<< Return to article

The FBI's Cybercrime Crackdown

A new breed of special agent is taking on high tech criminals.

Make my day: Special Agent Nenette Day hunts down computer crooks from her Boston office. (Photograph by Paul Foley)

By Simson Garfinkel
November 2002

To protect the classified information stored on her desktop computer, Special Agent Nenette Day uses one of the most powerful tools on the planet—an air gap.

Day points to an IBM ThinkPad resting on the table behind her desk. “That computer is hooked up to the Internet,” she says. “But if you break into it, have a good time: there’s no secret work on it.”

Two meters away on her desk sits Day’s other computer—a gray-and-chrome minitower emblazoned with a red sticker proclaiming that its hard drive is classified SECRET. “This,” she says protectively, “holds my e-mail.” Day readily talks about the ThinkPad, describing how she got it as part of a big purchase by the Federal Bureau of Investigation (FBI) a few years ago and explaining that it’s now somewhat out-of-date. And she happily shows off a collectible action figure—still in its display box—a colleague brought back from Belgium. It’s a “cyberagent” with a gun in one hand and a laptop computer in the other. But if you let your eyes drift back to that red sticker and try to copy the bold, black words printed on it, Day will throw you out of her office.

Day belongs to the FBI’s Boston Computer Crime Squad, one of 16 such units located throughout the United States. Each is composed of about 15 agents who investigate all manner of assaults on computers and networks—everything from lone-hacker to cyberterrorist attacks—with a dose of international espionage thrown in for good measure. Crimes range from Web site defacements and break-ins to so-

called denial-of-service attacks, which prevent legitimate users from accessing targeted networks.

The Computer Crime Squads form the heart of the FBI's new Cyber Division. Created as part of the FBI's reorganization that followed September 11, the Cyber Division is the U.S. government's first line of defense against cybercrime and cyberterrorism. Its mission, said FBI Director Robert S. Mueller, when he appeared before the Senate Committee on the Judiciary last May, is "preventing and responding to high tech and computer crimes, which terrorists around the world are increasingly exploiting to attack America and its allies."

The emphasis on cybercrime is a big departure for the FBI. The bureau's agents traditionally got the most attention—and the biggest promotions—by pursuing bank robbers, kidnappers, and extortionists. J. Michael Gibbons worked on one of the FBI's very first computer-crime cases back in 1986; when he left the FBI in 1999, he was chief of computer investigations. "Frankly," says Gibbons, now a senior manager at KPMG Consulting in McLean, VA, "there was no great glory in the FBI on working computer investigation cases."

Hall of Cyberinfamy

John Draper, "Captain Crunch"

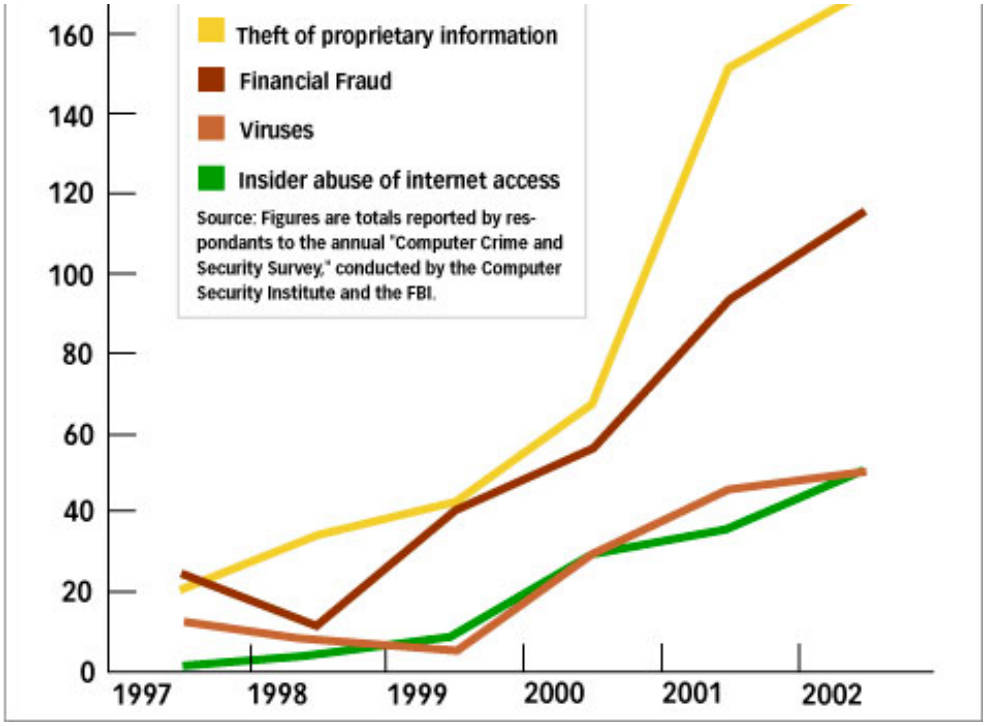
Crime: Draper discovered in 1972 that by blowing the whistle that came with Cap'n Crunch cereal, he could create the 2600-hertz tone necessary to seize control of telephone systems and place free long-distance phone calls.

