ASIS INTERNATIONAL
Advancing Security Worldwide™

Trends in Proprietary Information Loss

Survey Report
September 2002

PricewaterhouseCoopers

ASIS FOUNDATION™

Sponsored by PricewaterhouseCoopers, U.S. Chamber of Commerce & ASIS Foundation

PRICEWATERHOUSECOOPERS

The PricewaterhouseCoopers Cybercrime Prevention and Response (CPR) group assists organizations in the prevention, detection, response, and remediation of computer crimes and other security-related incidents including the costliest of computer-based crimes—theft of proprietary information. The PricewaterhouseCoopers CPR practice sponsored this survey with ASIS International and the U.S. Chamber of Commerce to facilitate a better understanding of the losses actually incurred and the preventive best practices that organizations are following related to theft of proprietary information. To further assist organizations around the world in addressing computer-based crimes, the CPR practice maintains computer forensic lab centers in the United States, Europe, and Asia Pacific. These labs are used to analyze security breaches and support technical investigations. The CPR practice is an integral part of PricewaterhouseCoopers' global security and privacy practice, one of the largest technology security practices in the world. The practice provides cybercrime emergency response and works closely with the PricewaterhouseCoopers Dispute Analysis and Investigations practice to provide litigation and investigative support, resulting in unmatched technical and legal resources available to clients around the world. To contact the CPR practice, call Andrew Toner, partner, at 646–471–8018. Additional information is located at the PricewaterhouseCoopers Security and Privacy website at *www.pwcglobal.com/security*.

The U.S. Chamber of Commerce is the world's largest business federation, representing over three million businesses, 3000 state and local chambers of commerce, 900 business associations, and 90 American Chambers in countries around the world. The U.S. Chamber was founded in 1912 and is headquartered directly in front of the White House in Washington, DC. The U.S. Chamber's primary mission is to advocate for the interests of business and free enterprise, and to work with its members, government agencies, the media, and other organizations to accomplish these goals. The U.S. Chamber has been extremely active in supporting efforts to promote economic security and critical infrastructure protection. Its Economic Security Working Group provides policy briefings and updates on issues ranging from economic espionage to security information sharing efforts. The U.S. Chamber is a founding member of the Partnership for Critical Infrastructure Security and serves as the private sector administrator for the PCIS. The U.S. Chamber also supports the National Cyber Security Alliance and its Internet security education effort on *www.staysafeonline.info*. For more information on the U.S. Chamber's economic security programs, please call (202) 463-5517 or visit *www.uschamber.com/ccc*.

ASIS INTERNATIONAL
Advancing Security Worldwide™

Trends in Proprietary Information Loss

Survey Report
September 2002

PRICEWATERHOUSECOOPERS

THE SPIRIT OF ENTERPRISE · U.S. CHAMBER OF COMMERCE

ASIS FOUNDATION™

Sponsored by PricewaterhouseCoopers, U.S. Chamber of Commerce & ASIS Foundation

Trends in Proprietary Information Loss

Survey Report
September 2002

Table of Contents

Executive Summary

The following findings are from a study conducted among the *Fortune 1,000* list of corporations and 600 small and mid-sized companies belonging to the U.S. Chamber of Commerce. A total of 138 companies responded, reporting information for the period July 1, 2000 to June 30, 2001.

FREQUENCY AND MAGNITUDE

- In 2001, the companies represented by study respondents are likely to have experienced proprietary information[1] and intellectual property (IP) losses of between $53 and $59 billion.
- Of the companies participating in this survey, 40% reported incidents of known or suspected losses of proprietary information in the reporting period.
- On average, companies reporting incidents of proprietary information or intellectual property loss experienced two such incidents in the reporting period.
- The largest average dollar value of loss per incident occurred in research and development ($404,000), followed by financial data ($356,000).

Findings suggest losses of proprietary information and intellectual property in the range of $53 to $59 billion.

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 tech-

1 For purposes of this survey, the definition of proprietary information is limited to that information which is not within the public domain and which the owner has taken some measures to protect. While commonly referred to as "trade secrets," this information is typically protected under both State and Federal Law.

nology 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.

POLICIES AND ATTITUDES

- Although most respondents (about three-fourths) indicated that information associated with new products and services was vital to the company's success, only 55% said that management was concerned about information loss and was taking necessary precautions.

- Based on a ranking of best practices by respondents, it appears that proper labeling and handling of classified information is not the norm among companies, although high-tech companies are more likely to correctly mark intellectual property to protect it and large companies (over $15 billion) are most likely to correctly destroy sensitive information when it is no longer needed.

- The ranking of best practices also suggests that employees are not typically trained to safeguard proprietary information in the office or when on travel.

- Although most companies indicated that the Internet represents a new threat, most do not require that information sent over the Internet be encrypted.

- Many responding companies do attempt to reduce the risk of proprietary information and intellectual property loss by employing "need to know" policies; using screen savers and/or server passwords; and maintaining nondisclosure agreements.

- Attitudes about intellectual property loss and "best practice" strategies varied among companies that had and had not experienced incidents of loss. Information security was given a lower priority at companies where loss incidents occurred. Companies that made IP protection a higher priority were also those that indicated no loss incidents.

- Many companies, especially in the service sector, do not assign a value to their intellectual property until they are in litigation.

Section 1

Introduction and Overview

Information loss continues to be a serious threat to American business. Every indication is that corporations face increasing risk of theft, loss, misappropriation, or destruction of their intellectual property. Finding the most effective safeguards to protect these critical assets must become a priority for public policymakers, as well as corporation executives. However, beyond anecdotal press reports, there is little impartial information available to guide national policy and enhance and promote organizational response of individual businesses.

The objectives of the *10th Trends in Proprietary Information Loss Survey* are to collect data about the current state of proprietary information loss; to determine the types of practices used by corporations to safeguard their intellectual property assets; and to provide an advocacy role to the corporate community, enhancing awareness of the problem and its extent. As a result of this effort, we hope to provide business executives with data that they can consider in establishing priorities within their companies.

In the aftermath of September 11, many U.S. companies have reconsidered the status, focus, and effectiveness of their overall security programs. However, in the rush to update and enhance physical security and business continuity planning to address obvious implications of the terrorist threats, some companies may be overlooking the critical importance of sustaining their efforts to safeguard sensitive proprietary information. At a time when businesses in every sector of the economy are struggling with profitability issues, the sources of competitive advantage—new products and services, and innovative ways of producing products—often are based on proprietary information. Given the essential role of proprietary information in strengthening the U.S. economy, protecting it should be a vital component of the global war on terrorism, as well as an everyday concern to corporate executives and their shareholders.

Although 70 percent or more of the market value of a typical U.S. company may derive from its intellectual property (IP) assets, formalized valuation procedures exist in too few companies to assure that managements have a complete appreciation of the extent and importance of these resources. In far too many organizations, these assets are not tracked in corporate accounting systems. Since the value of IP assets is not well established, they often are not well protected, thereby contributing to the current problems associated with theft of trade secrets and sensitive proprietary information.

