Biggest Security Threat? Insiders
Wed Oct 2, 5:00 AM ET

Juan Carlos Perez, IDG News Service

U.S. companies worried about hackers stealing their trade secrets should be even more afraid of former employees, competitors and contractors, according to a new study.

Intellectual property and proprietary information are more at risk from ex-employees, foreign and domestic competitors and contractors working on-site than from computer hackers, according to a study released this week PricewaterhouseCoopers, the U.S. Chamber of Commerce (news - web sites) and the American Society for Industrial Security (ASIS) International.

Losses Hit $59 Billion

The study, titled "Trends in proprietary information loss," defines proprietary information and intellectual property as "information that is not within the public domain and which the owner has taken some measures to protect." It refers to, for example, information about new products and services.

"The 'insider' threat problem is perceived to be the most serious. This means that companies may want to consider investing more in human resources and vendor screening processes, as well as educating employees about tools and techniques to upgrade their information technology security practices," the study reads.

The study's findings are based on survey responses from 138 chief executive officers of U.S. companies of all sizes. Respondents were asked about intellectual property and proprietary information losses incurred between July 1, 2000 and June 30, 2001. About 40 percent of the companies polled reported suffering the loss of this type of confidential information.

Based on the survey responses, the study concluded that U.S. companies suffered up to $59 billion in intellectual property and proprietary information losses between July 2000 and June 2001. Most of those losses resulted from legal fees and lost revenue associated with the theft of this privileged information. Areas affected included research and development, customer information and financial data.

Don't Forget Hackers

Computer hackers ranked fifth in terms of risks to intellectual property and proprietary information, followed by vendors and suppliers, current employees, partners, intelligence services, external manufacturers and the media.

However, as more and more sensitive corporate information is stored and transmitted using IT systems, the issue of hackers "is an area that should be earmarked for heightened scrutiny by businesses," the study reads.

In what will be good news to hackers, most respondents don't require that this type of confidential information be encrypted when sent over the Internet. However, most respondents do recognize that the Internet, computer networks, computing devices and related products create new threats to the protection of intellectual property and proprietary information.