June 2007

CYBERCRIME

Public and Private Entities Face Challenges in Addressing Cyber Threats

GAO Accountability · Integrity · Reliability

Highlights

Highlights of GAO-07-705, a report to congressional requesters

Why GAO Did This Study

Computer interconnectivity has produced enormous benefits but has also enabled criminal activity that exploits this interconnectivity for financial gain and other malicious purposes, such as Internet fraud, child exploitation, identity theft, and terrorism. Efforts to address cybercrime include activities associated with protecting networks and information, detecting criminal activity, investigating crime, and prosecuting criminals.

GAO's objectives were to (1) determine the impact of cybercrime on our nation's economy and security; (2) describe key federal entities, as well as nonfederal and private sector entities, responsible for addressing cybercrime; and (3) determine challenges being faced in addressing cybercrime. To accomplish these objectives, GAO analyzed multiple reports, studies, and surveys and held interviews with public and private officials.

What GAO Recommends

GAO recommends that the Attorney General and the Secretary of Homeland Security help ensure adequate law enforcement analytical and technical capabilities. In written comments on a draft of this report, the FBI and the U.S. Secret Service noted efforts to assess and enhance these capabilities.

www.gao.gov/cgi-bin/getrpt?GAO-07-705.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Dave Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

Cybercrime has significant economic impacts and threatens U.S. national security interests. Various studies and experts estimate the direct economic impact from cybercrime to be in the billions of dollars annually. The annual loss due to computer crime was estimated to be $67.2 billion for U.S. organizations, according to a 2005 Federal Bureau of Investigation (FBI) survey. In addition, there is continued concern about the threat that our adversaries, including nation-states and terrorists, pose to our national security. For example, intelligence officials have stated that nation-states and terrorists could conduct a coordinated cyber attack to seriously disrupt electric power distribution, air traffic control, and financial sectors. Also, according to FBI testimony, terrorist organizations have used cybercrime to raise money to fund their activities. Despite the estimated loss of money and information and known threats from adversaries, the precise impact of cybercrime is unknown because it is not always detected and reported (cybercrime reporting is discussed further in GAO's challenges section).

Numerous public and private entities have responsibilities to protect against, detect, investigate, and prosecute cybercrime. The Departments of Justice, Homeland Security, and Defense, and the Federal Trade Commission have prominent roles in addressing cybercrime within the federal government, and state and local law enforcement entities play similar roles at their levels. Private entities such as Internet service providers and software developers focus on the development and implementation of technology systems to detect and protect against cybercrime, as well as gather evidence for investigations. In addition, numerous cybercrime partnerships have been established between public sector entities, between public and private sector entities, and internationally, including information-sharing efforts.

Entities face a number of key challenges in addressing cybercrime, including reporting cybercrime and ensuring that there are adequate analytical capabilities to support law enforcement (see table). While public and private entities, partnerships, and tasks forces have initiated efforts to address these challenges, federal agencies can take additional action to help ensure adequate law enforcement capabilities.

Challenges to Addressing Cybercrime

Challenge	Description
Reporting cybercrime	Accurately reporting cybercrime to law enforcement
Ensuring adequate law enforcement analytical and technical capabilities	Obtaining and retaining investigators, prosecutors, and cyberforensics examiners Keeping up-to-date with current technology and criminal techniques
Working in a borderless environment with laws of multiple jurisdictions	Investigating and prosecuting cybercrime that transcends borders with laws and legal procedures of multiple jurisdictions
Implementing information security practices and raising awareness	Protecting information and information systems Raising awareness about criminal behavior

Source: GAO.