National Counterintelligence Executive

The National Counterintelligence Executive (NCIX) serves as the head of national counterintelligence (CI) for the U.S. government and is directly responsible to the Director of National Intelligence. The NCIX facilitates and enhances U.S. CI efforts and awareness by:

- Enabling the CI community to better identify, assess, prioritize, and counter intelligence threats from foreign powers, terrorist groups, and other non-state entities.
- Ensuring that the CI community acts efficiently and effectively.
- Providing for the integration of all U.S. CI activities.

The NCIX chairs the National Counterintelligence Policy Board, the principal interagency mechanism for developing national CI policies and procedures, and it leads the Office of the National Counterintelligence Executive, which is staffed by senior CI and other specialists from across the national intelligence and security communities.

ASIS Information Asset Protection Council

Originally established as the Safeguarding Proprietary Information Committee, the Information Asset Protection (IAP) Council is comprised of a select group of ASIS members who are subject-matter experts representing a wide variety of organizations including Fortune 1000 companies, as well as independent consultants and educators. The council’s name was changed in 2004 to reflect the increasing complexity of the global environment and the associated broadening of information-protection issues. IAP is one of approximately 30 ASIS councils that serve as clearinghouses for topical information, provide educational resources, and act as liaisons between ASIS and the outside community.

The IAP Council promotes education and awareness, exchanges best practices, supports the ASIS certification programs, reviews articles, and develops products to assist the business and security communities with information-protection issues. Through its activities and products, the council encourages the exchange of best practices to achieve optimum protection of information assets for organizations, both public and private, worldwide. Among the key concepts promoted by the council are the use of a risk-based approach along with the integration of carefully selected, environment-appropriate protection measures as part of a comprehensive strategy to protect sensitive information, intellectual property rights, and other intangible assets.
# Table of Contents

Executive Summary .................................................. 1  

Section 1. Introduction and Overview ................................. 4  

Section 2. Survey Methodology ........................................ 6  

Section 3. Key Findings ................................................ 11  

Section 4. Survey Results .............................................. 14  

About the Principal Investigators .................................... 42  

Appendix (Glossary of Terms) ....................................... 45
Executive Summary

American industry is being challenged, both at home and abroad, in its efforts to protect against traditional and emerging foreign threats to its property. Documented losses of trade secrets and other proprietary information have had a major negative impact on U.S. companies, financially and otherwise. Although as much as 75 percent of the market value of a typical U.S. company resides in intellectual property (IP) assets, firms rarely perform formalized valuations of these assets. As a result, corporate accounting systems may not be adequately tracking them. This omission has become even more significant with the passage of the Sarbanes-Oxley Act. Since the value of IP assets is not well established, often they are not protected at a level commensurate with their value or criticality to the business. This contributes to the current problems associated with theft of proprietary information and trade secrets.

The lack of formal information-security management processes for the identification, valuation, risk assessment, and mitigation of information assets continues to contribute to the current problems associated with the compromise of proprietary information. According to The National Counterintelligence Strategy of the United States, “comprehensive risk management, valid security practices, and an informed strategic world view are among the best guarantors of success against foreign intelligence threats.”

To determine how well America is succeeding in confronting this challenge, the ASIS Foundation and ASIS Information Asset Protection (IAP) Council, with the support of the Office of the National Counterintelligence Executive, conducted the 2006 ASIS Trends in Proprietary Information Loss Survey. This is the seventh edition of the survey that, since 1991, has come to be recognized as the premier study of its kind. The results of this survey are used to educate audiences about the variety of ways in which information is compromised within the private sector and the effect that these losses have on U.S. corporations and the nation’s economic well-being.

The objectives of this survey were to collect data about the current state of proprietary information loss experienced by U.S. businesses from both U.S. and foreign competitors; determine the types of practices used by corporations to safeguard their intellectual property assets; advocate on behalf of the corporate community, so as to enhance awareness of the problem and its extent; and report changes in targeting or threats so that organizations can determine whether their current security controls are adequate.

The survey was conducted in the spring and summer of 2006. A total of 144 respondents from a diverse array of businesses participated. The results of the survey were compiled and tabulated to produce the findings in this report. Results from the survey will allow security professionals to better design and manage security programs to protect information assets.
Consistent with previous editions, this survey tracks current and emerging threats as well as incidents of compromise of, or unauthorized access to, proprietary and/or trade secret information. The 2006 survey also addresses trends in due diligence and risk-assessment practices, including those related to outsourcing and doing business overseas, and measures the organizational impact of compromises.

The results of this survey will be used to report changes in targeting and collection methods and include information that U.S. corporations must examine when planning to do business in or with a foreign country. The survey report provides the corporate community with information to help mitigate new and evolving threats and serves to increase national awareness of the problem and its extent. This survey is important to all in the security profession whose job it is to design and manage security programs to protect information assets.

**Major Findings**

**Risks**

- Organizations are performing regular risk assessments of information assets, but valuation of information assets and identification of the potential impact of loss or disclosure are lagging behind.

- Changes in the levels of risk to information assets are being identified and more routinely reported to management.

- Due-diligence reviews before partnering with U.S. or foreign organizations have expanded to include the identification of foreign ownership, management control and relationships, and on-site inspection of both U.S. and foreign facilities.

- Most information reported as having been compromised was physically located in the United States when the compromise occurred.

- Information assets in all formats (paper, electronic, oral, prototypes, and models) are being targeted for possible compromise.

**Threats**

- The top three foreign countries identified as the intended recipients in reported compromise incidents were China, Russia, and India.

- Deliberate actions of current and former employees are a primary threat to proprietary information.
• Inadvertent actions of current and former employees continue to be a major threat to proprietary information.

• Exploitation of trusted relationships—including those involving vendors, customers, joint ventures, and subcontractors/outsourced providers—is a threat to proprietary information.

• Data mining software and the availability of open-source and public information, along with social engineering, present significant threats to the U.S. economy.

** Magnitude, Frequency, and Impact of Loss**

• The number of information-compromise attempts and their impact costs in 2005 were comparable to or higher than in 2004.

• Respondents reported varying degrees of financial impact ranging from less than $10,000 to more than $5.5 million.

• All types of business transactions are targets of compromise attempts.

• Information compromises have resulted in losses to reputation, image, goodwill, competitive advantage, core technology, and profitability.

Richard J. Heffernan, CPP, CISM
Chair, ASIS Trends in Proprietary Information Loss Survey
ASIS conducted the first *Trends in Proprietary Information Loss Survey* in 1991 at the invitation of the Judiciary Committee of the U.S. House of Representatives to determine the nature and extent of foreign espionage directed against American businesses. Richard Heffernan and the committee he chaired at the time—the ASIS Safeguarding Proprietary Information Committee—developed a questionnaire, collected and analyzed the results, and reported them to the Judiciary Committee. The results were also published in *Security Management* magazine.

Since 1991, ASIS has conducted a new *Trends in Proprietary Information Loss Survey* every two to three years. The resulting reports have been used by U.S. government agencies and private entities. For example, survey results have been used by all levels of the U.S. government to help provide an estimate of evolving threats, identify methods and impact of loss, and catalog organizational responses to address identified risks. Survey findings have been cited in the *Annual Report to Congress on Foreign Economic Collection and Industrial Espionage* by the Office of the National Counterintelligence Executive. Mr. Heffernan’s testimony before the House Judiciary Committee was a key factor in shaping the Economic Espionage Act (USC §§1831-1832), the major federal legislation designed to protect U.S. trade secrets. In addition, security practitioners, legal professionals, investigators, academicians, and students in both the public and private sectors have found value in the information ASIS provided.

In today’s complex world, the survey must explore the practices and experiences of the respondents in greater depth. Issues such as risk assessment, due diligence, and evolving targeting techniques are addressed in the survey. The 2006 survey focuses on emerging globalization issues, the corporate regulatory environment, and the continued blurring of the threats to American industry.

