NATIONAL LAW ENFORCEMENT AND CORRECTIONS TECHNOLOGY CENTER
A program of the National Institute of Justice

From Summer 2000 *TechBeat*

TECH b•e•a•t

Dedicated to Reporting Developments in Technology for Law Enforcement, Corrections, and Forensic Sciences

Catching the Cyber Crook

It's a "win-win." And the only losers . . . those intent on committing electronic crimes.

That win-win is the New York Electronic Crimes Task Force (NYECTF), a partnership between the U.S. Secret Service and a host of other public safety agencies and private corporations engaged in a fight against electronic crime.

NYECTF was formed in January 1995, according to Robert Weaver, assistant to the special agent in charge of the task force. Prior to 1995, it was a small squad of Secret Service agents primarily involved with telecommunications fraud. "But criminal abuse of technology followed the evolution of technology," Weaver says. "As technology improved and became more sophisticated, so did the criminal enterprises that were abusing it. We followed that trend."

Weaver says it had become obvious that the already successful 10-agent squad was going to require support and input from outside agencies if it was going to branch out and stay on top of technology developments. Turning the squad into a task force, he says, allowed its members to form partnerships with outside entities. Today, that membership represents 25 law enforcement/criminal justice agencies, 45 private companies, and 3 universities.

Cases typically are generated by the proactive investigation by Secret Service agents, member agencies, or nonmember departments or companies that simply need help, Weaver says. The task force has an open-door assistance policy and will help any agency that requests assistance "with no strings attached."

Each case is headed by a group supervisor or group leader. "But, we don't assign the best cases to our [Secret Service] agents," Weaver says. "Whoever brings in the case keeps the case, and we wrap the task force around them. Not all of the NYECTF's group leaders are Secret Service agents. They come from a number of outside agencies."

These "outstanding investigators," as Weaver calls them, can make command decisions and are responsible for putting a case together and for the safety of its operation. Jurisdictional problems are solved by coordinating

A History of Success

The initial U.S. Secret Service electronic crime squad and subsequent New York Electronic Crimes Task Force have had significant accomplishments and several "firsts" since beginning the investigation of electronic crimes. Robert Weaver, assistant to the special agent in charge of the task force, points to the team's 750 arrests and convictions and its $7 million in seized assets as proof of continuing success.

1993. A well-dressed, polished, impeccably credentialed and obviously professional 50-year-old former bank president convinces the manager of an upscale mall in Manchester, Connecticut, to rent space for an automated teller machine (ATM). But the machine is a fake. Over a 3-day weekend, the perpetrator and his two assistants glue shut the openings in the real ATMs, and use the fake one to collect credit card, debit card, and PIN numbers. They then empty out their victims' bank accounts and "bust out" the limit on the credit cards, netting about $120,000 in stolen goods and services. Six weeks later, the perpetrators are arrested by Secret Service and Drug Enforcement Administration agents while preparing to set up another ATM in a Coral Gables, Florida, mall. It is the end of a 10-year crime spree for the leader, a sophisticated, serious, extremely talented computer expert who writes source codes for computer programs and does demographic studies on target areas prior to installing a new ATM. It is one of the country's first cybercrime attacks on financial institutions.

1995. Secret Service agents pose as drug dealers in search of cheap telecommunications equipment after receiving a tip that it is being sold illegally and internationally on the Internet. In this, the first e-mail wiretap in the United States, they eavesdrop on a transaction. In their role as drug dealers, the agents agree to purchase a sophisticated piece of equipment that intercepts wireless messages for their narcotics operation. The device

Continued on page 2

with the U.S. Marshals Service to deputize those who are not Federal officers so they can execute Federal search and arrest warrants.

"We let what's in the best interest of the case decide how it gets worked," Weaver says. "We do a significant amount of State prosecution at the district attorney level. But if penalties are more severe under Federal statutes, we'll move to the Federal level."

Weaver says that NYECTF aims to stay on the leading edge of technology. But, because budgetary concerns always seem to make that difficult, the relationships with partner agencies and industry are the backbone of the team. "You need every asset at your disposal to take the wiggle room out for the bad guys," he says. "But that's easier said than done. That's why we see our relationships with the private sector and with the other agencies on the task force as our most important asset—more important than the cases themselves. Cases come and go."

Weaver says the task force keeps an eye on what it considers to be the top six infrastructure targets for electronic crime or cyberterrorism: financial institutions, telecommunications, the energy industry, transportation, the environment, and emergency services. In addition, task force members are active in the community, take a proactive investigative stance, and help educate private industry about "cyber" threats. NYECTF also cooperates with universities on an internship program that has graduates with computer-related degrees working either for private industry or for an area law enforcement agency.

The New York Electronic Crimes Task Force also has an "open-door" policy when it comes to membership. There is only one caveat: "We do not take reformed hackers and turn them into heroes. We don't need their help. We don't want their help. The only thing we'll do with hackers is debrief them and use the information they provide," Weaver says. Otherwise, prospective members need only a willingness to share information and the ability to work as a team.

