SECURITY STUDY

Trends in Competitive Intelligence

BY RICHARD J. HEFFERNAN, CPP, AND DAN T. SWARTWOOD

THE PER MONTH INCIDENCE OF proprietary business information theft has risen a dramatic 260 percent since 1985, and foreign involvement is up nearly fourfold, according to a study conducted by the authors.

The study,* a nationwide sampling of 246 companies, was sponsored by the American Society for Industrial Security's (ASIS) Standing Committee on Safeguarding Proprietary Information (SPI). Customer lists were the most frequently reported target of proprietary information thieves, while pricing data was considered more financially damaging when stolen.

In all, the 246 companies reported 589 misappropriation attempts targeting U.S. technology, trade secrets, and business plans. The combined losses for 32 of the companies reporting exact figures are $1.8 billion. This study is the first objective data concerning the financial impact of technology theft on American business.

The survey looks not only at losses but also at preventive policies. It provides a comprehensive assessment of proprietary information practices and procedures in use in U.S. industry. It provides security professionals and senior company management with an understanding of the acquisition methods used in misappropriation attempts, which can assist in the evaluation of the adequacy of a company's present SPI program components.

Methodology. Using responses, comments, and requests from the participants in an earlier survey conducted in 1991, a format was designed to obtain precise information not only on the theft attempts but also on protection methods used and the financial impact of this technological drain on U.S. industry. In July 1992, surveys were mailed to 5,000 ASIS members. A total of 246 companies responded.

A double-blind methodology was used where the researchers knew neither the identity of the prospects nor the respondents. The survey data presented here has not been extrapolated. The seriousness of the problem and the impact on America's corporate resources documented by the survey speak for themselves.

THE SURVEY EXAMINED HOW COMPANIES are protecting themselves against misappropriation and theft of business and technical information. Questions were designed to reveal how many companies have a SPI program and what policies and program elements are in use as part of an overall protection of proprietary information program.

The survey's bottom line presents both good and bad news for the industry.

SPI programs. Overall, 76% of the 246 companies surveyed reported having a formal SPI program. Of the 15 smaller companies with annual sales of less than $1 million, only 33% had programs.

More encouraging were the figures from the other companies: Of the 28 companies with sales of $1 million to $10 million, 79% have SPI programs; of the 27 companies with $11 million to $50 million in sales, 70% have programs; of the 58 companies with $51 million to $500 million in sales, 78% have programs. And finally—the largest group of respondents—of the 118 companies with annual sales of more than $500 million a year, 82% have a formal SPI program.

Sixty-three of the companies have had programs in place for more than ten years, 46 companies have had programs in place for six to ten years, 59 companies have had programs in place for three to five years, and 32 companies have had programs in place less than two years.

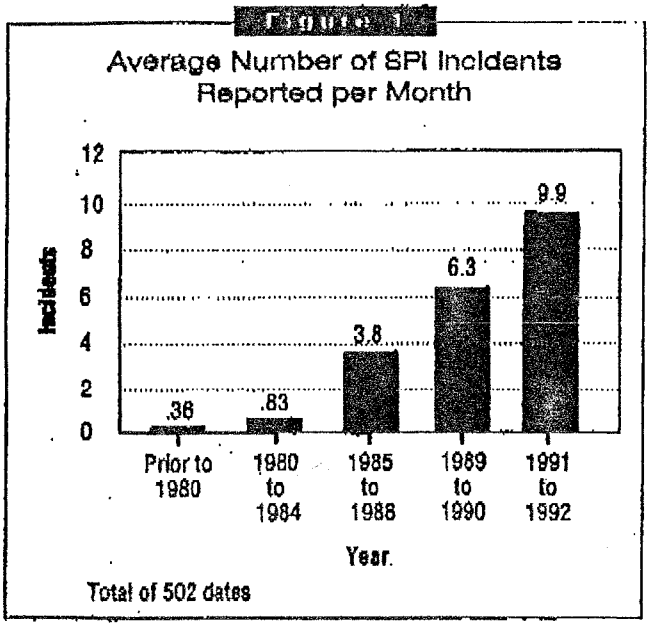
These programs are reviewed annually by 33% of the companies, biannually by 10%, as required by 46%, and not reviewed by 11%.

