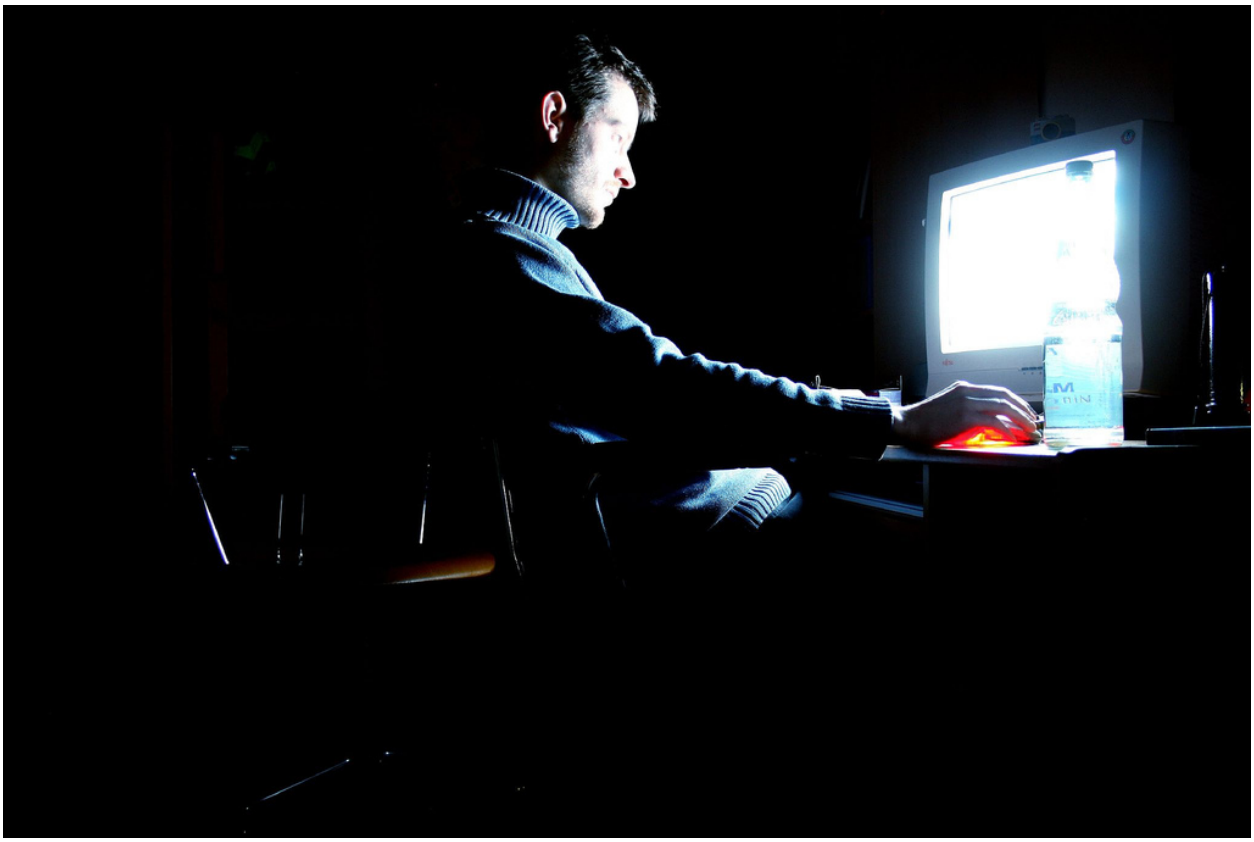
Feds Admit Cooperation Remains an Obstacle With Corporations and Cyber threats

July 31, 2014



A key to reducing cyber crime is getting victims — often major corporations — to cooperate with authorities, two top federal law enforcement officials said on Wednesday during visits to Pittsburgh.

Assistant Attorney General for National Security John P. Carlin said investigators don't just need to know how cyber criminals breached a system.

“We also need to figure out what the companies are doing in their business to attract the threat,” Carlin said, noting some companies are reluctant to share inside information to catch a thief.

“Some companies worry about the embarrassment factor of reporting an attack or working with law enforcement. There are others who are concerned their business will be turned into a crime scene and an investigation will do more harm than good,” Carlin said.

Pittsburgh figures prominently in the global war on cyber crime. Chinese military hackers are accused of targeting some of its biggest companies, and some of the

world's top cyber sleuths are based here, helping to bring indictments against the military hackers and bring down two Russian-based cyber crime schemes accused of stealing more than $100 million worldwide, officials said.

“Pittsburgh is the leader in our nation in fighting that threat,” FBI Director James B. Comey said, referring to locally based FBI agents who specialize in the field as well as groups such as the National Cyber-Forensics & Training Alliance, whose work has helped convict more than 300 cyber criminals.

Comey, sworn in as the FBI's seventh director in November, said he intends to hire 1,500 agents and would be “sending a bunch” to work in Pittsburgh's cyber unit, though he did not provide specifics.

Audrey Russo, president and CEO of the Pittsburgh Technology Council, said some companies believe they did something wrong by not properly safeguarding their networks.

Carlin said taking precautions is critical, but he added, “The first question shouldn't be, ‘What did that company do wrong?' It should be, ‘How can we get the people who did this?' If you're a company today, you've either been hacked or you just don't know that you have been hacked.”

Cooperation has improved over the past eight or nine years, but Carlin said it needs to get better.

Among steps taken to spur cooperation, he said, the Justice Department and Federal Trade Commission in April released a statement noting that antitrust law should not be a barrier to legitimate sharing of cyber security information. In May, the Justice Department released a white paper saying the Stored Communications Act does not ordinarily restrict network operators from sharing certain data with the government to protect information.

Lack of cooperation is just one of many challenges authorities face as they try to clamp down on cyber attacks that threaten American companies and security. Others include gaining more cooperation from foreign governments, attracting top talent to fight cyber criminals, and bringing the elusive criminals to justice, the officials said.

Critics questioned the May indictments of the military hackers, arguing the Chinese government never will agree to extradite them. Former Pennsylvania Gov. Tom Ridge, a former Homeland Security secretary, called the indictments a “public relations stunt” in an interview with the Tribune-Review in June.

Responded Carlin: “We should not and will not stand idly by, tacitly giving permission to anyone to steal from us. We will hold accountable those who steal, no matter who they are, where they are or whether they steal in person or through the Internet.”