Proprietary information assets are critical to the success of many, perhaps most businesses. The importance of this property, while too often not yet "formally valued" by many companies, cannot be underestimated. In today's highly competitive global marketplace, it is essential for American managers to recognize that the intellectual assets of business are highly sought-after commodities.

This survey is the latest in a continuing series conducted by ASIS International through the auspices of its Council on Safeguarding Proprietary Information. The effort has been greatly enhanced this year through the sponsorship of PricewaterhouseCoopers, the U.S. Chamber of Commerce, and the ASIS Foundation.

Section 2

Survey Methodology

A multifaceted research methodology was used to complete this *10th Survey of Trends in Proprietary Information Loss*.

- **Survey Questionnaire:** Members of the ASIS Council on Safeguarding Proprietary Information, chaired by William C. Boni, Jr., CPP, developed the survey questionnaire. Dr. Philip G. Kuehl of Westat, the ASIS Foundation's research consultant, reviewed the questionnaire to assure its conformity to accepted survey research standards. The content of the questionnaire was based on questions used in the 1998 *Trends in Proprietary Information Loss Survey* conducted by ASIS and PricewaterhouseCoopers LLP. It also included new subject areas introduced by the Council. The timeframe used in this survey for the reporting of known or suspected losses of proprietary information and intellectual property was July 1, 2000 to June 30, 2001.

- **Survey Sample and Respondents:** The Chief Executive Officers (CEOs) of the *Fortune 1000* companies and of 600 mid- and small-sized U.S. Chamber of Commerce members made up the sample of respondents used in this survey. The CEOs were designated to act as the primary respondent for their company though it was expected that they would seek input from key security and security-oriented professionals, such as security executives, legal counsel, and information technology managers. It should be noted that directors and other key security management personnel in these same companies were contacted so that they were aware of the study effort.

- **Data Collection:** In early October 2001, an initial mailing of the survey questionnaire to the respondent CEOs occurred. A second mailing of the survey questionnaire was sent to respondent company security directors and other key security management personnel in late October 2001. These two mailings produced 69 responding companies for the survey database. Follow-up telephone calls subsequently were made to potential respondents in November 2001. This process resulted in another 69 completed interviews so that a total of 138 responding companies are in the survey database (resulting in an overall 9% response rate). In the 1998 study of proprietary information loss, a total of 97 companies provided data. The 1998 study response rate was also 9%.

- **Data Preparation:** Data from all responding companies was received, coded, and tabulated by Dr. Kuehl and other Westat staff. ASIS maintains a list of all companies who were selected to participate in the survey. In order to protect the confidentiality of the data, the names of the 138 responding companies are not known by ASIS nor Westat.

- **Report Preparation:** William C, Boni, Jr., CPP, Chairman, and Dan Swartwood of the ASIS Council on Safeguarding Proprietary Information used the Westat data to draft the report with the assistance of Dr. Kuehl. This draft was subsequently reviewed by all Council members and staff from the U.S. Chamber of Commerce and PricewaterhouseCoopers LLP.

- **Underreporting Bias:** Gathering reliable statistics about proprietary information loss is difficult for several reasons. Many companies prefer not to report this information or have specific nondisclosure policies for their proprietary and intellectual property loss data. At companies where information can be shared, survey respondents sometimes did not have access to comprehensive loss data in their companies because it was not compiled in a centralized database. In addition, this time the risk of underreporting was greater because the horrific events of the "9-11" tragedy and related security concerns in potential respondent companies dampened interest and cooperation levels for obvious reasons. As a result of these factors, it is likely that many incidents of loss in responding companies were not reported; and relatively few of the reported incidents could be valued in dollar terms.

- **Extrapolation of the Study Data:** As a result of the preceding factors, the reader should recognize that the extrapolation of these findings is dependent on assumptions made about underreporting bias in the forecasting model. Irrespective of the statistical model used to extrapolate the results, study data provide a good indication of the types of proprietary losses and issues affecting large companies in the U.S. Further, the data provides insights into the way that companies manage systems and processes associated with the loss of proprietary information.

- **Profile of Responding Companies:** Findings given in Tables 2.1 and 2.2 present the profile characteristics of the 138 responding companies in this survey. These are the baseline of companies that provided all of the data included in the Summary Findings.

    - As shown in Table 2.1, a large proportion of responding companies are in the: (1) services and (2) manufacturing industry groups, and have fiscal year revenues of less than $5 billion.

    - As shown in Table 2.2, the overwhelming proportion of responding companies' workforces are comprised of full- and part-time employees who work in the United States.

Table 2.1 Profile of Respondents by Industry Group and Fiscal Year Revenues

Industry Group and Fiscal Year Revenues	Percent[1]
Respondents by Industry Group	
• Services	39
• Manufacturing	38
• Financial	12
• High Technology	11
Respondents by Fiscal Year Revenues	
• Less than or equal to $5 BL	57
• $6 BL to $15 BL	23
• Over $15 BL	14
• Not stated	6

1 Percents are based on 138 responding companies.

Table 2.2 Profile of Respondents' Total Workforce by Employment Status and Location

Workforce Profile	Percent[1]
Employment Status of Workforce	
• Full- and part-time employees	90
• On-site contractors/temporary employees	7
• Outsourced/employees of third parties	3
Location of Workforce	
• United States	86
• Canada and Mexico	4
• International (not including the United States, Canada, or Mexico)	10

1 Percents are based on 138 responding companies.

Section 3

Summary Findings

All major findings are summarized in this section through the presentation of detailed data tables and related commentary. Summary Findings are organized for the presentation of statistical tables and related discussion points in the following way:

In many of the tables, data are given for responding companies in these subsamples: (1) all responding companies; (2) industry group (including services, manufacturing, high technology, and financial); (3) fiscal year revenues (including $5 billion or less, $6 billion to $15 billion, and over $15 billion); (4) companies reporting loss incidents; and (5) companies not reporting loss incidents. In several tables, only aggregate or combined data are presented due to the number of respondents. The footnotes accompanying many of the data tables are an integral part of this report.

3.1 Risk Factors Associated with Proprietary Information and Intellectual Property Loss

Findings given in Table 3.1 summarize the risk order results for the importance of risk factors associated with proprietary and intellectual property loss. As a guide to the interpretation of these data, the reader should note the following observations:

- Based upon the detailed rating data used to report these rank order results, four major risk factors were identified by most reporting companies: (1) former employees; (2) foreign competitors; (3) on-site contractors; and (4) domestic competitors. These four items dominate and encompass the overall views of most responding companies.

Former employees and foreign competitors pose the greatest potential threats to corporate information.

