Local police grapple with response to cybercrimes

EILEEN SULLIVAN, Associated Press

WASHINGTON (AP) -- If a purse with $900 is stolen, the victim probably would call the police. If a computer hacker steals $900 from that same person's bank account, what then? Call the police? Could they even help?

As it is now, local police don't have widespread know-how to investigate cybercrimes. They rely heavily on the expertise of the federal government, which focuses on large, often international cybercrimes.

What's missing is the first response role, typically the preserve of local police departments that respond to calls for help from individuals and communities.

Obama administration officials have said that cyberterrorism is the leading worldwide threat to national security. So far, the discussion about such threats and security has focused on breaking classified foreign government codes, monitoring overseas communications and protecting the U.S. from devastating attacks that could jeopardize massive amounts of data and valuable corporate trade secrets.

It's been about businesses protecting their networks and individuals using the Internet safely, for instance, by choosing smart passwords.

But when one person hacks into someone else's computer to access a bank account, credit cards or even email, the crime fighting path is uncertain.

"I am not sure who owns cybercrime at the local level. And that is a problem," said Chuck Wexler, executive director of the Police Executive Research Forum.

Local police departments are looking to boost their expertise so they can respond to cybercrimes and cyberthreats that are expected to only get worse.

The hypothetical victim who had $900 stolen from the bank account should call the police, and the police should document the theft in a report, said Darrel Stephens, executive director of the Major City Chiefs Association, which represents police chiefs in major U.S. metropolitan areas.

"What they can do after that gets very complicated," Stephens said.

For instance, police departments work within jurisdictions, but cybercrime knows no boundaries.

"The victim may live in one place, their bank is in another jurisdiction and the person that committed the theft could be anywhere in the world," Stephens said.

Then there's the matter of determining who the victim is.

Most banks and credit card companies typically replace the accountholder's stolen funds, he said, which makes the banks and credit companies the victims of the theft.

"Most local police do not have the capacity to investigate these cases even if they have jurisdiction," Stephens said.

Further complicating the issue is that the response to a cyberoffense is not the same as the response to a physical offense such as a burglary.

When someone's home is burglarized, the homeowner doesn't usually repair the broken window, clean up the crime scene and then call the police. But in cases such as network intrusions, the victim's first goal typically is intended to get the network restored and working again. In doing this, initial crime scene evidence may be sacrificed, complicating an investigation down the road.

"Police will need to become more equipped to deal with cybercrime in the future," Stephens said. "Most major cities have a limited capability, but more will be required."

Bart Johnson, executive director of the International Association of Chiefs of Police, said police need to have a better understanding of what a cyberthreat is and how to address it. Johnson said his organization has been working with the FBI and Homeland Security Department since December to confront these issues.

"The unfortunate thing is that law enforcement at a state and local level are not fully apprised of the threat, who the actors are," said Johnson. The FBI and Secret Service have the capabilities to address this, he said, but more expertise is needed at the local level.

The Secret Service has trained some 1,400 state and local law enforcement officers on cybercrimes since the agency began the education program in 2008, said Hugh Dunleavy, deputy assistant director of the Secret Service, which specializes in investigating such crimes. But the demand for training is greater than the agency can provide, he said.

Some local police officers may participate on some task forces with the FBI, Secret Service and other federal agencies, but the cases typically are those with international components and involve millions of dollars.

Mike Sena, president of the National Fusion Center Association, an organization that represents state and local intelligence centers around the country, recalled a case in which a California business was the victim of a cybercrime and lost $40,000. Sena said the theft wasn't great enough for the federal government to take up the investigation, and there was confusion about where to turn at the local level.

"The FBI and Secret Service are looking at just large amounts of thefts. Who takes care of that lower tier," Sena said.

Several current task forces coordinate with local law enforcement on cyberissues, and the federal government offers some guidance for where to turn, depending on the incident and depending on who is asked.

According to the Justice Department, if a computer is hacked, you can call your local FBI office or the Secret Service or the Internet Crime Complaint Center, which is run by the FBI and the nonprofit National White Collar Crime Center.

For Internet fraud and spam, you can call your local FBI office, the Secret Service, or file an online complaint with the Federal Trade Commission or the Securities and Exchange Commission. There are also Secret Service-led Electronic Crimes Task Forces in 29 cities, and they regularly work with state and local law enforcement.

But figuring out which task force or which federal investigative agency to turn to can be a challenge. Not everyone will have the expertise to know what time of crime occurred so that the right agency can be contacted, said Shawn Henry, former top cybercop at the FBI and currently president of CrowdStrike Services, a security technology company.

That leaves few options for a victim of a cybercrime whose loss would be considered small by the federal government but crippling to the individual or small business.

"Right now there's such a level of confusion on where to push the information," Sena said.

Dunleavy said he is confident that local law enforcement at least knows who to call, but there is a need for more training.

"The general public is going to call who they know the best," Dunleavy said. "They're going to call the police officer that they see on a daily basis for response."