Procedures, policies, and costs. Two hundred companies have formal programs, and 46 companies have partial programs or individual policies. Access restrictions are used by 183 companies, nondisclosure agreements by 176, marking of documents and other material by 168, computer security measures by 161, copy restrictions by 103, exit briefings and interviews by 99, internal inspections by 113, external audits by 84, electronic eavesdropping countermeasures surveys by 50, secured or encrypted communications by 77, knowledge ability lists by 55, and other procedures by 29.

How are the companies' employees informed of SPI policies? According to the respondents, preemployment or initial employment training is used by 138 companies, employee handbooks by 131, refresher awareness training by 99, information security awareness posters by 63, films detailing awareness by 49, and 16 companies used other methods of keeping the information security awareness level up.

Most of the companies conducted self-evaluations of program effectiveness. Of the 246 responding companies,

Figure 1



56% evaluated their programs' effectiveness to be adequate. Another 25% evaluated their programs to be above average, and 7% thought their programs' effectiveness was outstanding. An additional 10% judged their programs ineffective, and 2% fell into the "other" category.

Management support for SPI programs is a critical issue. Adequate management support of the SPI program was reported by 29% of the respondents, followed by 26% who believe that support is above average. Moderate support of the program was indicated by 22% of the companies, outstanding management support enjoyed by 13%, and little support by 11%.

Companies were also asked to determine the cost of initiating their SPI programs. Approximately half (49%) of the 200 companies reporting formal programs had no record of costs involved in the start-up of their program; 33% indicated an expenditure of $1 thousand to $10 thousand; 12% spent $11 thousand to $50 thousand; 5% spent $51 thousand to $100 thousand; and 2% spent more than $100 thousand. (Due to rounding, these percentages add up to 101.)

These costs seem low when compared with recent known expenditures on program development including employee handbooks, newsletters, and films and may not indicate the salary costs of employees and materials funded from other internal sources.

The annual cost to administer a program is $1 thousand to $10 thousand a year for 78 of the companies responding, $11 thousand to $50 thousand for 16 of the companies, $51 thousand to $100 thousand for 11 companies, and more than $100 thousand for 5 of the companies. The remaining 90 companies do not track annual program expenditures.

Incidents. The number of companies reporting misappropriation attempts increased significantly from the 1991 survey results. Only 37% of the firms reported incidents in that survey. In the 1992 study, 49% of all responding companies reported incidents.

The 1992 assessment also indicated that, since 1985, the number of incidents reported on a monthly basis has increased 260 percent. The 246 companies that responded reported a combined average of 10 incidents per month.

THIS SIGNIFICANT INCREASE MAY BE ATtributed to several factors, including a higher awareness in the business community that the problem exists. This is partly because of the publicity of the first SPI committee survey and the media attention given such notable examples as the French intelligence penetration of IBM, Texas Instruments, and Corning in France.

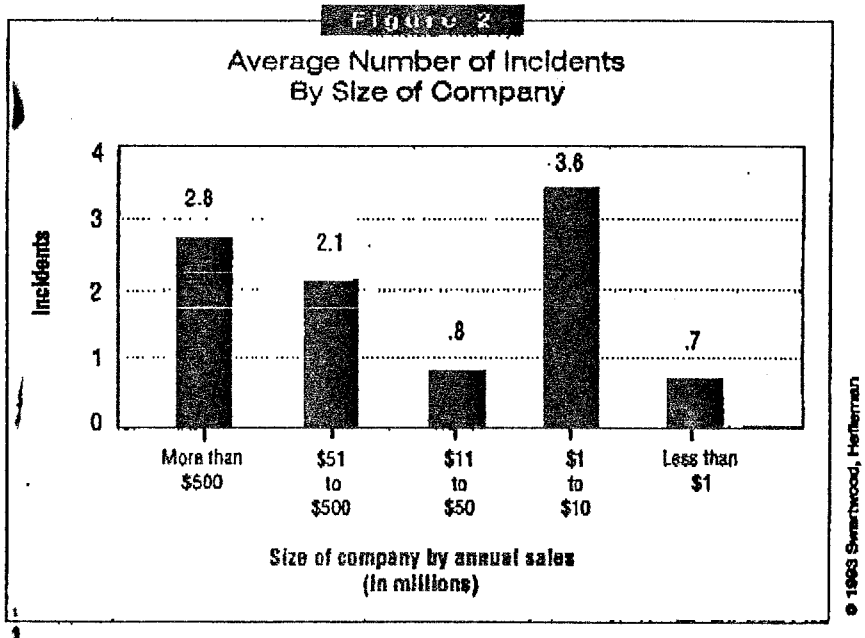
Another possible cause for the increase in incidents could be the poor economy. Many U.S. companies have recently been forced to lay off employees. An increased risk exists that these employees may attempt to hurt their employer before being laid off or enhance their future employment prospects by misappropriating proprietary information. This theory is supported by the current assessment reporting that 58% of all incidents were caused by current or former employees.

