The “10th Annual Trends in Proprietary Information Loss Survey” (2002; PDF available at <http://tinyurl.com/cyca3>) organized by ASIS reported that respondents in 138 companies in the Fortune 1,000 and from the US Chamber of Commerce membership list experienced losses totaling over $50B. About 40% of the respondents reported industrial espionage incidents during the period July 1, 2000 to June 30, 2001. The Executive Summary (pages 1-2) summarizes the risk factors and impacts of loss as follows:

RISK FACTORS
- The greatest risk factors associated with the loss of proprietary information and intellectual property among all companies responding were former employees, foreign competitors, on-site contractors, and domestic competitors. Hackers also were cited as a major concern among some sectors.
- The most commonly cited areas of risk by companies that reported an incident were: research and development (49%), customer lists and related data (36%), and financial data (27%).
- The number of reported incidents, in order of magnitude, were: 1) customer data, 2) strategic plans, 3) financial data, and 4) R&D.

IMPACT OF LOSS
- Among all companies, the greatest impacts of proprietary information loss were increased legal fees and loss of revenue. For large companies (over $15 billion), loss of competitive advantage was the most serious problem. For financial firms, embarrassment was the biggest concern; and for high technology companies, the major issue was loss of competitive advantage.
- The assessment or assignment of intellectual property value is the responsibility of in-house patent and legal counsel who base their judgments on competitive advantage, profitability, and research and development criteria.

In 2004, the ONCIX reported to Congress that
- “… a recent private US survey indicated that more than half of the impacted firms do not
report the breach for fear of reducing shareholder value. As a result, no one is certain how much technology and sensitive proprietary information are lost annually to cyber theft.”

- “During FY2004, the US Department of Immigrations and Customs Enforcement (ICE) conducted more than 2,500 export investigations involving violations of the Arms Export Control Act, International Traffic in Arms Regulations (ITAR), Export Administration Regulations (EAR), International Emergency Economic Powers Act, and the Trading With the Enemy Act. These investigations resulted in 146 arrests, 97 criminal indictments, and 79 criminal convictions.”

In the next article in this series, I review information about the origin of these industrial espionage attacks.

* * *


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.