

Corporate Espionage and Theft of Trade Secrets

In September, 2000, a special Subcommittee on International Economic Policy and Trade conducted a hearing and subsequently issued a report on “Corporate and Industrial Espionage and Their Effects on American Competitiveness.” The report began by stating, “*The threat of economic and industrial espionage looms over the horizon of the business world like a gray cloud threatening a placid sea.*”

According to this report and other multiple sources, intellectual property crimes are on the rise in the United States. This is due to 1) society’s and businesses’ increasing use of and reliance on technological advancements for communication, research, design, and storage of information, 2) a highly competitive marketplace coupled with corporate willingness to venture into the “gray areas” of information gathering, and 3) a modern, transitory workforce with a different concept of company loyalty than what was once considered the norm. Statistics show that:

- Between 1990 and 1995, acts of economic espionage increased 300% as a result of the ease with which trade secrets can be misappropriated and disseminated via the Internetⁱ
- Fortune 1000 companies sustained losses of more than \$45 billion in 1999 from the theft of proprietary information—up from \$24 billion in the mid-1990’s according to FBI estimates—with manufacturing experiencing the highest losses at nearly \$900 millionⁱⁱ
- A 2002 survey by the Computer Security Institute revealed that 90% of respondents had detected computer security breaches within the past 12 months, and 89% acknowledged financial losses due to those breaches, with the most serious financial losses occurring through the theft of proprietary information (26 respondents/\$170,827,000)ⁱⁱⁱ
- The average Fortune 1000 company reported 2.5 incidents of unauthorized use of proprietary information with an average loss per incident in excess of \$500,000, with most incidents occurring in the high technology and service sectors^{iv}
- Forty-four of the 97 companies that participated in an American Society for Industrial Security (ASIS) survey reported a total of more than 1,000 separate incidents of theft of intellectual property or trade secrets^v
- According to a recent study by the SANS (SysAdmin, Audit, Networking, and Security) Institute, total losses from theft of trade secrets are estimated in the range of \$100 billion^{vi}
- According to a survey conducted by the Computer Security Institute, approximately 20% of the 585 respondents said they had been victims of trade secret information theft, with those losses being the most expensive crime (as compared to other security breaches, i.e., hacking, phishing, etc), with 66 of the 585 respondents reporting over \$66 million in losses^{vii}
- 90% of businesses have had one major security breach in the last two years^{viii}
- In Silicon Valley, at least 20 foreign nations have tried repeatedly to steal U.S. trade secrets over the past five years^{ix}

What is a Trade Secret?

Trade secrets are *not* patents, trademarks, or copyrights. Unlike these other forms of intellectual property, trade secrets are “unregulated” and have no pre-determined life-span; they are trade secrets until they become publicly known or are otherwise no longer valuable to the company.

A trade secret is generally defined as information—client lists, marketing plans, new product designs, formulas, methods, manufacturing processes, supplier agreements, pricing strategies, source code, technological innovations, etc—that is intrinsically valuable to a company’s business and which would be detrimental to the company if the information was known by a competitor.

However, it is not only the importance of the information and the damage that would be done to the company if the information were known that defines a trade secret in the eyes of the law; it is further defined by 1) the extent to which the information may be known outside the company and/or the ease with which it could be discovered, and 2) the actions the company takes to protect that information. If a company cannot demonstrate that it has taken “reasonable” precautions to protect trade secret information, there is little or no recourse under the law if that information is acquired by a competitor.

Those “reasonable” precautions that establish company information as a trade secret may include (but are not limited to) advising employees of the existence of a trade secret, limiting access to information to a “need to know basis,” requiring employees to sign confidentiality agreements, developing a security plan for safeguarding the information, clearly identify all trade secret documents as “Confidential,” and keeping documents containing trade secret information under lock and key.

Who Steals Trade Secrets—and How?

Although corporate espionage by outsiders penetrating corporate offices does occur and can be damaging, it is not the major avenue for the theft of corporate trade secrets. Studies agree overwhelmingly that the number one threat of corporate espionage comes from *within* an organization; either with deliberate intention or innocently unknowing, individuals on the inside (employees, partners, vendors, etc) are the largest source of trade secret information.

The majority of corporate information lost through corporate espionage—i.e., theft of trade secrets—can be attributed to one of three primary causes:

- Lack of training and/or mistakes made by authorized members of an organization
- Failure of administrators to implement and maintain security measures
- Disgruntled and/or dissatisfied individuals within an organization, i.e., past and present employees

The methods by which the theft of trade secrets is accomplished include such diverse techniques as a review of publicly available records, the Internet (legitimately or through scams), employee solicitation, conferences, facility/office visitors, dumpster diving, and independent entrepreneurs or organized crime (including terrorists) expressly hired to steal trade secrets.