Punishment: Draper was arrested in May 1972 for illegal use of telephone company property. He was put on probation, but in 1976 he was arrested again on wire fraud charges and spent four months in prison. While serving time, he started programming the EasyWriter word processor for the Apple II computer.

But that attitude is changing as Washington increasingly realizes that big damage can be inflicted on U.S. businesses through their computers and networks. Remember back in February 2000 when a massive denial-of-service attack shut down Web sites belonging to companies such as Yahoo!, eBay, and Amazon.com? It cost those companies literally millions of dollars in lost revenue. That attack, it turns out, was executed by a single high school student. Experts worry that a similar assault on the nation's electric utilities, financial sector, and news delivery infrastructure, could dramatically exacerbate the resulting confusion and possibly even the death toll of a conventional terrorist attack, if the two attacks were coordinated.

Even without the specter of terrorism, cybercrime is bleeding millions of dollars from businesses. Earlier this year, the Computer Security Institute surveyed 503 organizations: together, they reported $456 million dollars in damages due to attacks on their computers and networks over the past year, and more than $1 billion in damage over the previous six years. Those numbers—which are the closest thing that the computer establishment has to reliable figures for the incidence of computer crime—have climbed more than 20 percent since 2001.

Day's activities show that although the FBI, the nation's premier law-enforcement agency, is starting to come to terms with cybercrime, it still has a long way to go. Agents such as Day receive special training and have access to specialized tools (many of which the FBI refuses to discuss). Their equipment, if not always at the James Bond cutting edge, is no longer embarrassingly outdated. On the other hand, the FBI's cybercrime squads are locked in a battle to keep current in the face of unrelenting technological change, and they are so short-staffed that they can investigate only a tiny fraction of the computer crimes that occur. Agents such as Day have served as only a small deterrent to hackers and high tech criminals bent on attacking a society that has become hopelessly dependent on its machines. But the deterrent is growing.



How to Catch a Cybercrook

The phone rings at the FBI Crime Squad and a “complaint agent” answers. Most calls are short, not too sweet, and not terribly satisfying for the person seeking help. “We get a lot of phone calls from people who say that somebody has hacked their home computer,” says Day. Others report death threats delivered in online chat rooms.

Unsettling as such events are for the victims, most callers are told that there’s nothing the FBI can do for them. For one thing, federal computer-crime statutes don’t even kick in unless there is at least $5,000 damage or an attack on a so-called “federal interest computer”—a broad category that includes computers owned by the federal government, as well as those involved in interstate banking, communications, or commerce. In places especially rife with computer crime, like New York City, the intervention bar is even higher.

Even cases whose damages reach the threshold often die for lack of evidence. Many victims don’t call the FBI right away. Instead, they try to fix their computers themselves, erasing their hard drives and reinstalling the operating system. That’s like wiping fingerprints off the handle of a murder weapon: “If you have no evidence, we can’t work it,” says Day. And, of course, an attack over the Internet can originate from practically anywhere—the other side of the street or the other side of the world. “We can’t do a neighborhood sweep and ask, ‘Did you see anybody suspicious walking around here?’” she explains.

