MILLIONS INVESTED IN FIGHTING CYBERCRIME AROUND THE WORLD

Law enforcement officials are spending millions of dollars on training and investigations as part of a global effort to thwart the theft and disruption of digital information, according to experts attending the Workshop on the Economics of Information Security (WEIS) hosted by the Center for Digital Strategies at the Dartmouth's Tuck School of Business in Hanover, NH.

The annual conference, sponsored by CDS, Microsoft, The Institute for Infrastructure Information Protection (I3P) and Dartmouth's Institute for Security Technology Studies, attracted more than 100 academics, researchers, government officials and law enforcement agents from around the world.

"Our primary focus is counter- intelligence and counter- terrorism using computers, so called cyber-terrorism," said Jim Burrell, assistant special agent in charge of the Federal Bureau of Investigation's Boston office. "I put about 80% of my resources there. The other side is everything else…from intellectual property theft to internet fraud and child pornography, things along those lines where the computer is used to facilitate a more traditional crime."

Burrell, an internationally respect expert on cybercrime, said back in the late 1990's, "we treated cybercrime and a lot of these issues as a single violation. Now, we have about 300 different cyber-criminal violations as well as national security issues."

He said the FBI is investing millions of dollars in training top agents to fight cybercrime with assistance from law enforcement agencies in 48 countries. When dealing abroad, Burrell said, the first priority for investigators and agents is to preserve digital data. Without intact data, it's almost impossible to build a strong case again savvy cybercriminals.

"The issue we worry about first is preserving the evidence so it doesn't get deleted or altered," said Burrell, who also teaches digital forensics at Boston University. "That doesn't mean they (local agents) have to turn it over to us, but (we ask them to) make it so it doesn't go away until we can figure out what's going on. Then, we can get the proper diplomatic or legal process in order to obtain physical custody of the information or the data."

Federal prosecutor Arnold Huftalin agreed that data preservation is critical to successful prosecutions.

"I learned early on in my computer crime experience that data is extraordinarily volatile," said Huftalin, an assistant U.S. attorney based in New Hampshire. He said his biggest challenge was tracking down how criminals are accessing the internet. For example, a few years ago, he had a case where he had to locate hundreds of people around the country through IP addresses that they were using to access servers.

“I was appalled to find out there was no nationwide database of internet service providers,” said Huftalin. To remedy that, he assigned a paralegal to set up an extensive database, which is still being used by cybercrime prosecutors around the country.

Once the providers were found, subpoenas for information could be issued, but that’s tough because people can change ISP’s (internet service providers) on a moment’s notice, he said.

“Nobody but the dumbest of the dumbest people in the world is going to go into somebody’s (computer) system from their own static IP (address),” he said. “They are going to come in through some innocent person’s box in Romania which is going to be access through some other innocent person’s box in Turkey.”

He said the federal Electronic Communications Privacy Act (ECPA) dictates how federal, state and local law enforcement agencies can compel disclosure in order to collect data for criminal cases.

Because organized crime is now heavily involved in computer crimes, Huftalin said it’s actually easier to track them down.

“They tend to be a bit more static and they’re not as elusive as the 19 year-old whiz kid who just happens to want to bounce through 18 machines and they for giggles and grins, destroys somebody’s network.”

Huftalin said cracking computer cases is tough and “there are a lot of prosecutors who, when they see a laptop, will walk away from it,” because it takes computer savvy to work in the field.

“When there’s a bank robbery and it’s in the winter, you follow the footprints in the snow,” he said. “But when somebody intrudes into, let’s say, Google, there aren’t any footprints in the snow.”

Despite firewalls and sophisticated software, panelists said corporations continue to be attacked by cybercriminals, the panel said. “Corporations that experience security breaches may be reluctant to provide information to law enforcement because it will affect their bottom line,” said Huftalin, the federal prosecutor from New Hampshire. “But, if they don’t provide the information, then law enforcement can’t share that information with other corporations so they can plug the holes or take security measures in advance, as opposed to after the fact.”

He said there is a program called “InfoGuard” which encourages companies to report data breaches to law enforcement agencies so criminals can be prosecuted in a timely manner.

In addition to the FBI’s efforts, panelists said state and local officials are working hard to combat cybercrime at all levels.

“Almost every crime that we deal with at the state level has some kind of computer component,” said Lucy Carrillo, assistant attorney general for the New Hampshire Criminal Justice Bureau. “Whether it’s the drug dealer who has lists, phone numbers addresses on his cell phone or whether it’s a homicide scene where the individual has done research on how he was going to commit a homicide.”

William “Trip” Cantwell, with the New Hampshire State Police, said public awareness is critical to thwarting all sorts of computer crime. For example, he makes presentations to school children about the dangers of the internet.

“We reach out to them and show them some presentations,” he said. “Hopefully it will hit home and prevent one kid from being victimized.”

Jane Applegate

PR & Marketing Manager
Center for Digital Strategies