The survey’s authors intend that this survey and future editions will enable security professionals and business and government leaders to better understand current and evolving information-asset protection issues and implement effective protective strategies.
2006 Survey Goals and Philosophy

The 2006 survey was structured to:

- Collect and report data showing the current magnitude, frequency, and impacts of proprietary information losses experienced by U.S. businesses.
- Report changes in targeting and collection.
- Explore details on the factors that organizations must examine before the consummation of new business opportunities in a global market.
- Balance historic information collected in past surveys with new questions that reflect today’s complex environment.
- Retain selected questions and issues from previous editions of the Trends in Proprietary Information Loss Survey.
- Recognize the nature of the contemporary world using questions on global relationships, risk-assessment procedures, and the regulatory environment.
- Request specific and detailed data on the “single-most serious” incident of compromise.
- Complement other products and issues under study by the ASIS Foundation, IAP Council, and the Office of the National Counterintelligence Executive.

It also is important to note that the 2006 target survey audience includes a greater number of small and medium-sized businesses than previous editions. The authors recognize that enterprises and entrepreneurial ventures at this scale are making increasingly important contributions to the global economy, particularly in the areas of high technology and innovation.

Besides including a broader range of businesses, this report incorporates the authors’ underlying philosophy that the security and assets protection function must serve as a business enabler rather than an obstacle in the interpretation and analysis of the survey results. The authors believe strongly that meaningful protection strategies—particularly in today’s environment—must be grounded in this premise.
The ASIS Information Asset Protection (IAP) Council tasked a team of four subject-matter expert members with developing this year’s survey, overseeing the process, and interpreting and reporting the results. These principal investigators collaborated with the National Counterintelligence Executive to define specific objectives, set the tone of the survey, and identify the contemporary issues to be included in the survey instrument. With the assistance of Westat Corporation, a well-respected research and statistical analysis firm located in Rockville, Maryland, the team formulated the survey questions and outlined the data-collection and analysis procedures. Westat then administered the survey and managed the data-collection effort.

In 2006, for the first time, the survey was divided into two parts. Part A asked respondents to provide information on the processes in place to assess and address potential information loss as well as their experience with incidents of targeting. The areas of inquiry included the processes for risk assessments, the due-diligence steps taken before contracting to work with another corporation, and a summary of the incidents of attempted or successful acquisitions of proprietary information and their impact.

Part B asked respondents to provide information on the single-most-significant successful attempt to compromise or gain unauthorized access to their organization’s proprietary and trade secret information during 2005. Part B had a significantly lower response rate, as companies are reluctant to share this kind of information publicly—even if anonymously.

Once the survey questionnaire was developed, a “pilot” survey was conducted among select members of the ASIS Chief Security Officer Roundtable, the ASIS Board of Directors, and past and present members of the IAP Council. These participants represented a wide range of commercial enterprises from Fortune 500 companies to small, high-tech start-ups. The results of the pilot survey were evaluated to ensure that the survey questions were commonly understood, straightforward, relevant, and reasonable in terms of the effort required to complete the survey.

When the pilot was successfully completed, an initial survey audience consisting of 1,400 U.S.-based commercial businesses was defined from among organizations that included ASIS members. The survey team collected data from this group between May and July 2006. The survey procedures were designed to ensure the confidentiality of the respondents and isolate the identity of any responding companies from ASIS, the Foundation, and the principal investigators.

From the initial audience pool, the survey team received a total of 144 responses for a response rate of approximately 10.3 percent. Westat tabulated the responses and reported the data to the principal investigators for analysis. On the basis of this information, the team then developed the key findings, conclusions, recommendations, and supporting material presented in this report. Preliminary results and conclusions were reported at the September 2006 ASIS Annual Seminar & Exhibits in San Diego, California.
The principal investigators would like to express their appreciation to the following individuals who provided outstanding support to this effort:

- Mr. Robert Rowe, Director of Development, ASIS International.
- Dr. Dean W. Carver, Office of the National Counterintelligence Executive.
- Dr. Philip G. Kuehl, Senior Staff Consultant, Westat Corporation.
- Members of the ASIS Information Asset Protection Council.

**Profile of Respondents**

The first three questions on the survey provided demographic information, allowing readers to understand the industry sectors represented and the types of business activities in which they are primarily engaged. The information is based on self-reporting. In other words, it shows how the respondents characterized their own industry sector and the primary nature of their business. This understanding is valuable in demonstrating that a wide variety of industries—both high-tech and low-tech—are represented in the survey data, and, even within industries, companies play different roles such as producer, service provider, researcher and developer, or product distributor.

Table 1 and Figures 1 and 2 provide responses to questions 1 and 2.
Table 1.  Respondent Profile by Industry Sector and Primary Nature of Business Activity

<table>
<thead>
<tr>
<th>Industry sector</th>
<th>Academic research</th>
<th>Manufacturing</th>
<th>Product sales or distribution</th>
<th>Service provider</th>
<th>Other</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aerospace &amp; aviation systems or components</td>
<td>5</td>
<td>2</td>
<td>7</td>
<td></td>
<td></td>
<td>12</td>
</tr>
<tr>
<td>Chemical &amp; composite materials</td>
<td>1</td>
<td></td>
<td>1</td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Consumer products</td>
<td>8</td>
<td>6</td>
<td>4</td>
<td>1</td>
<td></td>
<td>15</td>
</tr>
<tr>
<td>Financial products &amp; services</td>
<td>1</td>
<td>1</td>
<td>14</td>
<td>16</td>
<td></td>
<td>18</td>
</tr>
<tr>
<td>Healthcare services</td>
<td>1</td>
<td>2</td>
<td>18</td>
<td>21</td>
<td></td>
<td>32</td>
</tr>
<tr>
<td>Information/telecommunications systems, components, or services</td>
<td>3</td>
<td>8</td>
<td>2</td>
<td>13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Life science, pharmaceuticals, biotech, medical devices, or agriculture</td>
<td>3</td>
<td>4</td>
<td>1</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Motor vehicles &amp; components</td>
<td>2</td>
<td></td>
<td>2</td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Natural resources, electric power, or utilities</td>
<td>3</td>
<td>5</td>
<td>8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Transportation service providers</td>
<td></td>
<td>2</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Educational institutions or services</td>
<td>10</td>
<td>1</td>
<td>1</td>
<td>11</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>2</td>
<td>30</td>
<td>2</td>
<td>36</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>All respondents</strong></td>
<td><strong>16</strong></td>
<td><strong>29</strong></td>
<td><strong>9</strong></td>
<td><strong>85</strong></td>
<td><strong>4</strong></td>
<td><strong>143</strong></td>
</tr>
</tbody>
</table>

Note: Not all respondents reported their industry sector or primary business activity. Results are based on 143 respondents.
Figure 1. Percentage of Respondents by Industry Sector

- Aerospace & aviation: 5%
- Chemical & composite materials: 1%
- Consumer products: 13%
- Financial products & services: 11%
- Healthcare services: 15%
- IT & telecommunications: 9%
- Education: 8%
- Natural resources, electric power, utilities: 6%
- Motor vehicles: 1%
- Life science, pharmaceuticals, biotech, agriculture: 6%
- Other: 24%

Note: Results are based on 143 respondents.

Figure 2. Percentage of Respondents by Nature of Business

- Service providers: 59%
- Academic research: 12%
- Manufacturing: 20%
- Product sales, distribution: 6%
- Other: 3%

Respondents also provided data on their organization’s annual revenue. To help ensure consistency, the survey team requested the inclusion of revenue for all business units of the company for the last fiscal year. This provided some perspective on the size of each enterprise in terms of its financial volume. The responses are shown in Table 2. Again, the survey respondents represent a wide variety of revenue levels.