For many computer offenses, the FBI lacks not only solid evidence but even the knowledge that an incident has occurred at all. According to this year’s Computer Security Institute survey, only

Hall of Cyberinfamy

Kevin Mitnick

Crime: While in high school, Mitnick broke into computer systems operated by Digital Equipment Corp. and downloaded the source code to the operating system. By 1994 Mitnick was considered the federal government’s most wanted computer hacker.

Punishment: Following a nationwide manhunt, Mitnick was arrested in February 1995 and held for four years without trial. Specific allegations were never published on the grounds of “national security.” Mitnick was released from prison in January 2000 under a plea bargain.

about one-third of computer intrusions are ever reported to law enforcement.
"There is much more illegal and unauthorized activity going on in cyberspace than corporations admit to their clients, stockholders, and business partners, or report to law enforcement," says Computer Security Institute director Patrice Rapalus.

Every now and then, however, all the ingredients for a successful case come together: a caller who has suffered a significant loss, undisturbed evidence, and a perpetrator who is either known or easily findable.

Day remembers a case from October 2000. The call came from the vice president of Bricsnet US, a software company in Portsmouth, NH. Bricsnet had just suffered a massive attack over the Internet. Somebody had broken into its systems, erased customer files, modified financial records, and sent e-mail to Bricsnet's customers, announcing that the company was going out of business.

When Day arrived on the scene she went quickly for what she hoped would be the key source of evidence: the log files. These are the routine records—the digital diary—computers retain about their actions. Computers can keep highly detailed logs: an e-mail server, for example, might track the "To" and "From" addresses, as well as the date, of every message it processes. Some computers keep no log files at all. Getting lucky, Day found that Bricsnet's log file contained the time of the attack and the Internet Protocol, or IP, address, of the attacker's computer.

Every address on the Internet is assigned to either an organization or an Internet service provider. In the Bricsnet case, the address belonged to a local service provider. Day issued a subpoena to that company, asking for the name of the customer "who had connected on this IP address" when the attack took place. This information came from the service provider's own log files.

It turned out that the offending address corresponded to a dial-up connection. Each time a subscriber dials in, the service provider's log files record the date, time, username, and the originating phone number. Within a week of launching the investigation, Day had fingered a likely suspect: Patrick McKenna, a help desk worker whom Bricsnet had fired on the morning of the first attack. McKenna was arrested, charged, and convicted under the Computer Fraud and Abuse Act. He was sentenced in June 2001 to six months in federal prison, followed by a two-year parole. He was also ordered to pay restitution for the damage he had caused, which the court determined to be $13,614.11.

Masked Men and Dead Ends

Day's bust in the Bricsnet case was unusual for its speed and for the resulting conviction. That's because many crimes are perpetrated with stolen usernames and passwords. In the Bricsnet case, for instance, McKenna had broken into the company's computers using his former supervisor's username and password.

The key to cracking the Bricsnet case was caller ID and automatic number identification (ANI), two technologies more and more Internet service providers are using to automatically record the phone numbers of people dialing up their servers. When a crime is committed over a telephone line, this information is invaluable.

"I love ANI," says Day. "The last thing you want to do is show up at Joe Smith's house because some hacker has logged in using Smith's username and password." This tool, she says, "lets you know if you are on the right track. It has made a huge difference." Not all new telecommunications technologies are so helpful, though. Many recent computer attacks, for example, flow from the growing availability of always-on high-speed Internet connections. Attackers employ computer viruses and other

Hall of Cyberinfamy

Kevin Poulsen

Crime: A friend of Kevin Mitnick, Poulsen rigged Los Angeles radio call-in shows to guarantee that a pal would win a car giveaway. He also broke into the FBI's National Crime Information Center, downloading active case files and alerting suspects in undercover

programs to compromise users' home computers, and then they use the compromised computers as platforms for launching other attacks without the owners' knowledge. Even worse, an attacker can jump from system to system, forging a long chain that cannot be traced. Microsoft Windows typically does not keep logs of its activity. "A lot of our investigations have been stopped cold in their tracks because someone is trotting through one of those computers," Day says, referring to cable-modem-connected PCs that run vulnerable copies of Microsoft Windows 95.

FBI investigations.

