Industrial Espionage (3):
Survey Results
by M. E. Kabay, PhD, CISSP
Associate Professor, Information Assurance
Norwich University, Northfield VT

In the first two articles in this series, I reviewed some of the information in the annual reports of the National Counterintelligence Center (NACIC) and later the Office of the National Counterintelligence Executive (ONCIX). In this article, I cite some interesting estimates from a survey of industrial espionage conducted by security associations and by the NACIC itself.

In 1995, the American Society for Industrial Security (ASIS, <http://www.asisonline.org>) ran a survey that was used by NACIC in its report. Among the significant findings were the following (quoting NACIC but adding bullets):

- Reported incidents increased 323 percent since 1992.
- Losses of corporate information increased from a reported 9.9 incidents per month in 1992 to an average of 32 incidents per month in 1995.
- About three-fourths of reported losses occurred in the United States, and the majority of those incidents involved "trusted relationships" (employees, vendors, contractors, retirees, and so forth).
- Other incidents were attributable to a variety of sources: domestic competitors, computer hackers, foreign competitors, foreign intelligence services, and foreign business partners.
- Of incidents outside the United States, approximately half took place in countries traditionally considered allies of the United States.
- Foreign nationals were identified in 21 percent of the incidents where the perpetrator's nationality was known.

The 1997 NACIC report cited work by the Computer Security Institute (CSI <http://www.gocsi.com>) in cooperation with the FBI’s International Computer Crime Squad in San Francisco. Interesting results included the following (bullets added to verbatim quotes):

- According to the survey, about 75 percent of the 563 responding corporations, government agencies, financial institutions and universities surveyed by CSI reported financial losses in the past 12 months.
- [In 1996] financial losses from financial fraud, computer viruses, sabotage, and theft of proprietary information and laptops were up seven percent and topped $100 million. Reflecting the increased competition in the global marketplace, over 50 percent of the respondents cited foreign competitors as a likely source of attack and 22 percent cited foreign governments as a likely source of attack.
- The survey also showed that only 17 percent of the respondents reported crimes to law enforcement authorities. There appears to be reluctance on the part of the private sector to report allegations of computer and economic crime to law enforcement authorities. A large number of these crimes go unreported because of a company's fear of undermining...
the confidence of their shareholders, negative publicity, and further exposure of trade secret information during prosecution.

In 1998, NACIC reported on a then-new economic modeling tool developed at the Department of Energy’s Pacific Northwest National Laboratory (PNNL) that was applied to a single case of theft of intellectual property in which a foreign competitor succeeded in capturing the market due to the theft. “Using this tool, the misappropriation of intellectual property in this case resulted in over $600 million in lost sales, the direct loss of 2,600 full-time jobs, and a resulting loss of 9,542 jobs for the economy as a whole over a 14-year time frame. Analysis also determined that the US trade balance was negatively impacted by $714 million and lost tax revenues totaled $129 million.”

I continue my survey of industrial-espionage surveys in the next article in this series.

* * *


M. E. Kabay, PhD, CISSP is Associate Professor in the Division of Business and Management at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mkabay@norwich.edu>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2005 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.