- A degree of variation exists when these rank order results are assessed by industry group, fiscal year revenues, and loss experience. These subsample results show that other risk factors emerge as important for some reporting companies: (1) computer hackers (for service and financial industry group companies, companies with revenues over $15 billion, and companies not reporting loss incidents); (2) vendors and suppliers (for service group companies and companies with sales between $6 billion and $15 billion); (3) current employees (for manufacturing group companies and companies reporting loss incidents); and (3) intelligence services (for high technology group companies).

In summary, four major risk factors—former employees, foreign competitors, on-site contractors, and domestic competitors—are major risk factors associated with the loss of proprietary information and intellectual property. Several other factors—computer hackers, vendors/suppliers, current employees, and intelligence services—pose a significant risk factor on a secondary or selected basis within subsample segments.

Table 3.1 Risk Factors Associated With Proprietary Information and Intellectual Property Loss by Industry Group and Revenues

Risk Factor	All Responding Companies	Rank Order Results[1]								
		Industry Group				Fiscal Year Revenues				
		Services	Manufacturing	High Technology	Financial	$5 BL or Less	$6 BL–$15 BL	Over $15 BL	Companies Reporting Loss Incidents	Companies Not Reporting Loss Incidents
Former Employees	1	1	5	2	1	1	6	1	2	2
Foreign Competitors	2	7	1	1	3	3	1	2	6	1
On-site Contractors	3	4	2	3	4	2	3	6	1	5
Domestic Competitors	4	5	3	5	5	4	4	3	4	3
Computer Hackers	5	2	8	7	2	5	5	4	7	4
Vendors/Suppliers	6	3	9	6	7	8	2	5	5	6
Current Employees	7	6	4	10	9	6	7	8	3	9
Strategic Partners	8	9	6	8	6	7	8	9	8	7
Intelligence Services	9	8	10	4	8	9	9	7	9	8
OEMs/Outsource Manufacturers	10	11	7	11	10	10	10	10	10	10
Media	11	10	11	9	11	11	11	11	11	11

1 Results are based on 138 responding companies.

3.2 Known or Suspected Losses of Proprietary Information

Findings given in Table 3.2 summarize known or suspected losses of proprietary information reported by responding companies. As a guide to the interpretation of these data, the reader should note the following observations:

- In total, 40% of all responding companies reported known or suspected proprietary information loss. The highest reported incidence rates occurred in the service industry group and in companies with revenues in excess of $6 billion in fiscal year revenues. The lowest reported rates occurred among companies in the financial industry group. It is likely that these and other study data reflect a significant degree of underreporting by responding companies.

- Given the composition of the study sample, it is not surprising that most reported known or suspected losses occurred in North America (including the United States, Canada, and Mexico). This geographic factor is most dominant among reporting companies in the financial and service industry groups; and those companies with $5 billion or less in fiscal year revenues. At the other extreme, companies in the high technology industry group reported some suspected or known incidents in many different geographic regions.

- The largest number of known or suspected losses of proprietary information occurred among companies in the service and manufacturing industry groups; and those with revenues of $5 billion or less. This pattern of results influences the types of analyses of results given in Tables 3.3, 3.4, and 3.5.

40% of responding companies reported suspected or known losses of proprietary information.

In summary, 40% of the companies participating in this study reported known or suspected losses of proprietary information in the period from July 1, 2000 to June 30, 2001.

3.3 Losses of Proprietary Information and Intellectual Property

Findings given in Table 3.3 summarize losses of proprietary information and intellectual property given by responding companies. As a guide to the interpretation of these data, the reader should note the following observations:

- A total of 55 responding companies in the study reported losses of proprietary information and intellectual property as shown in both Tables 3.2 and 3.3. Of the 105 total loss incidents reported by these companies, only 24 incidents (or about 23%) were valued by responding companies.

Table 3.2 Summary of Known or Suspected Losses of Proprietary Information by Region, Industry Group, and Revenues

Summary of Known or Suspected Losses	Percents							
		Industry Groups				Fiscal Year Revenues		
	All Responding Companies	Services	Manufacturing	High Technology	Financial	$5 BL or Less	$6 BL–$15 BL	Over $15 BL
Responding Companies Report Known or Suspected Losses[1]								
• Yes	40	44	38	40	29	26	47	58
• No	60	56	62	60	71	74	53	42
IF YES: Proportion of Known or Suspected Losses Reported by Region[2]								
• North America (U.S., Canada, Mexico)	65	88	53	27	100	78	59	44
• Asia Pacific (PRC, India, Japan, Australia)	13	9	17	18	*	10	23	11
• Central/South America	10	3	14	*	*	10	4	22
• Europe (including Russia and CIS)	9	*	11	27	*	1	14	17
• Africa/Middle East (including Turkey)	3	*	5	18	*	1	*	6
IF YES: Proportion of Known or Suspected Losses by Industry Group and Revenues[2]	—	44	36	11	9	56	26	18

1 Results are based on 138 responding companies.
2 Percents are based on 55 responding companies that reported known or suspected losses of proprietary information.
* Insufficient cell size to calculate findings.

- It was possible to calculate an average dollar loss per incident for only those responding companies in the manufacturing industry group ($306,427) and for companies with fiscal year revenues equal to or less than $5 billion ($332,618).

As highlighted in the Methodology, it appears that significant levels of proprietary information and intellectual property loss underreporting characterize results obtained in this study since many responding companies were unable or unwilling to: (1) disclose whether they had experienced loss incidents; or (2) value losses they had incurred. Using a set of realistic assumptions about the comparability of companies that were and were not able to report and value incidents of loss, it is likely that companies represented by this study experienced losses of proprietary information and intellectual property in the $53 to $59 billion range during the reporting year which ended June 30, 2001. On an industry group and annual revenue basis, it would appear that average dollar losses per incident are in excess of $300,000 for manufacturing companies and for companies with revenues of $5 billion or less.

Average dollar loss per incident exceeds $300,000 for responding manufacturing companies and companies with revenues of $5 billion or less.

Hence, the reader should treat data generated in this study as suggestive—but not conclusive—of proprietary information and intellectual property loss in major U.S. corporations.

Table 3.3 Summary of Losses of Proprietary and Intellectual Property by Industry Group and Revenues

Sample Categories	Average Dollar Losses[1]	Number of Responding Companies[2]	Number of Companies Reporting Losses[3]	Percent of Companies Reporting Losses[4]	Number of Losses Reported[5]	Number of Losses Valued[6]	Percent of Losses Valued[7]
Industry Group							
• Services	*	54	24	44	25	8	32
• Manufacturing	$306,427	52	20	38	50	14	28
• High Technology	*	15	6	40	9	0	0
• Financial	*	17	5	29	13	2	15
Revenues							
• $5 BL or Less	$332,618	79	21	26	40	16	40
• $6 to $15 BL	*	32	15	47	17	5	29
• Over $15 BL	*	19	11	58	23	1	4
• Not Stated	*	8	*	*	*	*	*

1 Average Dollar Loss is loss per valued incident.
2 Results are based on 138 responding companies.
3 Number of Companies Reporting Loss (N=55) is based on Table 3.2 data.
4 Percent of Companies Reporting Loss is proportion of companies reporting loss.
5 Number of Losses Reported are incidents where companies with losses reported incidents.
6 Number of Losses Valued are incidents where companies with losses provided loss data.
7 Percent of Losses Valued is proportion of valued losses divided by number of reported incidents.
* Insufficient cell size to calculate findings.