Punishment: Poulsen spent three years in prison for hacking and was forbidden to touch a computer for three additional years after his release. He is now a journalist, covering computer security for SecurityFocus, an online business service.

Even caller ID and automatic number-identification information can be faked by a person who has control of a corporate telephone system with a certain kind of connection to the public telephone network. So far, faked caller ID hasn't been a problem—but that could change, too.

The Internet's cloak of anonymity has made fighting crime especially tough. It's almost as if there were booths outside banks distributing free ski masks and sunglasses to everybody walking inside. "Anonymity is one of the biggest problems for the FBI crime squads," former agent Gibbons says. He maintains that cybercriminals' ability to disguise their identities does more than just complicate investigations; it also makes attackers more aggressive and more willing to take chances and do damage.

"People act differently when they don't think that they are being held accountable for their actions," says Gibbons. For years, computer security experts have maintained that corrupt employees and former insiders—such as McKenna at Bricsnet—perpetrate the lion's share of computer crime. But Day's experience contradicts this prevailing wisdom. Today things are changing: according to Day, most cases she investigates involve outsiders who commit their crimes anonymously over the Internet—frequently from overseas. Day says she has traced some 70 percent of the attacks to foreign Internet addresses. Nevertheless, insiders still represent the bulk of her investigations as they represent the most damaging attacks.

In one case, Day says, she determined that a major break-in had originated at a cybercafé in a small town in Romania. Because computer hacking is not a crime in Romania, the local police offered no assistance. Seeking help elsewhere, she phoned the café itself and talked with its owner, who spoke fluent English. "The owner said he has a bunch of cyberhackers who come there, but this is Romania, and they pay cash," Day says.

The investigation was terminated.

Attack of the Grownups

The media frequently portray the typical computer criminal as a disaffected male youth, a computer wizard who lacks social skills. In the archetypal scene, FBI agents conduct a predawn raid: with their guns drawn, they arrest a teenager while his horrified parents look on. And in fact, Day says that as recently as five years ago, juveniles made up the majority of the perpetrators she encountered. They were teenagers who broke into Web sites that had little security, and their digital crowbars were tools that they downloaded freely from the Internet. These kids made no attempt to hide their success. Instead, they set up their own servers on the penetrated computers, bragged to their friends, and left behind lots of evidence of their misdeeds.

But such attacks are no longer the most important cases that Day's office investigates. Recent years have brought "an interesting shift," she says. Now she sees attackers breaking into computers that are supposedly protected by firewalls and security systems. These perpetrators—virtually all of them adults—mount extremely sophisticated attacks. They don't brag, and they don't leave obvious tracks. "It's economic espionage," Day concludes.

It's not surprising that these cases are the hardest to crack, she says. One incident involved a suspect who had used a stolen credit card to purchase dial-up accounts at Internet service providers,

Hall of Cyberinfamy

"Mafiaboy"

specifically smaller providers that did not use caller ID or automatic number identification. He then proceeded to quietly break into thousands of computers. Day monitored the attacker for four months, trying to figure out who he was. “He was very good,” she recounts. Then, in the middle of her investigation, the stolen credit card was canceled and the dial-up accounts were closed. “I was horrified,” she says. The investigation fell apart, and the perpetrator is still at large.

Crime: This Canadian juvenile was responsible for the February 2000 denial-of-service attacks on CNN, Yahoo!, E*Trade, and other major Web sites.

Punishment: Arrested in April 2000 by the Royal Canadian Mounted Police working in cooperation with the FBI, the youth, whose name was withheld because of his age, pled guilty to 56 counts of computer crime in January 2001. He was sentenced in September 2001 to eight months of “open custody” and one year probation, as well as restricted access to the Internet.

Computer crime culprits defy stereotyping. One case that was successfully prosecuted—after a three-year investigation by the FBI—involved an assistant principal at a Long Island high school. The school administrator flooded the e-mail systems at Suffolk, James Madison, and Drexel universities with tens of thousands of messages, causing significant damage. In July 2001 the culprit, whose crimes carried punishments as high as a year in jail and $200,000 in fines, was sentenced to six months in a halfway house.