Starting your own task force can be equally simple, Weaver says. The team's most important assets should include talented people, the support of each member's department or company, the ability to track technology and the current state of electronic crime, and the ability to anticipate the future. Funding is another component. For NYECTF, he says, it comes from the U.S. Secret Service and corporate donations. The rest—hardware and software included—comes from a number of outside sources. "We are very appreciative of the private sector's cooperation and support with equipment and technology resources."

One of the members of the New York Electronic Crimes Task Force is the National Law Enforcement and Corrections Technology Center (NLECTC)–Northeast, which will lend its technological assistance to the law enforcement

***A History of Success** (continued)*

was developed and was being sold by a talented, well-educated German engineer who speaks three languages and routinely travels to Hong Kong, Taiwan, Europe, and the United States. The engineer is subsequently arrested, convicted, and sentenced to serve 51 months plus a probationary period.

1997. The president and vice president of Breaking News Network, a legitimate news agency, are arrested after Federal officers discover that they have been intercepting the voice and text messages of the New York police and fire departments' commanders. Reporters use the information to scoop their rival media outlets on breaking stories. In particular, they are credited as the first to publicize the story of the Trans World Airlines Flight 800 crash. The maximum penalty for this type of crime, however, is only 6 months' probation per charge. The defendants plead guilty to two charges—illegal interception and dissemination of the police and fire departments' messages. They both receive 12 months' probation.

1999. Federal agents arrest a man selling equipment to intercept information transmitted between police headquarters and the mobile data terminals in patrol cars, and between ambulances and hospitals. This equipment allows the user to access emergency services traffic that includes such sensitive and personal data as accident information, blood type, and physical allergies of crash victims, which can then be changed and retransmitted to the hospital. They can also intercept police transmissions, including incident information, charges, driver's license number, date of birth, criminal history, Social Security number, occupation, and home address. In one case, a Nassau County, New York, resident uses his interception equipment to learn that the local SWAT team is getting ready to execute a high-risk arrest warrant. The radio dispatcher informs all marked units to stay clear of the target area so the suspect will not be forewarned. But the buyer of the equipment immediately posts the SWAT team's plan on the Internet, where it can be read by anyone with a computer and a phone line, including the suspect and his associates.

Best Practices for Seizing Electronic Evidence

Best Practices for Seizing Electronic Evidence is a free, 10-page, pocket-sized manual that provides a basic understanding of key technical and legal factors regarding searching and seizing electronic storage devices and media. Covered are personal computers (including tracing e-mails), electronic paging devices, facsimile machines, caller identification devices, and smart cards.

Continued on page 3

agencies, universities, research laboratories, and private companies comprising the task force.

This partnership will allow NLECTC–Northeast to demonstrate to both public and private sectors those technologies developed for addressing electronic crime, says Fred Demma, a member of NLECTC–Northeast's technical staff. At the same time, the Northeast center will make its knowledge base available to the task force, while learning what kinds of tools investigators need to work cases involving electronic crime. This partnership also gives center personnel the opportunity to participate in the task force's educational effort about how an information system can be compromised and how the system can be protected.

"Private industry may have been reluctant to admit they have a problem," Demma says. "But if you analyze it on a global scale, private industry has had the greatest amount of economic loss."

For more information about the New York Electronic Crimes Task Force, for assistance with an electronic crime-related case, or for task force membership information, call 212–637–4650, or contact Robert Weaver, 212–637–4647. For information about NLECTC–Northeast's participation in the task force, contact Fred Demma, 315–339–6184.

The National Law Enforcement and Corrections Technology Center System

Your Technology Partner

www.justnet.org

800–248–2742

Best Practices *(continued)*

The manual was developed as a project of the International Association of Chiefs of Police Advisory Committee for Police Investigative Operations. The committee convened a working group of various law enforcement representatives, facilitated by the U.S. Secret Service, to identify common issues encountered in today's crime scene.

To order a copy of *Best Practices for Seizing Electronic Evidence,* please contact the International Association of Chiefs of Police, 800–THE–IACP. The publication may also be downloaded from the association's World Wide Web site at www.theiacp.org.

This article was reprinted from the Summer 2000 edition of *TechBeat,* the award-winning quarterly newsmagazine of the National Law Enforcement and Corrections Technology Center system, a program of the National Institute of Justice under Cooperative Agreement #96–MU–MU–K011, awarded by the U.S. Department of Justice.

Analyses of test results do not represent product approval or endorsement by the National Institute of Justice, U.S. Department of Justice; the National Institute of Standards and Technology, U.S. Department of Commerce; or Aspen Systems Corporation. Points of view or opinions contained within this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

The National Institute of Justice is a component of the Office of Justice Programs, which also includes the Bureau of Justice Assistance, Bureau of Justice Statistics, Office of Juvenile Justice and Delinquency Prevention, and Office for Victims of Crime.