A third possible cause for the increase could be the increasing global nature of business. As U.S. firms increase their efforts to gain overseas market share, they more directly compete with foreign companies that operate with different ethics and ground rules. Some nations use all available government resources, including their intelligence services, to support their business communities.

Foreign involvement accounted for a significant portion of recent misappropriation attempts. About 30% of all incidents in 1991 and 1992 were reported to have foreign involvement. In comparison, from 1985 through 1988, foreign involvement was reported in only 21% of all incidents. This increase may seem small. However, if both trends of increasing incidents and increasing foreign involvement continue, the impact on U.S. competitiveness cannot be ignored.

In total, 21% of all incidents occurred overseas. Of greater signifi-

Figure 2



cance, however, is that 37% of all involved individuals identified in the study were foreign nationals. The Japanese tied with Europeans with 6% involvement in all incidents. The French were listed separately, but they accounted for only 4% of the total reported incidents.

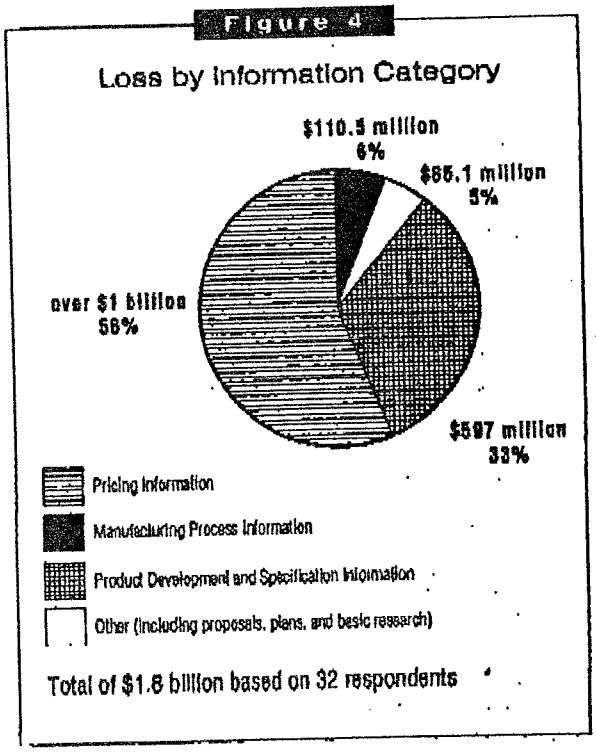
What types of proprietary information cause these losses? Companies reported that they lost slightly more than $1 billion due to the loss of pricing information. What is significant here is that pricing information was only the second most often stolen type of information (at 11%). Although customer lists were the most often stolen type of proprietary information, when pricing information was stolen it had the most financial impact.

The loss of product development and specification information (PDSI) caused the loss of $597 million. PDSI was tied with basic research information at 8% of all misappropriated information. And although manufacturing process information was tied for sixth place (at 6%), this data accounted for the third largest reported loss involving $110.5 million.

Methods. Understanding the methods used in these attempts can assist a company in designing or evaluating the sufficiency of its current SPI program. Of the 817 methods reported by the respondents, 33% involved the actual theft of information. However, break-ins accounted for only 12 of the 817 methods reported, while current or former unauthorized use and reproduction accounted for 43% of the methods reported. Once again, these methods would be used primarily by those who had authorized access but exceeded their responsibilities. Bribery was reported in less than 8% of all incidents.

The use of electronic surveillance and communication intercept in misappropriation incidents really needs to be addressed as a separate issue. The study only showed these methods used in approximately 8% of cases. However, this figure could be misleading and the real number is actually much larger.

