, protocols, and financial and personnel support is critical to the development of a realistic and substantial program. Stakeholders may vary from one region to another, but the local

“

Law enforcement administrators should identify university faculty and staff as a significant training resource....

”

district attorney, college or university, area law enforcement agencies, and the FBI provide a basic formula. Businesses, which can provide information technology specialists and financial support, also should be considered an integral part of the plan.

Line-Level Personnel

Once stakeholder organizational leaders agree to support a move toward the development

of a high-tech, multiagency crime investigation group, they should identify line-level personnel who can accommodate the program's efforts. For colleges and universities, this includes their police investigators, as well as high-tech faculty and staff members. Each organizational leader should charge these individuals with the responsibilities of communicating with line-level members in partner agencies. Fundamentally, the grassroots members will form many of the long-term and functional relationships.

While it may be helpful for line-level law enforcement personnel to have extensive high-tech investigative expertise, it is *not* necessary. The preliminary development of a high-tech partnership should include those agencies with little or no high-tech expertise; an important element of this process is the development of expertise and resources over time.

A Model for the Future

The University Police Department (UPD) at California Polytechnic State University in San Luis Obispo reviewed its cybercrime issue and implemented several approaches to address the problem. First, several UPD officers received extensive training from the university's wealth of staff members and faculty with broad expertise in technology,

emerging high-tech trends, and education/training abilities. The training centered on the application of computer forensics and investigative protocol as they related to high-tech crime. Next, UPD invited representatives of local law enforcement agencies to discuss the formation of a high-tech task force. The response was outstanding; representatives from departments in a four-county area attended the meeting, along with university faculty and staff.

UPD then developed an e-group site¹⁵ using university faculty. A list of 30 investigators from 14 agencies in 3 counties signed on to use this site as a mechanism to exchange high-tech investigation information and as a forum to solicit help with their investigations. Other meetings occurred and, subsequently, interest in a high-tech resource group grew to 46 investigators representing 5 counties in the region. Faculty members provided training and discussion ensued about joining the High-Tech Crime Investigators Association International. At that point, participation included local city police and county sheriffs' departments, state agencies, the district attorney's office, and the FBI. Additionally, the group sought participation from corporations, recognizing that they also are victims of



high-tech crime and could provide high-tech expertise and resources.

Currently, this group includes about 100 members, representing dozens of agencies. Members continue to meet, communicate via the e-group site, provide high-tech training, and share investigative expertise with each other on a variety of high-tech crime investigations. This effort specifically has resulted in the successful outcome of numerous regional, multiagency, high-tech investigations with direct involvement from the forensic expertise of UPD officers and the support of high-tech faculty and staff. UPD, as an educationally oriented police agency, influenced a region and helped coordinate the high-tech resources of university police, faculty and staff, and corporations. It also provided an organized venue to

coordinate the high-tech resources of regional allied agencies.

CONCLUSION

The United States is not yet adequately prepared to deal with cybercrime and terrorism. The significant cost of cybercrime, coupled with the difficulty of identifying it, is of national concern, and the law enforcement profession should align agencies and resources to address these issues. The inclusion of college and university resources in the fight against cybercrime and the threat of terrorism may be a pivotal step. High-tech faculty, staff, and facilities, as well as university police departments, are a powerful combination of resources—one which exists in thousands of communities. In-depth technological expertise, high-tech classrooms,

information systems support, and a built-in policing conduit all can be used to mitigate the potential impacts of high-tech crime and terrorism. ♦

Endnotes

¹ California High-Tech Task Force Committee, *Combating High-Tech Crime in California: The Task Force Approach*, (June 1997), 3.

² Blumberg, "ID Anti-Theft Efforts Stir Capitol Debate," *The Daily Recorder*, August 7, 1998, 7.

³ Testimony of FBI Deputy Assistant Director Steven M. Martinez before the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, September 2004.

⁴ U.S. Federal Trade Commission, "FTC Releases Top 10 Consumer Complaint Categories in 2003," retrieved on November 8, 2004, from <http://www.ftc.gov/opa/2004/01/top10.htm>.

⁵ For additional information, see Robert D'Ovidio and James Doyle, "A Study on Cyberstalking: Understanding Investigative Hurdles," *FBI Law Enforcement Bulletin*, March 2003, 10-17; John Pollock and James May, "Authentication Technology: Identity Theft and Account Takeover," *FBI Law Enforcement Bulletin*, June 2002, 1-4; Thomas R. Stutler, "Stealing Secrets Solved: Examining the Economic Espionage Act of 1996," *FBI Law Enforcement Bulletin*, November 2000, 11-16; and Matthew L. Lease and Tod W. Burke, "Identity Theft: A Fast-Growing Crime," *FBI Law Enforcement Bulletin*, August 2000, 8-12.

⁶ Jerry Seper, "Justice Sets Up Web Site to Combat Internet Crimes," *The Washington Times*, May 9, 2000, sec. A., p. 6.

⁷ *IFCC 2002 Internet Fraud Report*, retrieved on June 9, 2004, from http://www.ifccfbi.gov/strategy/2002_IFCCReport.pdf.

⁸ *Ibid.*

⁹ Marc Goodman, "Making Computer Crime Count," *FBI Law Enforcement Bulletin*, August 2001, 13.

¹⁰ Dibya Sarkar, "Homeland Security Focuses Coordination," retrieved on April 2, 2004, from <http://www.fcw.com/fcw/articles/2002/0401/news-home-04-01-02.asp>.

¹¹ The FBI's Cyber Task Force Unit (CTFU) assists in the creation, maintenance, and operation of cyber task forces throughout the United States. The unit ensures that these task forces are capable of responding to significant criminal and national security threats involving the use of computers, the Internet, and high technology. The unit ensures that 1) task forces have state-of-the-art equipment and sufficient technical talent so that the United States is prepared to respond to cyber-related threats; 2) an effective infrastructure enables law enforcement to have a coordinated approach to the investigation of cybercrime; and 3) the relationship between the FBI's cyber task forces and those associated with other agencies are complementary.

¹² *Supra* note 1, 17.

¹³ Dan Carnevale, "White House Official Asks Colleges to Help Create National Computer-Security Strategy," *The Chronicle of Higher Education*, April 19, 2002, 12; retrieved on April 5, 2004, from <http://chronicle.com/free/2002/04/2002041901t.htm>.

¹⁴ Richard A. Clarke, special advisor to the President for cyberspace security, in Dan Carnevale, "White House Official Asks Colleges to Help Create National Computer-Security Strategy," *The Chronicle of Higher Education*, April 19, 2002, 12; retrieved on April 5, 2004, from <http://chronicle.com/free/2002/04/2002041901t.htm>.

¹⁵ An e-group site hosts special interest groups on the Internet. These sites often offer free, usually advertising-supported, service for anyone who wants to create an electronic forum in which individual and group discussions can take place about a particular area of interest. The site may be restricted by password protection.

Wanted: Photographs



The *Bulletin* staff is always on the lookout for dynamic, law enforcement-related photos for possible publication in the magazine. We are interested in photos that visually depict the many aspects of the law enforcement profession and illustrate the various tasks law enforcement personnel perform.

We can use either black-and-white glossy or color prints or slides, although we prefer prints (5x7 or 8x10). We will give appropriate credit to photographers when their work appears in the magazine. Contributors should send duplicate, not original, prints as we do not accept responsibility for damaged or lost prints. Send photographs to:

Art Director
FBI Law Enforcement Bulletin, FBI Academy,
Madison Building,
Room 201, Quantico,
VA 22135.