Note: Results are based on 143 respondents.
Table 2. Annual Revenue (Previous Fiscal Year)

<table>
<thead>
<tr>
<th>Annual revenue (U.S. dollars)</th>
<th>Number of respondents</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt; $10 million</td>
<td>15</td>
<td>10.4</td>
</tr>
<tr>
<td>$10-$49 million</td>
<td>20</td>
<td>13.9</td>
</tr>
<tr>
<td>$50-$99 million</td>
<td>13</td>
<td>9.0</td>
</tr>
<tr>
<td>$100-$499 million</td>
<td>13</td>
<td>9.0</td>
</tr>
<tr>
<td>$500-$999 million</td>
<td>16</td>
<td>11.1</td>
</tr>
<tr>
<td>$1-$4.9 billion</td>
<td>30</td>
<td>20.8</td>
</tr>
<tr>
<td>$5-$9.9 billion</td>
<td>7</td>
<td>4.9</td>
</tr>
<tr>
<td>$10 billion and over</td>
<td>10</td>
<td>6.9</td>
</tr>
<tr>
<td><strong>Total reporting</strong></td>
<td><strong>124</strong></td>
<td><strong>86.1</strong></td>
</tr>
<tr>
<td><strong>Not available</strong></td>
<td><strong>20</strong></td>
<td><strong>13.9</strong></td>
</tr>
<tr>
<td><strong>Total respondents</strong></td>
<td><strong>144</strong></td>
<td><strong>100.0</strong></td>
</tr>
</tbody>
</table>

Note: Totals may not add due to rounding. Results are based on 144 respondents.

Figure 3. Number of Respondents by Annual Revenue

Note: Results are based on 144 respondents.
Key Findings

The survey revealed a number of significant points in terms of the respondents’ business practices and experiences relevant to protecting information assets. The key findings from the survey results are presented below. More detailed information and response data is provided in Section 4 along with commentary.

I. Major Findings

The survey indicates that:

- Organizations are performing regular risk assessments of information assets, but valuation of information assets and the identification of impact of loss and disclosure lag behind; that is, companies lack procedures to track, monitor, and account for losses and compromises.

- Changes in levels of risk to information assets are being identified and more routinely reported to management, but the levels of information safeguards in place are not consistent with the value and criticality of the assets.

- Due-diligence reviews done before partnering with U.S. or foreign organizations have expanded to include:
  - Identification of foreign ownership.
  - Management control and relationships.
  - On-site inspection of both U.S. and foreign facilities.

- Most information reported as being compromised was physically located in the United States when the compromise occurred.

- Information assets in all formats (paper, electronic, oral, prototypes, and models) are being targeted for possible compromise.

II. Responses to Compromise Incidents

In response to compromise incidents, companies are:

- Conducting investigations.

- Performing damage assessments.
• Reassessing security controls.
• Revising due-diligence and risk-assessment processes.
• Bringing civil and criminal court actions.
• Withdrawing from business transactions.
• Redesigning product offerings.

III. PRIMARY RISKS/THREATS TO INFORMATION ASSETS

The survey indicates the following primary risks to information assets:

• Deliberate and inadvertent actions of current and former employees.
• Exploitation of trusted relationships by vendors, customers, joint venture partners, and subcontractors/outsourced providers.
• Data mining and software-driven collection of open-source data and public information joins social engineering as a significant threat.
• All types of business transactions are being targeted and subject to compromise attempts.
• The top three foreign countries identified as the intended recipients in reported compromise incidents were China, Russia, and India.

IV. MAGNITUDE, FREQUENCY, AND IMPACT OF LOSS

Survey findings on information loss are:

• The number of information-compromise attempts and business-impact costs in 2005 were comparable to or higher than 2004.
• Respondents reported varying degrees of financial impact ranging from less than $10,000 to more than $5.5 million.
• Information compromises have resulted in losses to reputation, image, goodwill, competitive advantage, core technology, and profitability.
V. SURVEY IMPLICATIONS/ACTIONS SUGGESTED BY THE DATA

Organizations should consider:

• Directing adequate resources toward identifying and mitigating the potential “insider threat.”

• Addressing how personnel associated with business transactions may be subject to exploitation, co-opting, and extortion to facilitate information compromise.

• Calculating and measuring enterprisewide business impacts of actual and potential information compromises and losses.

• Conducting risk assessments and due diligence for any business transaction or process in which intellectual property (IP) and other information-based intangible assets and proprietary competitive advantages are involved.

• Applying holistic enterprisewide approaches for conducting risk assessments and due diligence. Such approaches are preferable to viewing information-compromise attempts or infringement as individual or isolated acts.

• Addressing the value of intangible assets when conducting risk assessments and due diligence in ways that reflect U.S. and EU accounting and reporting mandates, including the Sarbanes-Oxley Act, standards issued by the Financial Accounting Standards Board (FASB), and standards promulgated by the Independence Standards Board (ISB).

• Examining nuances (that is, adequacy and enforceability) of IP laws in each country in which business transactions are being conducted.
This section presents the survey results along with commentary and interpretation of the data. The information is divided into two parts corresponding with the structure of the survey. The results for Part A are further divided into relevant topics that were addressed by survey questions. Each question is listed individually and followed by a table and/or chart exhibiting the results and a brief commentary.

**PART A: PROCESSES TO ADDRESS INFORMATION LOSS**

1. **PROPRIETARY INFORMATION–RISK ASSESSMENT**

A section on proprietary information–risk assessment sought replies on current processes employed to identify and value assets, other risk-assessment steps, preparation for outsourcing operations, and practices related to the reporting of changes in risk posture.

**QUESTION: HOW OFTEN DOES YOUR ORGANIZATION EMPLOY THE FOLLOWING RISK ASSESSMENT–PROCESS STEPS AT THE OVERALL PRODUCT, PROGRAM, OR PROCESS LEVEL?**

Table 3. Risk Assessment–Process Steps (Higher Level)

<table>
<thead>
<tr>
<th>Process Step</th>
<th>Always/ almost always</th>
<th>Usually</th>
<th>Seldom/ never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify information assets (total responses: 133)</td>
<td>91</td>
<td>38</td>
<td>4</td>
</tr>
<tr>
<td>Assign quantitative or qualitative value (total responses: 127)</td>
<td>65</td>
<td>40</td>
<td>22</td>
</tr>
<tr>
<td>Assess threats to information assets (total responses: 132)</td>
<td>83</td>
<td>42</td>
<td>7</td>
</tr>
<tr>
<td>Assess likelihood of occurrence of threats (total responses: 131)</td>
<td>77</td>
<td>44</td>
<td>10</td>
</tr>
<tr>
<td>Identify vulnerabilities to information assets (total responses: 134)</td>
<td>87</td>
<td>39</td>
<td>8</td>
</tr>
<tr>
<td>Assess impact of loss or disclosure (total responses: 132)</td>
<td>75</td>
<td>42</td>
<td>15</td>
</tr>
<tr>
<td>Identify existing and planned security controls (total responses: 138)</td>
<td>102</td>
<td>28</td>
<td>8</td>
</tr>
<tr>
<td>Assess, rank, and prioritize risks (total responses: 133)</td>
<td>77</td>
<td>40</td>
<td>16</td>
</tr>
</tbody>
</table>
PRINCIPAL INVESTIGATORS’ COMMENTARY

Risk assessment is a key element on which reasonable information-asset-protection strategies should be based. This question explores the nature of the risk assessments the respondents perform and the steps they include. It is important to note that risk assessment can be performed at various levels within any organization. This question asks what risk-assessment steps are performed at a relatively high level—the “overall product, program, or process level.”

The results reveal that, although most respondents do actively identify their information assets, many of them do not assign a quantitative or even qualitative value to them. The most likely reason for this is that it is far more difficult to assign value to information assets than to physical or tangible assets such as buildings and equipment. Assigning value, however, provides a basis for setting protection priorities and performing cost/benefit analyses. In addition, identifying the value of intangible assets is now required by various federal regulations (such as Sarbanes-Oxley and FASB) in many business settings. The results also indicate that some respondents who may engage in high-level risk assessment may not pay as much attention to the potential impact of a loss or to prioritizing the identified risks as they do to other steps in the assessment process.

QUESTION: HOW OFTEN DOES YOUR ORGANIZATION EMPLOY THE FOLLOWING RISK ASSESSMENT–PROCESS STEPS AT THE SUBCOMPONENT, SUBPROCESS, OR SPECIFIC TECHNOLOGY LEVEL?