In the coming years the widespread adoption of wireless-networking technology will probably pose the biggest problem for the FBI cybercrime squad. These networks, based on the 802.11(b), or Wi-Fi, standard, let people use laptops and handheld computers as they move freely about their homes and offices. But unless additional protective measures are taken, wireless signals invariably leak beyond buildings’ walls: simply lurking within the 100- to 300-meter range of a typical base station, an attacker can break into a network without even picking up a telephone or stepping onto the victim’s property. “Many people who are moving to wireless as a cost-saving measure don’t have any appreciation of the security measures they should employ,” explains Special Agent Jim Hegarty, Day’s supervisor.

And as the Boston cybercrime unit has discovered, wireless attacks are not just theoretical. The wireless network of one high tech company recently suffered a break-in. According to Hegarty, the attacker—an activist who was opposed to the company’s product and management—literally stationed himself on a park bench outside the company’s offices and over the course of several weeks, used the wireless network to “sniff” usernames and passwords of the company’s president and other senior-level executives. The activist then used the information to break into the company’s computers—again, making his entry through its wireless network. Armed with this illicit access, the attacker downloaded months of e-mail and posted it on the Web.

The e-mail contained confidential information about customers and their contracts. Once that became public, all hell broke loose. Some customers who discovered that they were paying higher rates than others demanded better deals; others canceled orders upon discovering that the vendor had been selling the same product to their competitors. Ultimately, the attacked company suffered more than $10 million in direct losses from the break-in. As wireless networks proliferate, attacks of this kind are likely to become more common, according to Hegarty. The advent of 802.11, he says, “is going to be a watershed event for us.”

All in a Day’s Work

When *Technology Review* first approached the FBI about interviewing an agent of the computer crime squad, the idea was to write about an agent’s “average day.” The public affairs manager at the FBI’s Boston office nixed the idea: there are no average days for an FBI agent, she said. Indeed, Day says that one of the best things about her job is its endless variety.

“I might spend one day in trial preparation. I could spend an entire day milling through computer files doing evidence assessment. The next day I could be scheduled to testify in a trial. And last month I spent a couple weeks in Bangkok, Thailand, teaching police from 10 different Asian countries.” She spends some days on the phone, perhaps overseeing a new case coming in from a financial institution or phoning FBI headquarters with information that needs to be relayed to other field offices. A few days later she might be off to the range for weapons training. Agent Day

carries a .40-caliber Glock 23 and assists on the occasional drug raid. “It is very long work, and it’s very hard,” she says about her job, “but it gives you something that you would never see in the private sector.”

The Glock doesn’t get much use out there on the Internet, of course, but Day’s FBI training in understanding criminal behavior does. She is, for example, involved in a project at the FBI’s research center in Quantico, VA, developing a psychological profile of serial hackers—people who might become criminals or could be hired by a foreign government. A serial hacker could be a powerful tool for Al Qaeda or some other terrorist organization.

Moving forward, the biggest challenge, says Day, will be for society as a whole “to try to define and distinguish between what is basically online vandalism—when somebody is damaging a business or a computer—and cyberterrorism. All of those things are conflated in the discussion of the criminal prosecution of hackers. In my mind those are different kinds of contact with different social harm.”

Hall of Cyberinfamy

Onel de Guzman

Crime: In May 2000 the ILOVEYOU computer worm spread throughout the world as an e-mail attachment. Worldwide damage in lost productivity and clogged networks was estimated at $10 billion.

Punishment: The FBI quickly traced the worm to the Philippines and identified computer science student De Guzman as the perpetrator. Phillipine authorities brought charges against him but then dismissed the case in August 2000, saying that the country’s laws did not cover computer crime.

Today cybercrime is one of the FBI’s top priorities—even above fraud, drugs, and gun running, says Day. But while scary talk of cyberterrorism captures the headlines, the most damaging cybercrime may actually be old-fashioned crimes being committed with new and virtually untraceable tools. Catching the new bad guys will require people like Nenette Day to stay on technology’s leading edge, but it will also require an FBI able to build an organization that gives Day and her fellow agents adequate support. Furthermore, it will require the capability to bring superior computing firepower against the cyberattackers and beat them at their own high tech game.

Simson Garfinkel writes on information technology and its impact. He is the author of *Database Nation* (O'Reilly, 2000).