3.4 Average Dollar Value of Loss

Findings given in Table 3.4 summarize the average dollar value of reported loss by area of risk. As a guide to the interpretation of these data, the reader should note the following observations:

Highest dollar losses per incident occur in research & development and financial data, which together account for 81% of total average dollar loss per incident identified.

- On an aggregate basis, the greatest average dollar value of loss per incident occurs in (1) research and development ($404,375) and (2) financial data ($356,035). These two areas of proprietary information and intellectual property loss account for 81% of the total average dollar loss per incident identified in this study.
- On an aggregate basis, two other areas of risk—second party information ($164,706) and customer lists and related data ($117,000)—account for another 16% of the total average dollar losses identified in this study.
- A variety of other risk areas—prototypes, strategic plans and roadmaps, manufacturing data, merger/acquisition, and unannounced product specifications—combine for low average dollar loss per incident ($20,342); and account for only 3% of the total average dollar losses identified in this study.
- Average dollar losses by area of risk cannot be calculated by company industry group or fiscal year revenues due to underreporting described in the Study Methodology.

In summary, two areas of risk—(1) research and development, and (2) financial data—dominate the areas of risk associated with the loss of proprietary information and intellectual property as measured on a per incidence basis. Second party information and customers' lists and related data pose a secondary level of risk for the loss of proprietary information and intellectual capital.

Table 3.4 Average Dollar Value and Percent of Dollar Loss by Areas of Risk

Areas of Risk	Average Dollar Value Loss per Incident[1]	Percent of Dollar Value Loss by Area
Research and Development	$404,375	43
Financial Data	356,035	38
Second Party Information	164,706	11
Customer Lists and Related Data	117,000	5
Other Sources	20,342	3
• Prototypes	*	*
• Strategic Plans and Roadmaps	*	*
• Manufacturing Data	*	*
• Merger/Acquisition	*	*
• Unannounced Product Specifications	*	*

1 Results are based on 55 responding companies that reported losses in Table 3.2.
* Insufficient cell size to calculate findings.

3.5 Reported Incidents of Proprietary Information Loss by Areas of Risk

Findings given in Table 3.5 summarize the percent of reported incidents of loss by areas of risk. As a guide to the interpretation of these data, the reader should note the following observations:

- On an aggregate basis, most responding companies reporting loss incidents had incidents in four areas: (1) research and development; (2) customer lists and related data; (3) financial data; and (4) strategic plans and roadmaps. (There was insufficient data to calculate percent and loss incident data by company industry group or fiscal year revenues.)

- Also on an aggregate basis, about two-thirds of total reported loss incidents occur in the same four areas of risk but in a slightly different rank order: (1) customer lists and related data; (2) strategic plans and roadmaps; (3) financial data; and (4) research and development.

- On average, companies reporting losses experienced about 1.9 incidents of loss.

On average, companies reporting losses experienced about two losses for the year.

In summary, areas of risk for most companies experiencing proprietary information loss incidents, as well as most such loss incidents, occur in four areas: (1) customer lists and related data; (2) strategic plans and roadmaps; (3) financial data; and (4) research and development. On average, companies with reported incidents experienced almost two such incidents in the reporting period.

Table 3.5 Reported Incidents of Proprietary Information Loss by Areas of Risk

Areas of Risk	Percent[1] Companies Reporting Loss Incidents	Total Reported Incidents[2]
Customer Lists and Related Data	36	19
Strategic Plans and Roadmaps	25	18
Financial Data	27	16
Research and Development	49	13
Merger/Acquisition	16	11
Manufacturing Data	16	9
Unannounced Product Specifications	11	7
Prototypes	15	6
Second Party Information	4	6

1 Percent is based on 55 responding companies that reported losses in Table 3.1. These companies can experience loss incidents in more than one area of risk.
2 Number of reported incidents shows incidents reported by companies that experienced a loss in this area of risk. The total number of incidents reported in this survey is 105 based on data from 55 responding companies who reported losses in Table 3.2. As a result, companies reporting proprietary information loss incidents identified an average of 1.9 incidents in the reporting period.

3.6 Problems Caused by Loss of Proprietary Information by Industry Group and Revenues

The most important problems associated with loss of proprietary information are increased legal costs and loss of revenue.

Findings given in Table 3.6 summarize the rank order results for the importance of problems caused by the loss of a company's proprietary information. As a guide to the interpretation of these data, the reader should note the following observations:

- Based upon the detailed rating data used to report these rank order results: (1) increased legal costs and (2) loss of revenue are regarded by responding companies to be the most important problems caused by the loss of proprietary information. However, these overall results vary among companies in the high technology and financial industry groups, and among the largest responding companies.

- Two problem areas—(1) loss of competitive advantage and (2) loss of market share—are viewed to be of mid-range importance based on ratings given by most responding companies. However, loss of competitive advantage is regarded by high technology and large companies to be an important problem caused by the loss of proprietary information.

- The last three problems in the overall rank order results—(1) embarrassment, (2) increased R&D costs, and (3) increased insurance costs—were rated to be relatively unimportant by most responding companies. A notable exception to these overall findings occurred when embarrassment was rated by companies in the financial industry group to be of highest importance.

In summary, impacts of proprietary information loss are found in (1) increased legal costs and (2) loss of revenues. Depending upon industry group or company size, companies also can experience (1) loss of competitive advantage or (2) embarrassment.

3.7 Valuation of Intellectual Property

Findings given in Table 3.7 summarize rank order results associated with how responding companies establish a valuation for their intellectual property. As a guide to the interpretation of these data, the reader should note the following observations:

- Based upon the detailed rating data used to report these rank order results, the assessment or assignment of value for intellectual property usually stems from three sources: (1) litigation, (2) transactions, and (3) licensing negotiations. These three items dominate and encompass the views of virtually all responding companies and only marginal differences exist in the detailed rating scores for these three assessment sources.

Table 3.6 Problems Caused by Loss of Proprietary Information by Industry Group and Revenues

Problems	All Responding Companies	Rank Order Results[1]								
		Industry Group				Fiscal Year Revenues				
		Services	Manufacturing	High Technology	Financial	$5 BL or Less	$6 BL–$15 BL	Over $15 BL	Companies Reporting Loss Incidents	Companies Not Reporting Loss Incidents
Increased Legal Costs	1	1	1	5	2	1	1	2	1	2
Loss of Revenue	2	2	2	1	3	2	2	3	2	1
Loss of Competitive Advantage	3	4	3	2	4	4	5	1	3	5
Loss of Market Share	4	3	4	3	5	3	3	4	4	3
Embarrassment	5	5	7	6	1	5	6	5	6	6
Increased R&D Costs	6	7	5	4	7	7	4	6	5	7
Increased Insurance Costs	7	6	6	7	6	6	7	7	7	4

1 Results are based on 138 responding companies.

The most important factor considered when valuing intellectual property is competitive advantage.