Table 4. Risk Assessment–Process Steps (Lower Level)

<table>
<thead>
<tr>
<th>Risk Assessment–Process Steps</th>
<th>Always/ almost always</th>
<th>Usually</th>
<th>Seldom/ never</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify information assets (total responses: 100)</td>
<td>55</td>
<td>41</td>
<td>4</td>
</tr>
<tr>
<td>Assign quantitative or qualitative value (total responses: 97)</td>
<td>46</td>
<td>34</td>
<td>17</td>
</tr>
<tr>
<td>Assess threats to information assets (total responses: 101)</td>
<td>55</td>
<td>38</td>
<td>8</td>
</tr>
<tr>
<td>Assess likelihood of occurrence of threats (total responses: 101)</td>
<td>52</td>
<td>37</td>
<td>12</td>
</tr>
<tr>
<td>Identify vulnerabilities to information assets (total responses: 101)</td>
<td>57</td>
<td>35</td>
<td>9</td>
</tr>
<tr>
<td>Assess impact of loss or disclosure (total responses: 98)</td>
<td>51</td>
<td>35</td>
<td>12</td>
</tr>
<tr>
<td>Identify existing and planned security controls (total responses: 101)</td>
<td>64</td>
<td>30</td>
<td>7</td>
</tr>
<tr>
<td>Assess, rank, and prioritize risks (total responses: 99)</td>
<td>53</td>
<td>32</td>
<td>14</td>
</tr>
</tbody>
</table>
Principal Investigators’ Commentary

This question addresses the same issues but at a more detailed level within an organization—the level of “subcomponent, subprocess, or specific technology.” As a simple example, the “product level” may be a new passenger-vehicle design, while the “subcomponent level” might be the engine design or even the fuel-injection technology, which contributes to the innovation or competitive advantage of the manufacturer. Performing risk assessment at this level obviously requires additional resource commitment and effort, but it is an important element in many cases.

Not surprisingly, respondents indicated they perform risk assessment far less often at this level than at the overall product level. However, the results also indicated a response pattern very similar to that at the higher level with respect to the risk-assessment steps. Information assets are often identified but less often evaluated. Similarly, the potential impact of a loss and prioritization of risks receives less attention than other risk-assessment steps.

The overall lower response rate for this question implies that even fewer survey respondents perform assessments at this more detailed level, although for some respondents the concept of a subcomponent, subprocess, or specific technology level may not be applicable. For typical contemporary business organizations, however, a more specific exploration of risks contributes to more-informed business decisions and/or more-appropriate protection strategies.

Question: When significant changes in level of risk are discovered, how frequently are such changes in risk reported to management?

The results show that:

- More than 66 percent (89 of 134 respondents) to this question reported that they always or almost always report significant changes in level of risk to information assets to management.

- 28 percent (38 respondents) usually report significant changes in level of risk to information assets to management.

- 5 percent (7 respondents) seldom or never report significant changes in level of risk to information assets to management.

Principal Investigators’ Commentary

Reporting changes in risk to information assets—regardless of what caused the change—is an important responsibility. By doing so, the information can be factored into the corporate decision making process, which can influence not only immediate business transactions but also longer-term strategies. In addition, regulatory reporting requirements may apply. In these cases, failure to report certain information can result in significant liability on the part of the enterprise and the corporate officers personally.
Although more than 66 percent of the respondents indicated that they generally report such changes, less than half of all respondents said that they “always” report them. Proper reporting warrants increased attention in many organizations to both bolster their protection posture and satisfy regulatory requirements.

According to the ASIS Information Asset Protection Guideline, as well as virtually all international information-protection standards, “reporting significant changes in risk and/or asset value to appropriate levels of management on a periodic and post-event basis” is an extremely important corporate responsibility. Failure to do so could not only increase the risk to information assets but also leave the enterprise and its executives open to significant civil and criminal liabilities.

In today’s fast-paced and dynamic business environment, risk-assessment results represent a mere snapshot in time. As such, thorough assessment and reporting must be part of a regular ongoing process rather than a static event.

**Question:** Where work will be outsourced, is an on-site assessment of physical and logical security controls for the protection of proprietary information and/or trade secrets included in your organization’s due-diligence process of potential partners prior to executing a business transaction?

<table>
<thead>
<tr>
<th></th>
<th>Always/ almost always</th>
<th>Usually</th>
<th>Seldom/ never</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. On-site assessment at U.S. sites (total responses: 115)</td>
<td>72</td>
<td>25</td>
<td>18</td>
</tr>
<tr>
<td>B. On-site assessment at foreign sites (total responses: 75)</td>
<td>46</td>
<td>9</td>
<td>20</td>
</tr>
</tbody>
</table>

**Principal Investigators’ Commentary**

With the practice of outsourcing skyrocketing, especially to non-U.S. entities, the issue of due diligence and related risk assessment becomes extremely important. This question explores respondents’ practices with respect to on-site assessments of existing security controls (both physical and logical) at outsource locations. This question was included, in part, because of the propensity for some evaluators to rely on “paper and pencil” or online questionnaires for answers to questions that truly need to be verified by on-site observation. The credibility of self-reporting or questionnaires as assessment tools does not provide a sufficient level of confidence to support critical business decisions in a moderate- to high-risk environment.
The difference in the response rate between lines A and B in Table 5 may be indicative that a number of the respondents do not currently have outsourcing arrangements outside the United States. The percentage of respondents indicating that they “seldom or never” conduct on-site assessments (16 percent for U.S. sites and 27 percent for foreign sites) is a bit disconcerting. Although on-site assessments do have a cost in terms of time and money—particularly for non-U.S. sites—the benefit of verification as well as the opportunity for two-way interface with site staff is almost always worth the cost. On-site visits at foreign locations also can help clarify influencing factors related to culture, customs, language, and laws that could have a bearing on protective strategies or measures.

2. **Due Diligence**

Due diligence is the process under which prospective relationships can be evaluated with respect to the potential for harm and risk. Before entering into a business relationship with another organization, proper inquiries should be made to determine the suitability of the partnering organization and its elements or associates. Since a new partnership generally involves the sharing of proprietary information or at least some level of access to it, this process is integral to the protection of an organization’s information assets. In this series of survey questions, respondents replied on the current due-diligence processes their organizations have in place.

**Question:** *Prior to the approval of a new business venture, partnership, or outsourcing opportunity, does your organization conduct a due-diligence assessment that considers how the proposed deal could alter both the threats to and the vulnerabilities of your firm’s existing information assets?*

**Table 6.** On-Site Assessment Before Outsourcing

<table>
<thead>
<tr>
<th></th>
<th>Always/almost always</th>
<th>Usually</th>
<th>Seldom/never</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Due diligence of ventures with U.S.-owned organizations (total responses: 125)</td>
<td>76</td>
<td>29</td>
<td>20</td>
</tr>
<tr>
<td>B. Due diligence of ventures with non-U.S.-owned organizations (total responses: 79)</td>
<td>55</td>
<td>11</td>
<td>13</td>
</tr>
</tbody>
</table>
**Principal Investigators' Commentary**

Due-diligence assessments are not only a prudent assets-protection measure but also a sound business practice. They support a decision-making process in which both dynamic risk and pure risk can be addressed simultaneously. Therefore, there is little reason not to perform a thorough due-diligence assessment before any significant business transaction, agreement, or venture.

Although there is a similar drop in the response rate between Table 5 and lines A and B in Table 6 (most likely because of the absence of any non-U.S. relationships on the part of some respondents), the results are comparable. In Table 6 in both line A (regarding ventures with other U.S.-owned organizations) and line B (regarding ventures with non-U.S.-owned organizations), approximately 84 percent of the respondents perform the described due-diligence assessment “usually,” “almost always,” or “always.”

It is encouraging that many organizations are conducting due-diligence assessments that consider how any proposed business transaction could alter the threats and/or vulnerabilities to information assets. However, the survey team believes that virtually all enterprises should use such assessments as a decision-making tool. This is especially true since data presented later in this report indicates that a large portion of compromise incidents occurred as a result of the exploitation of joint ventures, outsourcing, vendor/subcontractor arrangements, or customer relationships.

