June 28, 2012

INFORMATION SECURITY

Cyber Threats Facilitate Ability to Commit Economic Espionage

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-876T, a testimony before the Subcommittee on Counterterrorism and Intelligence, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

The threat of economic espionage—the theft of U.S. proprietary information, intellectual property (IP), or technology by foreign companies, governments, or other actors—has grown. Moreover, dependence on networked information technology (IT) systems has increased the reach and potential impact of this threat by making it possible for hostile actors to quickly steal massive amounts of information while remaining anonymous and difficult to detect. To address this threat, federal agencies have a key role to play in law enforcement, deterrence, and information sharing. Consistent with this threat, GAO has designated federal information security as a governmentwide high-risk area since 1997 and in 2003 expanded it to include protecting systems and assets vital to the nation (referred to as critical infrastructures). GAO was asked to testify on the cyber aspects of economic espionage. Accordingly, this statement discusses (1) cyber threats facing the nation's systems, (2) reported cyber incidents and their impacts, (3) security controls and other techniques available for reducing risk, and (4) the responsibilities of key federal entities in support of protecting IP. To do this, GAO relied on previously published work in this area, as well as reviews of reports from other federal agencies, media reports, and other publicly available sources.

What GAO Recommends

In prior reports, GAO has made hundreds of recommendations to better protect federal systems, critical infrastructures, and intellectual property.

View GAO-12-876T. For more information, contact Gregory C. Wilshusen (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The nation faces an evolving array of cyber-based threats arising from a variety of sources. These sources include criminal groups, hackers, terrorists, organization insiders, and foreign nations engaged in crime, political activism, or espionage and information warfare. These threat sources vary in terms of the capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage, among others. Moreover, potential threat actors have a variety of attack techniques at their disposal, which can adversely affect an organization's computers or networks and be used to intercept or steal valuable information. The magnitude of the threat is compounded by the ever-increasing sophistication of cyber attack techniques, such as attacks that may combine multiple techniques. Using these techniques, threat actors may target individuals and businesses, resulting in, among other things, loss of sensitive personal or proprietary information.

These concerns are highlighted by reports of cyber incidents that have had serious effects on consumers and businesses. These include the compromise of individuals' sensitive personal data such as credit- and debit-card information and the theft of businesses' IP and other proprietary information. While difficult to quantify monetarily, the loss of such information can result in identity theft; lower-quality counterfeit goods; lost sales or brand value to businesses; and lower overall economic growth and declining international trade.

To protect against these threats, a variety of security controls and other techniques are available. These include technical controls such as those that manage access to systems, ensure system integrity, and encrypt sensitive data. But they also include risk management and strategic planning that organizations undertake to improve their overall security posture and reduce their exposure to risk. Further, effective public-private partnerships are a key element for, among other things, sharing information about threats.

Multiple federal agencies undertake a wide range of activities in support of IP rights. Some of these agencies include the Departments of Commerce, Justice, and Homeland Security, among others. For example, components within the Justice Department and the Federal Bureau of Investigation are dedicated to fighting computer-based threats to IP. In addition, both Congress and the Administration have established interagency mechanisms for better coordinating the protection of IP. Ensuring effective coordination will be critical for better protecting the economic security of America's businesses.