- By a highly significant margin in the detailed rating scores, the persons responsible for valuing intellectual property in most companies are in-house patent counsel and/or legal department professionals. These persons play pivotal roles in valuing intellectual property in the vast majority of responding member companies. To a lesser extent, the (1) business department using the intellectual property or (2) a company's Chief Financial Officer (CFO) play a role in valuing intellectual property.

- By a highly significant margin in the detailed rating scores, competitive advantage is the single most important or dominant factor considered when valuing intellectual property. Among all responding companies, two other factors—(1) incremental profitability of intellectual property and (2) R&D costs—are viewed to be next in importance when intellectual property is valued. This differs among companies in the high technology and financial industry groups, which view licensing royalties and age of the intellectual property, respectively, to be the second most important factor when valuing intellectual property. The most important factor considered when valuing intellectual property is competitive advantage. Incremental profitability of intellectual property was rated the second most important factor by responding companies in the $5 billion or less and over $15 billion fiscal year revenue categories.

Table 3.7 Valuation of Intellectual Property by Industry Group and Revenues

Valuation of Intellectual Property	Rank Order Results[1]							
	All Mail Survey Responding Companies	Industry Groups				Fiscal Year Revenues		
		Services	Manufacturing	High Technology	Financial	$5 BL or Less	$6 BL–$15 BL	Over $15 BL
Timing of Assignment of Value for Intellectual Property								
• Result of Litigation	1	1	3	2	2	2	1	1
• Due to Transaction	2	3	2	3	1	3	2	2
• During Licensing Negotiations	3	3	4	1	4	4	3	4
• Upon Development/Creation	4	2	1	4	3	1	4	3
• Other	5	4	5	5	5	5	5	5
Persons Responsible for Valuing IP								
• In-house Patent Council/ Legal Department	1	1	1	1	1	1	1	1
• Business Department Using IP	2	3	2	2	3	2	3	2
• CFO	3	2	3	5	2	3	2	3
• CEO	4	4	4	4	4	4	4	6
• Outside Experts	5	6	5	3	6	5	5	4
• Other	6	5	6	6	5	6	6	5
Factors Considered When Valuing IP								
• Competitive Advantage	1	1	1	1	1	1	1	1
• Incremental Profitability of IP	2	2	3	5	3	2	4	2
• R&D Costs	3	3	2	4	6	3	2	4
• Royalties to be Earned From Licensing	4	4	4	2	7	4	3	5
• Age of IP	5	5	5	6	2	6	6	3
• Other License Agreements	6	6	6	3	5	5	5	6
• Design Ability	7	8	7	8	8	8	7	7
• Convoyed Sales	8	7	8	9	4	7	8	8
• Other	9	9	9	7	9	9	9	9
Factors Considered When Valuing Damages Associated with IP								
• Loss of Competitive Advantage	1	1	2	3	2	1	2	2
• Lost Sales	2	2	3	1	1	2	1	3
• Loss of Market Share	3	3	1	2	5	3	3	1
• Lost Goodwill	4	4	5	5	3	4	5	5
• Price Erosion	5	5	4	4	6	5	4	4
• Opportunity to Secure New IP	6	6	6	6	4	6	6	6
• Other	7	7	7	7	7	7	7	7

1 Results based on 69 mail survey responding companies; an analysis by companies reporting and not reporting loss incidents is not possible.

- Based upon the detailed rating data used to report these rank order results, (1) loss of competitive advantage, (2) lost sales, and (3) loss of market share are regarded by responding companies to be the most important factors considered when valuing damages associated with intellectual property loss. These three items dominate and encompass the views of virtually all responding companies and only marginal differences exist in the rating scores for these three damage valuation factors.

Most responding companies use intellectual property licensing negotiations when involved in litigation and negotiation activity.

In summary, the assessment or assignment of intellectual property value is usually based on multiple factors: litigation results; transaction characteristics; and licensing negotiations. Intellectual property is most frequently valued by in-house patent and legal counsel who use three major factors or criteria in their evaluation process: competitive advantage, incremental profitability of the intellectual property; and R&D costs. When damages associated with the loss of intellectual property are identified, three major factors are of greatest importance: loss of competitive advantage, lost sales, and loss of market share.

3.8 Litigation and Negotiation Activities

Findings given in Table 3.8 summarize results from responding companies on litigation and negotiation activities associated with loss of proprietary information or intellectual property. As a guide to the interpretation of these data, the reader should note the following observations:

- On an aggregate basis, only one type of litigation and negotiation activity—intellectual property licensing negotiations—was reported to have been employed by a majority of responding companies, though a substantial proportion of responding companies have (1) examined a competing product to determine potential infringements or (2) engaged in intellectual property litigation as either a plaintiff or defendant. Conversely, very few responding companies have retained outside intellectual property firms to evaluate potential infringement issues. (Data from responding companies given in Table 3.8 do not support an analysis of results by industry group, fiscal year revenues, or intellectual property loss experience.)

- In general, responding companies have most frequently employed any type of litigation or negotiation activity they have used between one and five times in the past. However, it is clear that intellectual property licensing negotiations, in addition to being the most frequently employed litigation and negotiation activity, are used much more extensively than any of the other means identified.

In summary, intellectual property licensing negotiations either "license in" or "license out" dominate the litigation and negotiation activities of responding companies. A second tier activity employed by responding companies is their examination of a competitor's product to determine potential areas of infringement.

Table 3.8 Litigation and Negotiation Activity

Litigation and Negotiation Activity	Percents[1]			
	Activity Used	Number of Times		
		1–5	6–10	11 and Over
Engaged in IP licensing negotiations (either "license in" or "license out")	58	30	12	16
Examined a competitor's product to determine potential infringement	48	30	6	12
Engaged in IP litigation (as plaintiff or defendant)	42	30	6	6
Hired an outside IP firm to evaluate potential infringement of respondent company's IP	29	20	3	6
Hired outside IP firm to evaluate whether respondent's company was infringing a third party's IP	29	22	3	4

1 Percents based on 69 mail survey responding companies.

3.9 Strongly Held Attitudes and "Best Practices" Strategies Associated with Protecting Proprietary Information

Findings given in Table 3.10 summarize the rank order results of strongly held and frequently used "best practice" strategies associated with protecting proprietary information. As a guide to the interpretation of these data, the reader should note the following observations:

- On an aggregate basis, a majority of all responding companies, particularly those which did not report loss incidents, expressed strong agreement with the 13 attitudinal and "best practice" strategy statements given in Table 3.10. Hence, the reader should regard this set of statements to be highly relevant to all of the responding companies in a baseline sense.