**Question:** When your organization is considering working closely with another U.S.-owned organization, what is the importance of knowing if the potential partner has:

**Table 7. Non-U.S. Affiliations**

<table>
<thead>
<tr>
<th></th>
<th>Very important</th>
<th>Moderately important</th>
<th>Less or not important</th>
</tr>
</thead>
<tbody>
<tr>
<td>Close link to non-U.S.-owned firms?</td>
<td>64</td>
<td>25</td>
<td>26</td>
</tr>
<tr>
<td>(total responses: 115)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Non-U.S. citizens who have full or partial</td>
<td>65</td>
<td>23</td>
<td>27</td>
</tr>
<tr>
<td>ownership or control? (total responses: 115)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Principal Investigators' Commentary**

Part of a thorough due-diligence assessment is the gathering of information that may be considered “below the surface” or beyond the superficial. This includes research into the peripheral relationships of the proposed partner or associate. Even U.S.-based firms often have a foreign or questionable parent, subsidiary, partner, or affiliate. Knowledge of these relationships is essential in making sound business- and assets-protection decisions.
In 2005, for example, the FBI reported that the Chinese government had more than 3,000 front companies based in the United States. Firms that may outwardly appear to be a U.S. company may be owned, controlled, or partnered with organizations that represent commercial competitors or are linked to foreign government interests.

Approximately 77 percent of the respondents indicated that knowing whether a proposed partner or associate has close ties with foreign-owned firms or whether there is some degree of foreign ownership or management control within the U.S.-based company is “somewhat important,” “important,” or “very important.”

**Question:** How important are each of the following in the due-diligence processes that your organization conducts on a potential partner?

**Table 8. Due Diligence–Process Elements**

<table>
<thead>
<tr>
<th>Financial metrics and performance of the potential partner (total responses: 132)</th>
<th>Very important</th>
<th>Moderately important</th>
<th>Less or not important</th>
</tr>
</thead>
<tbody>
<tr>
<td>84</td>
<td>24</td>
<td>24</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Reputation of the potential partner including IPR violations, trade complaints, and export-control issues (total responses: 111)</th>
<th>Very important</th>
<th>Moderately important</th>
<th>Less or not important</th>
</tr>
</thead>
<tbody>
<tr>
<td>83</td>
<td>22</td>
<td>6</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Potential partner links to other firms with IPR violations, trade complaints, or export-control issues (total responses: 111)</th>
<th>Very important</th>
<th>Moderately important</th>
<th>Less or not important</th>
</tr>
</thead>
<tbody>
<tr>
<td>78</td>
<td>22</td>
<td>11</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Potential partner ties to any foreign governments (total responses: 106)</th>
<th>Very important</th>
<th>Moderately important</th>
<th>Less or not important</th>
</tr>
</thead>
<tbody>
<tr>
<td>73</td>
<td>16</td>
<td>17</td>
<td></td>
</tr>
</tbody>
</table>

**Principal investigators’ commentary**

This question asks respondents to rate the importance of various elements or factors in their due-diligence process. The results indicate a fairly consistent level of importance among all four listed factors, with a range of 64 to 75 percent of respondents rating each factor as “very important.” The lowest percentage of “very important” ratings was for “financial metrics and performance of the potential partner.” This was most likely because of respondents’ focusing primarily on assets protection in terms of their frame of mind when completing the survey. It is encouraging that the results seem to indicate a shift away from due-diligence processes that focus solely on financial considerations toward ones that include a broader array of factors including intellectual property rights (IPR) and information-protection issues.

**Question:** When a due-diligence team is formed to consider a new business venture, does the organization use subject-matter experts who are experienced in countering threats to proprietary and/or trade secret information?
Effective Due Diligence is Essential

The authors believe strongly that the following factors must be adequately researched, presented, and given significant weight during deliberations before any major business decisions are made that could affect information-asset risk:

- Financial metrics and performance of the potential partner.
- Intellectual property rights violations and protection history.
- Trade complaints.
- Export-control issues.
- Extent and nature of foreign ownership and management control.
- On-site assessment of both U.S. and foreign work locations with respect to physical, personnel, and logical security controls.

The survey results reported in this section confirm that the respondents—and presumably many business enterprises in general—are paying increased attention to due-diligence processes that include a spectrum of relevant issues. Ideally, this trend will continue to expand, and people with the appropriate expertise will increasingly be represented as a key part of the business decision-making process in the future.
3. Analysis of Incidents

Question: For calendar year 2005, please indicate the total number of suspected, unsuccessful, or successful attempts to compromise or gain unauthorized access to proprietary and/or trade secret information of your organization.

Survey data revealed:

- Fifteen respondents reported between two and 10 attempts.
- Four respondents reported between 11 and 20 attempts.
- Seven respondents reported more than 20 attempts.
- Sixteen respondents reported no known attempts.
- Two of 144 survey respondents provided no information.

Figure 4. Respondents Reporting Knowledge of Incidents

Note: Share of 42 organizations reporting.
Of 144 survey respondents, 102 reported that the information on attempts was not available. These “not available” responses may further indicate that:

- Respondent lacks access to this data.
- Respondent is reluctant to provide this data.
- Respondent has difficulty in adequately quantifying attempt data.

**Principal Investigators’ Commentary**

It is very important that organizations provide a mechanism to record, compare, and analyze attempts and that these incidents not be treated as isolated events with no apparent connection. This is especially relevant because survey respondents reported multiple attempts involving the same perpetrators and intended recipients. The ASIS IAP Guideline provides the following advice: “Maintain easily accessible documentation (or an automated database) on incidents (including allegations and suspected incidents) related to the compromise or suspected compromise of sensitive information. This is extremely valuable for Root Cause Analysis subsequent to a known compromise and for historical-trend analysis. It is also useful in determining the aggregate information that has been released over time on a particular project or initiative.”

### 3.1 U.S. OR FOREIGN ENTITIES AS BENEFICIARIES OF THE INFORMATION

**Question:** Of the total number of suspected, unsuccessful, or successful attempts to compromise or gain unauthorized access to proprietary and/or trade secret information, please break down the incidents by whom the primary beneficiary of the compromised information was intended to be.

Foreign individuals, firms, and governments were identified as the beneficiary in 357 reported incidents, more than twice the 155 incidents where the primary beneficiary was a U.S. individual or firm. Eleven respondents reported they were unsure if the beneficiaries of their incidents were U.S. or foreign entities.

**Principal Investigators’ Commentary**

It is not surprising that 11 respondents were unsure whether the beneficiaries were U.S. or foreign entities. Identifying and proving the linkage to the intended recipients has proven to be even more difficult than identifying the perpetrators in most cases. Tracking incidents will allow organizations to build a database that may help in the identification of all parties involved in the incident attempts, especially where there are repeated or ongoing attempts to acquire the information.
3.2 The Perpetrators’ Citizenship

Question: How many of the incidents involved perpetrators who:

Table 10. Citizenship of Perpetrators

<table>
<thead>
<tr>
<th>Citizenship of perpetrators</th>
<th>Number of incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>Held non-U.S. citizenship</td>
<td>238 (32 respondents)</td>
</tr>
<tr>
<td>Were born outside U.S., but were U.S. citizens at the time of the compromise</td>
<td>21 (0 respondents)</td>
</tr>
<tr>
<td>Had a common ethnic background with the country benefiting from the compromise</td>
<td>191 (30 respondents)</td>
</tr>
</tbody>
</table>

Principal Investigators’ Commentary

Likewise, it is not surprising that many of the incidents involved perpetrators with ethnic connections to the non-U.S. country benefiting from the compromise. Although many of the perpetrators volunteer their services, individuals, firms, and governments often profile and target employees of an organization for co-opting, extortion, or coercion. This is especially the case if the employees, in addition to having ethnic connections, have trusted relationships and access to sensitive and desired information. Awareness campaigns should address this issue by alerting employees that they may be profiled and targeted for participation in illegal and/or unethical attempts to acquire sensitive information.

3.3 Recipient Countries

Question: Please list the total number of incidents attributed to each intended recipient country.