How to Protect Against Corporate Espionage

In general, security in private industry is not overseen by executives whose sole responsibility or area of expertise is security and who, therefore, are not experienced in spotting and assessing

security risks. Because they are not trained in security, these executives often do not fully understand the sophisticated and sometimes innocuous seeming means by which corporate espionage is accomplished and so do not know to guard against it and/or assign a low priority to it.

There are several generally acknowledged ways to protect against corporate espionage and provide what are considered “reasonable” precautions under the law (i.e., necessary to establish company information as a trade secret):

- Designate trade secret information as sensitive and proprietary—and keep it under lock and key, available on a “need to know basis” only
- Create a culture of security with formal corporate security policies that are implemented and enforced
- Provide employee awareness training of “social engineering ploys” and how to combat them
- Have a Floor Marshal Program in place so when employees think a person in the office or factory is out of place there is a procedure for them to follow
- Have a trash/refuse policy in place to combat dumpster diving
- Employ adequate physical security measures
- Conduct employee background checks
- Install the latest, most up-to-date security software
- Conduct assessments and security audits regularly, both physical and digital
- Hire security guards, if necessary

Prosecuting Intellectual Information and Trade Secret Violations

Patent, copyright, and trademark violations are regulated and controlled by federal law. Until the passage of the Economic Espionage Act of 1996, trade secret violations—when reported—were adjudicated in state civil courts, either under the Uniform Trade Secrets Act (adopted by most states) or state-specific statutory codes.

The Economic Espionage Act was passed in 1996, making it a federal crime to engage in economic espionage or steal a trade secret. The Act imposes a 10 year prison term and/or a maximum fine of \$250,000 on any person and \$5 million fine on any organization that knowingly steals or destroys any trade secret with intent to economically benefit anyone other than the owner of the trade secret. The act also allows the forfeiture to the U.S. government of proceeds or property derived from economic espionage and may require forfeiture of property used to commit economic espionage. The penalties increase to up to a 15-year prison term and/or a maximum \$500,000 fine on any person and a \$10 million fine on any organization that steals or destroys a trade secret of value with intent to benefit any foreign power.

During the September, 2000, Subcommittee on International Economic Policy and Trade hearing, and in the subsequent report entitled “Corporate and Industrial Espionage and Their Effects on American Competitiveness” one of the stated reasons for holding the hearing was to discuss ways to assess and strengthen the Economic Espionage Act of 1996. As of the date of the report (September 13, 2000) only 20 cases had been prosecuted under the Act. This scarcity of prosecutions was attributed, in part, to a lack of strong protection against disclosure of trade secrets during legal proceedings to prosecute corporate saboteurs. As a result, companies may not report corporate espionage or are not willing to engage with the Federal government for fear the company will lose control of the case and trade secrets will be revealed during court

proceedings. In addition, companies do not want their stockholders or the public to know there are security problems in the company.

Conclusion

As the threat of corporate espionage grows and the theft of trade secrets increases it becomes more and more clear that corporate security must be more than an afterthought. Companies must acknowledge this threat exists and take concrete, proactive steps to combat it. They must designate proprietary company information as a trade secret and protect it as such by instituting and enforcing strict, company-wide security procedures and policies.

ENDNOTES:

- ⁱ Deborah E. Bouchoux, *Protecting Your Company's Intellectual Property: A Practical Guide to Trademarks, Copyrights, Patents & Trade Secrets*, AMACOM (American Management Association), 2001
- ⁱⁱ Study sponsored by the American Society for Industrial Security (ASIS), Price Waterhouse Coopers, and the U.S. Chamber of Commerce
- ⁱⁱⁱ *Computer Security Issues & Trends*, Spring 2002, Volume VIII, No. 1, 2002; Computer Security Institute/FBI Computer Crime and Security Survey
- ^{iv} *Corporate and Industrial Espionage and Their Effects on American Competitiveness*, Subcommittee on International Economic Policy and Trade, September 13, 2000
- ^v Study sponsored by the American Society for Industrial Security (ASIS), Price Waterhouse Coopers, and the U.S. Chamber of Commerce
- ^{vi} C. Fitzgerald, *Spy Game*, Insight Magazine, April 2007
- ^{vii} *Corporate and Industrial Espionage and Their Effects on American Competitiveness*, Subcommittee on International Economic Policy and Trade, September 13, 2000
- ^{viii} D.W. Nicastro, *Cloak and Dagger in Corporate America*, Secure Source, Inc., 2005
- ^{ix} Edward Iwata, "More U.S. Trade Secrets Walk Out the Door with Foreign Spies," *USA Today*