- In most instances, strong attitudinal and "best practice" strategy agreement levels were found when the responding company data were analyzed by industry group and fiscal year revenues. However, some responding companies in some industry groups and fiscal year revenue categories did not agree strongly with some of the 13 statements given in Table 3.10. These subsample group exceptions are noted with an asterisk (*). In most instances, a lack of strong agreement by some respondents occurred at the lower end of the rank order scale.

- The preceding observations also apply when responding company attitudinal and "best practice" strategy statements were analyzed by loss incidence experience. In this analysis, however, extensive differences were found among responding companies that had and had not reported loss incidents. As shown by the asterisks (*) in Table 3.10, a majority of responding companies reporting loss incidents did not strongly agree with the attitudinal and "best practice" strategy statements. Table 3.9 documents the preceding findings in detail. In this table, the percent of companies strongly agreeing with each statement is presented for companies that had and had not experienced a loss.

Table 3.9 Attitudes and "Best Practices" of Companies Reporting/Not Reporting Loss Incidents

Attitudes and "Best Practices"	Percent[1]	
	Companies Reporting Loss Incidents	Companies Not Reporting Loss Incidents
Information associated with new products and services is vital to the success of our company	75	73
The Internet, networks, and computers and related technologies have created significant new threats to sensitive proprietary information	75	59
Only people with a need to know are given access to sensitive information	40	75
Information security is a priority within our company	45	71
Physical security in my location is adequate to safeguard sensitive documents	44	71
We require everyone to use screen savers and/or server passwords to protect computer systems when unattended	47	66
Our company's policies/guidelines concerning safeguarding sensitive/proprietary information are fit for the purposes for which they were intended	42	69
Non-disclosure agreements are effectively used in our company	49	60
Management is concerned about information loss and takes necessary precautions	36	67
Sensitive information is not seriously at risk in our organization	31	66
Our company has effective information system security procedures	38	64
Our company has not discovered vulnerabilities to electronic means of information gathering ("bugging devices") during assessments of offices and meeting rooms	49	58
Our company has not discovered vulnerabilities to electronic means of information gathering ("bugging devices") during assessments of telecommunications cables and equipment	47	53

1 Percent is based on "strong agreement" ratings from 138 responding companies.

In summary, the data in Table 3.10 provide an overall picture of responding companies' strongly held attitudes and "best practice" strategies associated with the loss of proprietary information. Many responding companies feel that:

- New product and service information is vital to their success;
- The Internet, networks, and computers create new threats of loss;
- Information security is a priority;
- Physical security is adequate to safeguard documents;
- Their policies and guidelines for safeguarding information are fit for intended purposes;
- Management is concerned about information loss and takes necessary precautions;
- Sensitive information is not at risk in their organization;
- Effective information system security procedures exist; and
- Vulnerabilities to electronic means (or "bugging devices") of information gathering have not been found.

Additionally, many companies reduce the risk of proprietary information and intellectual property loss by employing "need to know" policies; using screen savers and/or server passwords; and maintaining non-disclosure agreements.

A key factor in assessing the nature of these data is company experience with proprietary information loss. Many companies experiencing loss indicate less strongly held agreement levels across many different attitudinal and "best practice" strategy statements.

Table 3.10 Strongly Held Attitudes and Frequently Used "Best Practice" Strategies Associated with Protecting Proprietary Information

Strongly Held Attitudes and "Best Practice" Strategies	All Responding Companies	Rank Order Results[1]								
		Industry Group				Fiscal Year Revenues				
		Services	Manufacturing	High Technology	Financial	$5 BL or Less	$6 BL–$15 BL	Over $15 BL	Companies Reporting Loss Incidents	Companies Not Reporting Loss Incidents
Information associated with new products and services is vital to the success of our company	1	1	1	1	1	1	1	2	1	2
The Internet, networks, and computers and related technologies have created significant new threats to sensitive proprietary information	2	4	2	2	*11	9	2	1	2	11
Only people with a need to know are given access to sensitive information	3	3	7	3	5	2	8	7	*10	1
Information security is a priority within our company	4	7	4	4	4	4	5	4	*7	3
Physical security in my location is adequate to safeguard sensitive documents	5	8	6	7	2	5	9	3	*8	4
We require everyone to use screen savers and/or server passwords to protect computer systems when unattended	6	11	2	6	3	3	6	13	*5	7
Our company's policies/guidelines concerning safeguarding sensitive/proprietary information are fit for the purposes for which they were intended	7	2	11	8	6	7	4	5	*9	5
Non-disclosure agreements are effectively used in our company	8	*13	3	5	*13	11	3	8	*3	10
Management is concerned about information loss and takes necessary precautions	9	9	8	9	*12	10	7	9	*12	6

1 Results are based on 138 responding companies.
* Strong agreement with the statements was not found in a majority of responding companies.

Chart continued on next page

Table 3.10 Strongly Held Attitudes and Frequently Used "Best Practice" Strategies Associated With Protecting Proprietary Information (continued)

Strongly Held Attitudes and "Best Practice" Strategies	All Responding Companies	Rank Order Results[1]							Companies Reporting Loss Incidents	Companies Not Reporting Loss Incidents
		Industry Group				Fiscal Year Revenues				
		Services	Manufacturing	High Technology	Financial	$5 BL or Less	$6 BL–$15 BL	Over $15 BL		
Sensitive information is not seriously at risk in our organization	10	*12	9	10	7	*13	*10	10	*13	8
Our company has effective information system security procedures	11	10	10	*13	8	6	*13	12	*11	9
Our company has not discovered vulnerabilities to electronic means of information gathering ("bugging devices") during assessments of offices and meeting rooms	12	5	12	11	9	8	*12	6	*4	12
Our company has not discovered vulnerabilities to electronic means of information gathering ("bugging devices") during assessments of telecommunications cables and equipment	13	6	*13	12	10	12	*11	11	*6	13

1 Results are based on 138 responding companies.
* Strong agreement with the statements was not found in a majority of responding companies.

3.11 Other Attitudes and Less Frequently Used "Best Practice" Strategies Associated with Protecting Proprietary Information

Findings given in Table 3.11 summarize the rank order results of other attitudes and less frequently used "best practice" strategies associated with protecting proprietary information. As a guide to the interpretation of these data, the reader should note the following observations:

- On an aggregate basis, a majority of all responding companies did not express strong levels of agreement with the 22 attitudinal and "best practice" strategy statements given in Table 3.11. Hence, the reader should regard this set of statements to be less relevant to all responding companies in a baseline sense.

- In some instances, strong attitudinal and "best practice" strategy agreement levels were found when the responding company data were analyzed by industry group, revenue size, and loss incidence experience. These exceptions are noted with an asterisk (*).