Table 11. Top Four Countries in Terms of Number of Reported Incidents

<table>
<thead>
<tr>
<th>Number of respondents reporting incidents</th>
<th>Intended recipient country</th>
<th>Number of reported incidents</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>China</td>
<td>82</td>
</tr>
<tr>
<td>2</td>
<td>Russia</td>
<td>59</td>
</tr>
<tr>
<td>8</td>
<td>United States</td>
<td>51</td>
</tr>
<tr>
<td>2</td>
<td>India</td>
<td>45</td>
</tr>
</tbody>
</table>

Principal Investigators’ Commentary

Although China, Russia, and India were identified as the top intended non-U.S. recipients of compromised information, other recipient countries included (in alphabetical order): Bermuda, Canada, former Eastern Bloc nations, Iraq, Japan, the Philippines, Singapore, and the United States; respondents specifically identified the governments of China and Singapore. Organizations were unable to identify the intended recipient or benefiting country in 260 incidents.
**TARGETING OF INFORMATION ASSETS IN A GLOBAL ECONOMY**

The principal investigators recognize that a very significant amount of current and future business transactions are focused on partnering with many individuals, firms, and governments associated with countries identified as some of the intended recipients of compromised information as reported in this survey. U.S. Congressional testimony on intellectual property rights (IPR) and trade issues has indicated that up to 55 percent of U.S. companies operating in one of the foreign countries identified in this survey have been affected by IPR violations. It is most likely inevitable that your organization’s information assets will be targeted for compromise or infringement when doing business in a global market. If an organization’s information assets are unprotected or underprotected, that organization may risk loss of control, use, or ownership of some of its IPR at some point in any business relationship. The challenge is to develop a security strategy that identifies, assesses, and addresses risks, and enables business transactions in a global market.

### 3.4 TOTAL DOLLAR COST OF ALL INCIDENTS INCLUDING REACTION AND RESPONSE COSTS

**Question:** What was the total estimated cost of all suspected, unsuccessful, or successful attempts of the compromise of proprietary and trade secret information in 2005?

Because of an insufficient number of responses to this question, the survey team was unable to estimate losses. Information on financial and other impacts of losses is provided in Part B of the survey report. Among the possible reasons contributing to the low number of responses are:

- Respondent lacks access to this data.
- Respondent is reluctant to provide this data.
- Respondent has difficulty in adequately quantifying compromises and losses.

### 3.5 NUMBER OF INCIDENTS IN 2005 COMPARED TO 2004

**Question:** Was the total number of suspected, unsuccessful, and successful attempts of compromise of proprietary and trade secret information in 2005 higher or lower than 2004?

A total of 23 of 26 respondents (88 percent) reported that the total number of compromise attempts in 2005 was comparable or higher than 2004.
PRINCIPAL INVESTIGATORS’ COMMENTARY

An overwhelming 88 percent of respondents who expressed an opinion reported that compromise attempts were comparable or higher than the previous year. This response confirms the FBI reports of a dramatic increase in incident reporting and cases, especially involving countries identified by the respondents. Congressional testimony at hearings on IPR and trade issues have indicated that, although many countries contend they are addressing U.S. concerns about providing an IPR climate in their countries, there is little—if any—identifiable progress or drop in reported incidents of compromise or infringement where U.S. intellectual property rights are protected with adequate laws and enforcement.

3.6 THE COST OF INCIDENTS IN 2005 COMPARED TO 2004

QUESTION: WAS THE COST IMPACT OF SUSPECTED, UNSUCCESSFUL, AND SUCCESSFUL ATTEMPTS OF COMPROMISE OF PROPRIETARY AND TRADE SECRET INFORMATION IN 2005 HIGHER OR LOWER THAN 2004?

Eighty-one percent of respondents who expressed an opinion reported that the cost impact of proprietary information compromises was comparable or higher in 2005 than 2004.

PRINCIPAL INVESTIGATORS’ COMMENTARY

43 percent (of 123) respondents reported that this information was not available. The “not available” responses may indicate that:

- Respondent lacks access to this data.
- Respondent is reluctant to provide this data.
- Respondent has difficulty in adequately quantifying attempt data.

Cost-impact data concerning incidents is one of the most important factors that allows organizations to identify, assess, and rank risks in quantitative or qualitative terms. Without cost-impact data on attempts and potential losses, it is difficult to build a business case for the time and resources required to address identified risks in any business venture or transaction. Organizations must improve their ability to develop data that would allow cost impact of loss to be part of every risk assessment.
3.7 The Organization’s Assessment of the Impact of the Compromises

**Question:** How are the cost impacts of suspected, unsuccessful, and successful attempts of compromise of proprietary and trade secret information in 2005 rated by your organization?

Fifty-nine percent of the 29 survey respondents who expressed an opinion rated the impact of proprietary-information compromise incidents experienced in 2005 as moderate to very serious.

**Principal Investigators’ Commentary**

39 percent of 115 respondents reported that cost-impact information was not available.

Possible explanations for the “not available” responses include:

- Respondent lacks access to this data.
- Respondent is reluctant to provide this data.
- Respondent has difficulty in adequately quantifying attempt data.

When organizations develop information that allows them to rank the impact of compromise incidents and measure that impact against other business risks and impacts, their security organizations can build a business case for addressing these risks. The survey team hopes the organizations that answered “not available” would take steps to have the information available and that the estimate of impact would be part of developing a security strategy to support business goals.

3.8 Methods Employed by the Perpetrators

**Question:** Please identify all threats to proprietary and/or trade secret information including inadvertent or deliberate actions your organization experienced in 2005.
Table 12. Nature of Threats and Threat Sources Reported by Respondents

<table>
<thead>
<tr>
<th>Threats to proprietary and/or trade secret information experienced in 2005</th>
<th>All respondents</th>
<th>Respondents reporting the top ten losses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inadvertent actions by current or former employees</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>During oral seminar presentations</td>
<td>21</td>
<td>3</td>
</tr>
<tr>
<td>Via written material, publications, or handouts</td>
<td>21</td>
<td>2</td>
</tr>
<tr>
<td>Via electronically misdirected fax or e-mail</td>
<td>23</td>
<td>4</td>
</tr>
<tr>
<td>Via visual observation of written material, desktops, white boards, computer screens, etc.</td>
<td>19</td>
<td>3</td>
</tr>
<tr>
<td><strong>Deliberate actions by current or former employees</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deliberate disclosure to unauthorized parties</td>
<td>19</td>
<td>5</td>
</tr>
<tr>
<td>Unauthorized electronic access/penetration of information systems</td>
<td>18</td>
<td>4</td>
</tr>
<tr>
<td>Unauthorized physical access to information</td>
<td>21</td>
<td>5</td>
</tr>
<tr>
<td><strong>Deliberate actions by individuals/entities in trusted relationships (other than employee relationships)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploitation of joint ventures</td>
<td>10</td>
<td>1</td>
</tr>
<tr>
<td>Exploitation of vendor, subcontractor, or outsourced provider relationships</td>
<td>16</td>
<td>3</td>
</tr>
<tr>
<td>Exploitation of customer relationships</td>
<td>14</td>
<td>3</td>
</tr>
<tr>
<td><strong>Deliberate actions or activities by outsiders (those without a trusted relationship)</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Open-source collection of public information</td>
<td>20</td>
<td>3</td>
</tr>
<tr>
<td>Data mining or software-driven collection and analysis of open-source data</td>
<td>10</td>
<td>3</td>
</tr>
<tr>
<td>Exploitive social engineering techniques (manipulation of human tendencies such as misrepresentation to obtain passwords, false job interviews, visits to facilities and tradeshows, etc.)</td>
<td>14</td>
<td>5</td>
</tr>
<tr>
<td>Hiring away employees and placing them in positions where they must use trade secrets that they are obligated to protect to do their new job</td>
<td>13</td>
<td>3</td>
</tr>
<tr>
<td>Extortion or coercion of an unwilling trusted insider by an outsider</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Co-opting of an employee or former employee</td>
<td>12</td>
<td>3</td>
</tr>
<tr>
<td>Co-opting of a company vendor, subcontractor, or outsourced provider employee</td>
<td>9</td>
<td>2</td>
</tr>
<tr>
<td>Targeting of off-site meeting or conference</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>Electronic eavesdropping, wiretapping, or interception of communications</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>Theft of hard-copy information, samples, or prototypes; dumpster diving/theft of trash</td>
<td>10</td>
<td>2</td>
</tr>
<tr>
<td>Theft of proprietary source code/computer programs</td>
<td>6</td>
<td>0</td>
</tr>
<tr>
<td>Intentional unauthorized access/penetration of information systems</td>
<td>13</td>
<td>6</td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other deliberate or inadvertent action/threat</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: This was a multipart question and responses are reported using a multi-section table organized by the nature of the reported threat.
PRINCIPAL INVESTIGATORS’ COMMENTARY

The largest threats to proprietary information are from those with a trusted relationship with the organization—current and former employees and those partners, outsourced providers, and customers with a trusted relationship.