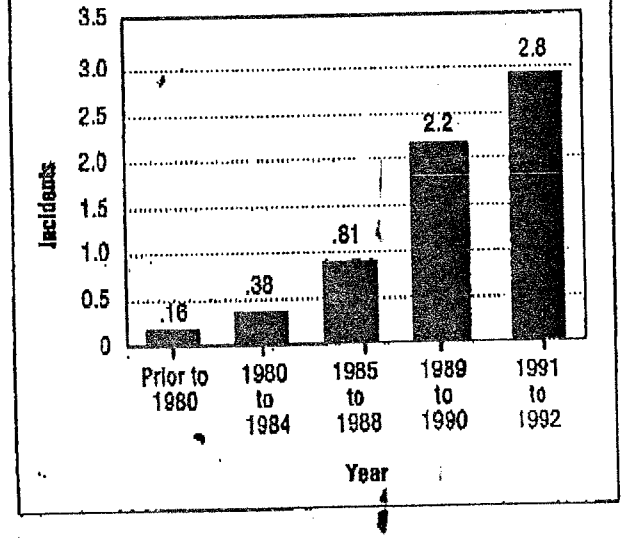
Figure 4



Communication intercept is extremely difficult to detect. For example, the only way a company may determine that it has been a victim is after the loss of a contract. What is difficult is tying the cause with the effect. This is usually attempted long after the intercept, when many potential causes might have contributed to the negative outcome.

Detecting electronic surveillance is also difficult. Technology and human behavior have given those with the access and time to implant such devices an edge over those tasked with detecting and neutralizing these illegal operations.

Figure 3



Impact on U.S. industry. Misappropriation attempts have had a significant impact on U.S. industry. In the 1992 assessment, 32 respondents that provided exact figures indicated that their companies had lost a combined $1.8 billion due to the incidents against their companies. Only 17 said there was no resource impact on the company.

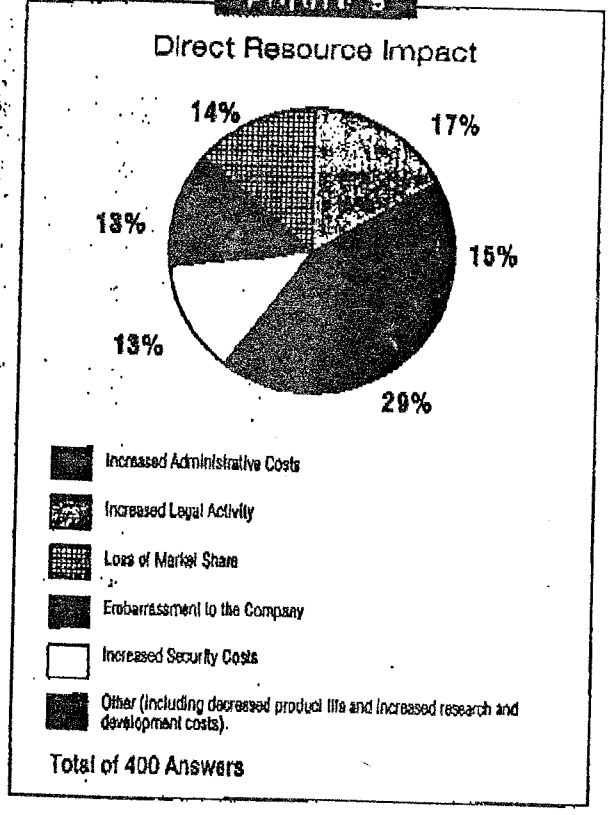
Averaging the reported losses of the rest of the respondents indicated that large firms (with annual revenues of more than $500 million) lost an average of $7.45 million and mid-size companies ($51 million to $500 million) lost more than twice as much—an average of $15.5 million—because of actions against their operations.

The frequency of incidents is also significant. The average firm with annual sales of more than $500 million has become aware of approximately three incidents involving proprietary data. Mid-size firms with sales of $51 million to $500 million have been involved in approximately two incidents. The largest reported number of incidents involved small companies with $1 million to $10 million in sales, with slightly more than 3.5 incidents reported per company.

THE ADDITIONAL COMMENTS WRITTEN ON the surveys concerning knowledge of incidents were enlightening. The remarks revealed a possible flaw in the survey. Respondents were given the opportunity to answer yes or no about the existence of misappropriation incidents in their companies.

More than 40 respondents indicated that their firms had no mechanism to discover if their proprietary data was

Figure 5



being taken. That suggests that several of the firms indicating no incidents may have experienced losses without being able to detect such attempts. It might also indicate that several of those reporting incidents became aware of them by chance.