- It is important to note that none of the companies reporting incidents of proprietary information loss strongly agree with any of the statements given in Table 3.11, while a majority of companies not experiencing such losses strongly agreed with six of these statements. Similarly, companies in the high technology industry group strongly agreed with seven of the statements given in Table 3.11. Thus, companies that had experienced losses also appear not to have adopted best practices for protecting their intellectual property.

In summary, the data given in Table 3.11 present less strongly held attitudinal and "best practices" strategy statements associated with the loss of proprietary information. However, some of these propositions might be relevant to the security needs of some companies and the actions of security management professionals in these companies.

Table 3.11 Other Attitudes and Less Frequently Used "Best Practice" Strategies Associated with Protecting Proprietary Information

Less Frequently Held Attitudes and "Best Practice" Strategies	All Responding Companies	Rank Order Results[1]								
		Industry Group				Fiscal Year Revenues				
		Services	Manufacturing	High Technology	Financial	$5 BL or Less	$6 BL–$15 BL	Over $15 BL	Companies Reporting Loss Incidents	Companies Not Reporting Loss Incidents
Employees know where to find answers to information security questions	1	1	*2	*3	5	1	1	8	7	*1
The digital forms of our trade secrets and proprietary information are at least as well protected as the hard copy sources of the same information	2	2	5	*1	*3	2	3	*3	4	*2
Our law department works closely with the information systems and security staff to help identify and protect the digital forms of trade secrets and sensitive proprietary information	3	5	*1	*4	6	3	4	*1	1	*4
Sensitive materials, when no longer needed, are destroyed completely	4	3	6	5	7	5	9	*2	10	*3

1 Results are based on 138 responding companies.
* Strong agreement with the statements was found in a majority of responding companies.

Chart continued on next page

Table 3.11 Other Attitudes and Less Frequently Used "Best Practice" Strategies Associated with Protecting Proprietary Information (continued)

Less Frequently Held Attitudes and "Best Practice" Strategies	All Responding Companies	Rank Order Results[1]							Companies Reporting Loss Incidents	Companies Not Reporting Loss Incidents
		Industry Group				Fiscal Year Revenues				
		Services	Manufacturing	High Technology	Financial	$5 BL or Less	$6 BL–$15 BL	Over $15 BL		
Our company performs complete background investigations of all full- and part-time employees	5	8	3	11	*1	4	2	14	5	*5
Our company ensures that temporary and contract staff have background investigations equivalent to regular staff of equivalent responsibility	6	6	8	12	4	7	7	*4	3	8
Our company formally assesses the security of business partners and vendors before extending our intranet or network connectivity to them	7	15	4	*6	*2	6	5	*6	6	7
Information losses are reported to law enforcement	8	7	7	8	12	8	8	*7	2	12
Information is safeguarded well at off-site conferences, trade shows, and meetings	9	9	9	*7	11	9	10	9	13	*6
Sensitive documents are properly classified, marked, and handled	10	4	10	8	16	10	12	10	8	9
Effective, continuing information security training/awareness is provided	11	11	11	15	8	11	11	22	15	10
Our company uses distinctive markings to identify and protect proprietary information	12	18	12	*2	13	16	6	11	11	14
We provide effective information security training soon after people start working here	13	12	13	16	9	12	13	12	18	11
People take adequate security precautions to protect sensitive proprietary information when traveling	14	10	14	13	19	13	15	15	19	13

1 Results are based on 138 responding companies.
* Strong agreement with the statements was found in a majority of responding companies.

Chart continued on next page

Table 3.11 Other Attitudes and Less Frequently Used "Best Practice" Strategies Associated with Protecting Proprietary Information (continued)

Less Frequently Held Attitudes and "Best Practice" Strategies	All Responding Companies	Rank Order Results[1]								
		Industry Group				Fiscal Year Revenues				
		Services	Manufacturing	High Technology	Financial	$5 BL or Less	$6 BL–$15 BL	Over $15 BL	Companies Reporting Loss Incidents	Companies Not Reporting Loss Incidents
Sensitive information is encrypted when transmitted over the Internet	15	14	15	17	10	14	18	5	9	16
Former employees comply with their obligation to safeguard our information	16	16	16	10	14	15	19	13	16	15
Sensitive information is always properly secured when not being used	17	13	21	18	17	17	16	19	21	17
OEM/partner companies provide adequate safeguards for our information	18	20	18	14	18	18	20	16	20	19
Temporary and contract employees are never assigned to critical projects or work areas containing trade secrets and other sensitive proprietary information	19	19	17	19	21	19	17	20	22	18
Law enforcement provides effective support for information loss incidents	20	17	19	20	20	20	14	21	12	20
Recent information loss incidents could seriously affect our company	21	21	22	21	15	21	22	17	14	21
Our company has been successfully targeted by business intelligence or competitive intelligence staff working for our competitors	22	22	20	22	22	22	21	18	17	22

1 Results are based on 138 responding companies.
* Strong agreement with the statements was found in a majority of responding companies.

Section 4

Study Conclusions

Intellectual property loss continues to represent a major threat to U.S. corporations. During the period covered by the survey, it affected nearly one in two of the responding companies and cost tens of billions of dollars annually. Given empirical and/or anecdotal evidence that companies are hesitant to admit to such losses, these numbers likely understate the problem.

There are a number of preliminary conclusions that can be drawn from the survey:

- The impacts of proprietary information loss are both short and long-term. Some effects of the problem are carefully documented, while others are difficult, if not impossible, to quantify precisely; could be far more costly; and may not be easily recognizable. Increased legal costs would fit into the short-term/documented category, while other problems associated with intellectual property theft would be manifested both short and long-term, such as lost sales revenue, erosion of market share, and loss of competitive advantage.

  Regardless of how these losses are perceived, all result in reducing the net present value of future operations. As such, these losses should concern investors and corporate strategic planners as much as they do operations, security managers, and corporate counsel.

- Four major risk factors—former employees, foreign competitors, on-site contractors, and domestic competitors—are associated with the loss of proprietary information and intellectual property. Several other factors—computer hackers, vendors/suppliers, current employees, and intelligence services—pose significant risks on a secondary or selected basis within subsample segments. 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 (IT) security practices.

  The finding that computer hackers were considered nearly as much a threat as unethical domestic competitors bears special note. Based on the experience of members of the ASIS Council on Safeguarding Proprietary Information (ASIS Council), hackers represent the greatest threat to an organization's sensitive proprietary information, as these assets are increasingly created, stored, and transmitted using computer and telecommunications networks. This is an area that should be earmarked for heightened scrutiny by businesses and in upcoming sequels to this survey.

- Those companies that have experienced information loss have a markedly different sense of the nature of the threats to information protection than those companies that have not. The reason for this is unknown, as it is unclear whether the absence of information loss is due to the use of "best practices", to good fortune, or to the absence of a centralized reporting mechanism. Regardless, it is incumbent on all companies to employ "best practices" to safeguard their proprietary information, to review these procedures on a regular basis, and to upgrade them when circumstances warrant such revisions.