1. Inadvertent actions by current or former employees

The inadvertent actions of current and former employees were identified as a major threat to proprietary information as follows:

- Oral seminar presentations or at an exhibit booth.
- Written materials such as publications and handouts.
- Electronically misdirected fax and/or e-mail.
- Visual observation of written material on desktops, white boards, or computer screens.

Any or all of these inadvertent actions may allow others to gain access to sensitive information using methodologies as simple as visual observation and as technically proficient as data mining to assemble a mosaic of an organization’s sensitive information with little or no risk of discovery or consequences.

2. Deliberate actions by current or former employees

The deliberate actions of current and former employees continue to be a primary threat to proprietary information. Such actions include:

- Unauthorized physical access to information—the deliberate action most identified by survey respondents as being a threat.
- Deliberate disclosure to unauthorized parties—identified by slightly fewer respondents than the action above.
- Unauthorized electronic access/penetration of information systems. This continues to be an ongoing issue given that most information at some point is created, transferred, and/or stored electronically. In this survey, however, this issue was identified as third out of three types of deliberate actions of employees involved in incidents experienced by responding organizations in 2005.
3. Deliberate actions by individuals/entities in trusted relationships other than employee relationships

- Exploitation of trusted relationships, including vendor-client relationships, subcontractor/outsourced provider relationships, joint ventures, and customer relationships are threats to proprietary information. This exploitation is potentially even more harmful when there is collusion between employees and partners to target information for compromise.

- The exploitation risk of trusted relationships in joint ventures and outsourced provider and customer relationships has been highlighted in Congressional hearings on trade and IPR issues and in statements by intelligence and law enforcement sources as one of the growing challenges with globalization and outsourcing. To ensure ownership and control of IPR during and after the transaction, these risks need to be considered as part of any due diligence before engaging in any deal or transaction involving sensitive information. Organizations should consider severely limiting exposure of sensitive information in any transaction where due diligence indicates that the potential partner or country has a poor track record concerning IPR, related issues in trade, and export-control violations or where there are indications of previous attempts to acquire the technology or business information through illegal or unethical means.

4. Deliberate actions or activities by outsiders—those without a trusted relationship

- Data mining and software-driven collection of open-source data and public information join social engineering as a significant threat.

- The practice of hiring away employees and placing them in a position where they must use trade secrets they are obligated to protect to do their new job is very prevalent. It can be addressed, in part, through agreements, notification, and litigation if necessary, but prevention starts with a risk assessment that identifies individuals needing such agreements.

- Co-opting, coercion, and extortion are often factors in ethnic profiling and targeting of employees by individuals, firms, and countries with the same ethnic background as the employee of the targeted organization. Security-awareness briefings of employees, including information on ethnic profiling and targeting, can educate employees that they may be targeted. Respondents reported that these were factors in a number of incidents.
Update Risk-Assessment Models and Aligning Security Strategies to Address Business Goals

Survey respondents have identified each of the methods of loss/risk listed in the survey as a factor in multiple compromise incidents. Many of these methods of loss/risks are not fully addressed in many current risk-assessment models that are primarily IT-based and do not consider all threats to an organization’s information assets and intellectual property rights as part of a comprehensive information asset protection (IAP) policy.

It is only by performing a risk assessment that is product-, technology-, and transaction-specific that your organization will be able to develop a risk-based approach and an IAP security strategy enabling business transactions and success in a global economy.

Part B: Respondents’ Single-Most-Significant Incident

The questions in Part B of the survey were designed to elicit responses that would allow the principal investigators to “develop a more comprehensive picture regarding the various ways in which information compromises and/or losses can impact a business in the context of today’s increasingly global and intertwined business (transaction) environments.”

Analysis of the survey results as a whole—and particularly Part B—will also lead to designing more comprehensive (holistic) risk-assessment protocols and due-diligence processes to mitigate the growing, and sometimes inevitable, risks increasingly common to global business ventures.

Questions in Part B asked respondents to focus solely on the “single-most-significant incident” during 2005 in terms of dollar loss or adverse impact on their organizations. Responses suggest that a significant number of respondents learned that they need enterprisewide collaboration and monitoring (for instance, of financials, valuation, and so forth) to actually determine the impact of information compromises and/or losses. Analysis of the results also suggests that respondents are more likely to have finely-tuned processes and procedures for assessing and addressing risks to physical assets than to their intangible or information-based assets.

Within the U.S. government, particularly in the Department of Defense (DoD), there are well-established procedures for conducting “damage assessments” following a known breach or compromise. These procedures assist in identifying the damage caused by the incident in terms of intelligence operations, sources and methods, strategic and tactical advantage, and operational effectiveness. In the authors’ views, it is prudent for organizations to take a page from DoD’s “damage assessment” approach and devote more time and effort to assessing (quantifying) and framing (qualifying) information compromises and losses relative to:
• The loss of competitive advantages.
• Devaluation of image and goodwill.
• Reduced returns and profitability.
• The loss of core business technologies.
• Weakened U.S. economic and/or strategic military advantages.
• Potential for increased vulnerability to terrorist and extremist threats.

In addition, the survey’s analysis suggests that organizations need to develop (or have in place) higher levels of awareness, alertness, and monitoring capability to counter the effects of these actions in closer, perhaps real time, proximity to a compromise.

**Question:** This question asked for detailed information on the respondent’s single-most-significant targeting incident. Specifically, what is known about the perpetrator and recipient of the compromised information?

Table 13. Single-Most-Significant Loss Incident
Citizenship or Country of the Perpetrator and Recipient

<table>
<thead>
<tr>
<th>Citizenship or country indicated</th>
<th>Perpetrator</th>
<th>Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>In alphabetical order</td>
<td>Canada, China, India, Mexico, Russia, Singapore, Sweden, Taiwan, United Kingdom, United States</td>
<td>China, Israel, Russia, Taiwan, United States</td>
</tr>
<tr>
<td>Other responses</td>
<td>Cannot disclose</td>
<td>Foreign operations of a U.S. subcontractor</td>
</tr>
<tr>
<td></td>
<td>Unknown</td>
<td>Unknown</td>
</tr>
</tbody>
</table>
Table 14. Single-Most-Significant Loss Incident  
Relationship of the Perpetrator and Recipient to the Targeted-Asset Owner

<table>
<thead>
<tr>
<th>Relationship of the Perpetrator and Recipient of the Compromised Information</th>
<th>Perpetrator</th>
<th>Recipient</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current employee <em>with</em> direct access to the information</td>
<td>20</td>
<td>7</td>
</tr>
<tr>
<td>Current employee <em>without</em> direct access to the information</td>
<td>4</td>
<td>5</td>
</tr>
<tr>
<td>Former employee(s)</td>
<td>9</td>
<td>8</td>
</tr>
<tr>
<td>U.S. subcontractor/outsourced provider</td>
<td>6</td>
<td>2</td>
</tr>
<tr>
<td>U.S. domestic competitor</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>U.S. domestic partner</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Foreign subcontractor/outsourced provider</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Foreign competitor</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Foreign partner</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Foreign government</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Computer hacker</td>
<td>11</td>
<td>4</td>
</tr>
<tr>
<td>Existing or potential customer</td>
<td>4</td>
<td>2</td>
</tr>
<tr>
<td>Information broker</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>3</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: The numbers listed are the number of respondents to Part B of the survey who indicated a specific "relationship" of the perpetrator and recipient of the compromised information in their single-most-significant loss incident. Respondents who listed "unknown" or "not available" were not included in the table.