What was as significant as reported losses was the large numbers of companies unable to quantify their losses due to misappropriation attempts. More than 50% of firms reporting loss of information indicated problems in assessing loss. Their companies either had not assessed the actual or potential damage caused by these actions or, more significantly, had no mechanism to assess the damage caused. Without a credible process of evaluating incidents and their impact, companies predispose themselves to continue to suffer similar incidents and the consequent effects when proprietary information is in the wrong hands.

Other important resource impacts on U.S. companies, in addition to the reported dollar losses, were apparent. The major responses included increased administrative costs (15%), increased legal activities (17%), loss of market share (14%), increased security costs (13%), and embarrassment to the company (13%).

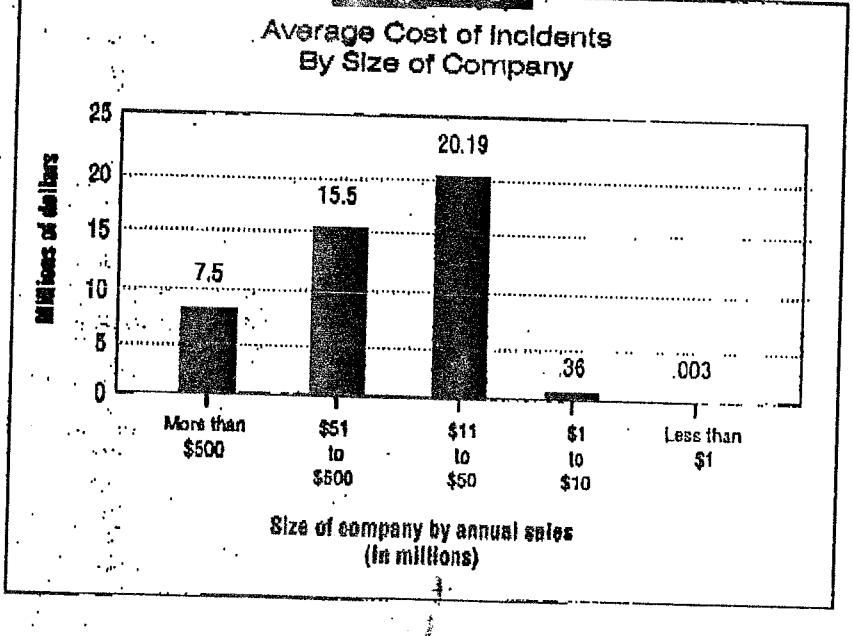
The survey's bottom line presents both good and bad news. The bad news is that the problem is growing and becoming more global. The good news is that the survey gives companies concerned about their security an objective means to benchmark their efforts. The assessment adds a needed level of credibility to the war stories and anecdotal evidence gathered from fellow security professionals.

Understanding the threat is another essential aspect of creating an effective SPI program. The FBI and other government agencies are beginning to address these issues to both government and private industry.

The problems that the assessment highlights are not insolvable. Solutions are available, and if implemented with imagination and resolve, a company can mitigate the ability of others to benefit from illegal activities. This survey and similar efforts will add to the growing body of literature on the nature of the threat to corporate secrets. ■

Richard J. Heffernan, CPP, is president of R. J. Heffernan and Associates, Inc., in Branford, Connecticut, and chairman of the ASIS Standing Committee on Safeguarding Proprietary Information. He has been involved in information and communications security consulting for more than 25 years. Dan T. Swartwood, OCP (Operations Security Certified Professional), is managing director of Strategic Corporate Safeguarding, Inc., in Washington, D.C., and a member of the safeguarding proprietary information committee.

Figure 6



The authors wish to thank those ASIS members who participated in the survey; the credit for its success belongs to them.

* The survey was coauthored by ASIS Standing Committee on Safeguarding Proprietary Information Chairman Richard J. Heffernan, CPP, and Committee Member Dan T. Swartwood. In March 1991, ASIS was contacted by the U.S. General Accounting Office on behalf of the Congressional House Judiciary Committee to help provide Congress with information on competitive intelligence activity directed at U.S. technological and business information, especially from overseas. Heffernan met with these officials and subsequently developed a survey to help ascertain the extent of the problem.

ASIS members were surveyed in April 1991, and the results were compiled and delivered in August 1991 (see *Security Management*, October 1991). The results raised further questions from both government and industry officials, resulting in the current study.