In addition, there are several issues related to intellectual property loss that need urgent attention:

1. Companies must overcome their reluctance to share, even anonymously, information about losses. The continued lack of information makes it difficult to determine the full extent and nature of the problem, which is a critical first step in developing an effective response. As a corollary to this issue, companies need to centralize their loss reporting systems to ensure that comprehensive data is gathered and can be reported. This is a problem especially for multinational corporations, given geographical dispersion, cultural and language differences which could make adherence to policies more challenging, and the potential for information being maintained at a facility or subsidiary level and not transmitted to corporate headquarters.

2. Businesses must make information protection a higher priority and must institute sound protection procedures. Research data about attitudes and best practices reveals that many companies do not follow important basic information protection policies, such as properly marking proprietary information, training employees to be aware of the risks, and taking proper precautions.

3. Corporations must set up a system for valuing intellectual property assets as they are created. Currently, as the survey shows, companies do not generally assess value up front. Consequently, by the time an incident occurs and security, legal, IT, or other departments are called in, the mode is one of retroactive damage control.

The lack of proper valuation procedures also results in misunderstandings about the damage caused by information loss. For example, the survey shows that many companies do not rank loss of market share as a major concern. Instead, respondents indicated that the problem caused by an information loss was increased legal fees and the immediate impact on revenues. In reality, although more difficult to measure, the cumulative impact over time of losses in competitive advantage and market share could be much greater than most parties realize, far outweighing legal fees. Since they are longer term and declines could be attributed to a wide range of other variables, it is likely that many organizations do not fully appreciate the real nature of their risks. However, members of the ASIS Council believe that the impacts of cumulative losses of proprietary information are not well tracked, even in very sophisticated organizations. As a consequence, losses could be playing a much greater role in market share erosion and, ultimately, in loss of competitive advantage, than may be apparent to individual executives and managers.

In the new world order since the attacks of September 11, we must consider how efforts to safeguard proprietary information can both benefit from other security disciplines and contribute toward efforts to combat global terrorism. Over the past years, the *Trends in Proprietary Information Loss Surveys* have highlighted the fact that documented losses of trade secrets and other proprietary information cost U.S. companies tens of billions of dollars annually. Yet, high profile incidents involving major corporations continue unabated, illustrating that misappropriation of intellectual property remains a serious problem afflicting many businesses.

It also is a major challenge for security management professionals. Protecting proprietary information is more important than ever. But until senior managers begin to value both their proprietary information and the measures required to protect it, the loss of these intangible assets will continue to dampen profits and rein in new opportunities for future business success.

Meanwhile, the three sponsors of this study—PricewaterhouseCoopers, the U.S. Chamber of Commerce, and the ASIS Foundation—will continue to draw attention to this issue by making more corporate managers and government officials aware of its significance. In addition to benchmarking the extent of corporate losses, this research serves as a call to action—action to protect information assets through the implementation of best practices; to prepare for future losses through immediate, thorough, and timely valuation; and to participate in sharing data in the future, both internally within the corporation through greater centralization of the information and externally through future *Trends in Proprietary Information Loss Surveys* and other research. Unless these measures are taken, the problem will continue to be undervalued and underreported.

Section 5

Acknowledgments

This survey is the latest in a continuing series by ASIS International and the first to be conducted under the auspices of the ASIS Foundation. It also is the first time that the survey has had the benefit of two prestigious sponsoring organizations: PriceWaterhouseCoopers, repeating sponsorship for the second time, and the U.S. Chamber of Commerce, which is marking its first-time involvement with ASIS on this project.

ASIS wishes to extend its thanks for the time, generosity, and support of those individuals from the sponsoring organizations who helped to coordinate this project:

- From PWC, the following practice leaders contributed to the survey: Andrew Toner, Partner (646–471–8327) and Jay Ehrenreich, Senior Manager (646–471–8018) based in the New York Practice Office; Greg Schaffer, Director (202–822–4384) based in the Washington, D.C. Practice Office; Andrew Beard, Director (44–207804–3971) based in London; and Malcolm Shackell, Partner (612–8266–2993) based in Sydney.

- From the U.S. Chamber of Commerce, the following individuals were closely involved: Stephen C. Jordan, Vice President and Executive Director, The Center for Corporate Citizenship (202–463–5490); Scott C. Algeier, Associate Director, Economic Security Affairs (202–463–5845); and Gregori Lebedev, Chief Operating Officer and Executive Vice President, International Policy.

Much gratitude also is extended to the members of the ASIS Council on Safeguarding Proprietary Information, which spearheaded this project and without which this survey would not have been possible. In particular, thanks are due to William C. Boni, CPP, chair of the Council, who saw the project through to its completion, and to Dan Swartwood, whose contribution warrants special recognition. Other members of the Council, all of whom participated in structuring the survey instrument and reviewing the final report, include: Stephen F. Argubright, Jr., Vice Chairman; Jonathan P. Binnie; Ross D. Bulla, CPP; Donald R. Charlesworth, CPP; Craig DeCampli; Donald E. Greenwood; William R. Halliday; John Hartmann; Richard J. Heffernan, CPP; Donna Jo Kahl, CPP; Jose Roman; Frank E. Rudewicz, CPP; Lindsey (Pete) Van De Gohm, CPP; and James Robert Wade.

And finally, many thanks to the membership of ASIS and the U.S. Chamber of Commerce, especially the companies that participated in the survey. We appreciate the continued support of security professionals who candidly assessed their own company's performance and shortcomings. Without this input, the value of these surveys would be substantially diminished. It is our hope that through this process and reporting mechanism, more companies will come to realize the value of shared data, and the pool of participants will grow over time.

ASIS International

ASIS International (ASIS) is the preeminent global educational organization for security practitioners, with over 32,000 members in 110 countries. ASIS also advocates the role and value of the security management profession and ASIS to business, the media, governmental entities, and the public.

Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar & Exhibits, as well as specific security topic areas. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's number one magazine—*Security Management*—ASIS leads the way for improved security performance and for advancing security worldwide.

ASIS Foundation

The ASIS Foundation provides a vital link between academic and professional development through funding and managing endowments for a wide range of activities. In addition, the ASIS Foundation participates in the development of academic programs such as the Masters of Arts Degree in Security Management, sponsors special security industry reports and research such as the *Trends in Proprietary Information Loss Survey Report*, and acknowledges security-related advancements and achievements through provision of educational scholarships and various award programs.

Foundation programs are made possible by financial contributions from individuals, chapters, companies employing ASIS members, and corporations with an interest in security. The ASIS Foundation also sponsors fundraising events.

Advancing Security Worldwide™

ASIS International
1625 Prince Street
Alexandria, VA 22314–2818 USA
1.703.519.6200
www.asisonline.org

PRICEWATERHOUSECOOPERS