**Principal Investigators’ Commentary**

On the basis of information presented in response to this question, it is apparent that information-asset owners should not limit their concern to those countries that are commonly thought to represent high-risk environments, but also should carefully assess the nature of business risks in all countries where they operate or have business relations. The data also reinforces the notion that "insiders" represent a very significant source of the threat to information assets.
**Question:** When the compromise incident occurred, in what form was the targeted information?

**Figure 5.** Single-Most-Significant Loss Incident Form of Information When it was Compromised

Note: Results are based on 58 respondents.

**Principal investigators’ commentary**

Although most respondents reported that the targeted information was in electronic (data) form when the compromise occurred, another large segment of respondents reported they “did not know” what form the targeted information was in at the time of the compromise.

It is probably safe to assume that most information is—at some point—developed, stored, and disseminated with the aid of electronic means; that is, computers and IT systems. The intent of this question, however, was to shed light on other formats in which information not only exists but is vulnerable to compromise and loss. It is important to acknowledge that not all of an organization’s valuable proprietary information lies solely in electronically formatted data. Therefore, it is important that information safeguards be relevant and sufficiently flexible to address vulnerabilities irrespective of format.
**QUESTION: WHERE WAS THE INFORMATION PHYSICALLY LOCATED WHEN IT WAS COMPROMISED?**

**PRINCIPAL INVESTIGATORS’ COMMENTARY**

Of the 46 respondents who provided data about the physical location, 42 (91 percent) indicated that the information was located in the United States.

Knowing the physical location of an organization’s information assets is important and necessary for several reasons. First, the laws and legal remedies that may be applied to address a compromise and/or loss may vary considerably from country to country (for example, China, the United States, Brazil), or between trade-governing bodies such as the EU, World Trade Organization, or Trade Related Aspects of Intellectual Property Rights.

Second, when information compromise occurs, economic- and competitive-advantage losses are felt very quickly in today’s environment. It is, therefore, no longer sufficient for practitioners to merely know that valuable and proprietary information such as trade secrets, intellectual property, or intangible assets exist in their organization and to have safeguards in place, but they must also have the means to routinely monitor their location and status.

**QUESTION: WHAT TYPE OF PROPRIETARY AND/OR TRADE SECRET INFORMATION WAS COMPROMISED?**

Table 15. Single-Most-Significant Loss Incident

<table>
<thead>
<tr>
<th>Type of Information Asset</th>
<th>Respondents (#)</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic research/R&amp;D</td>
<td>11</td>
<td>20</td>
</tr>
<tr>
<td>Manufacturing process</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Unannounced product specifications</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Product supply-chain information</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Customer-related information</td>
<td>14</td>
<td>26</td>
</tr>
<tr>
<td>Strategic business planning</td>
<td>9</td>
<td>16</td>
</tr>
<tr>
<td>Marketing plans</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>Source code</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>Other</td>
<td>12</td>
<td>22</td>
</tr>
</tbody>
</table>

*Note: Percentage of responses by type of information for those 55 respondents with knowledge of the information and willing to disclose it. ("Unknown" and "not available" answers omitted.)*
**Principal Investigators’ Commentary**

A majority of the respondents reported that information on the type of proprietary/trade secret information compromised was not available. The remainder of the respondents reported that the compromised information fell into categories such as:

- Customer-related information that included customer identification, preferences, and pricing.
- Basic research and R&D information.
- Strategic business plans.
- Manufacturing-process information.
- Source-code products.
- Unannounced product specifications, products supply-chain information, and/or marketing plans.

There is a growing necessity for businesses to continually identify and assess where valuable and proprietary information originates and lies within their organization. Lacking this information, the application of conventional information safeguards that do not include holistic and ongoing risk-assessment and due-diligence practices are unlikely to provide the level of protection warranted today and expected in the future.

**Figure 6. Single-Most-Significant Loss Incident**

*Type of Information Asset*

- Customer-related information 26%
- Basic research/R&D 20%
- Strategic business planning 16%
- Other 22%
- Source code 5%
- Marketing plans 2%
- Manufacturing process 5%
- Unannounced product specifications 2%
- Product supply chain information 2%
**Question:** What type of business transaction were you engaged in when this compromise occurred?

**Principal investigators’ commentary**

It is an economic fact today that as much as 75 percent of most organizations' value and sources of revenue (or wealth) creation are in intangible assets, intellectual property, and proprietary competitive advantages. The principal investigators also recognize that, for a growing percentage of business transactions, those same assets are most likely to be part of the deal. That is, they are likely to be bought, sold, disseminated, shared, licensed, or traded as part of the transaction.

These facts prompted the principal investigators to design a question which asked respondents to identify the “type of business transaction their organization was engaged in when this compromise occurred.” Interestingly, a majority of the respondents reported that “no business transaction was involved when the compromise occurred,” followed closely by “not available” responses. Other respondents reported joint ventures, product sales, subcontracting, outsourcing, coproduction, software design, licensing, and hardware design as being the type of business transaction in which a compromise occurred.

**Question:** What is the financial impact of the compromise?

(As used here, “financial impact” is defined as: the current or anticipated direct and indirect financial costs including costs related to reaction and response to the incident.)

**Principal investigators’ commentary**

This question goes to the heart of Part B’s overall focus by asking respondents to identify “the financial impact of the single-most-significant compromise” incurred by their organization. Interestingly, a significant majority of the respondents reported that this information was not available, with another segment reporting there was relatively little or no financial impact.
**Question:** What specific business impacts occurred or are anticipated as a result of this incident?

Table 16. Single-Most-Significant Loss Incident Business Impact of Loss

<table>
<thead>
<tr>
<th>Business Impact of Loss</th>
<th>Percentage (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of competitive advantage in one product/service</td>
<td>24</td>
</tr>
<tr>
<td>Loss of competitive advantage in multiple products/services</td>
<td>10</td>
</tr>
<tr>
<td>Loss of core business technology or process</td>
<td>10</td>
</tr>
<tr>
<td>Loss of company reputation, image, and/or goodwill</td>
<td>29</td>
</tr>
<tr>
<td>Reduced projected/anticipated returns or profitability</td>
<td>14</td>
</tr>
<tr>
<td>Loss of information or technology that may weaken U.S. economic and/or strategic military advantage</td>
<td>6</td>
</tr>
<tr>
<td>Loss of information that may make the organization more vulnerable to terrorist threats</td>
<td>6</td>
</tr>
<tr>
<td>Loss of information or prototypes that may facilitate product counterfeiting</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: Percentage of the 77 responses to this question (other than “not available”). The instructions for this question indicated that respondents should “check all that apply.”

**Principal investigators’ commentary**

For purposes of analysis, it is valuable to compare and contrast the responses to the previous two questions. Again, it is important to keep in mind that each Part B question asked respondents to focus solely on “the dollar impact/loss of their organization’s single-most-significant incident.”

As noted in Table 16, respondents were asked about the types of business impacts that resulted from the incident or loss event. A significant number of the respondents reported that specific business impact information was not available. However, other respondents were able to specifically describe or qualify the business impacts as shown in the table. Interestingly, the impacts that were cited most frequently were “loss of reputation, image, or goodwill” and “loss of competitive advantage in a single product or service line.” These responses highlight the tremendous importance of intangible assets such as those mentioned. Another impact that was listed frequently was a more tangible issue: the reduction of “projected/anticipated returns or profitability.”

The principal investigators suggest that, while it is a good first step to qualify a loss in terms of these impact “types,” it is also extremely important to establish a mechanism to quantify losses as quickly and accurately as possible. Quantifying past and potential organizationwide financial impacts of information losses is admittedly a challenging task. It is, however, a critical element in making a convincing business case for appropriate assessment mechanisms, protective strategies, and input to the decision-making process.
**Question:** What actions did your organization initiate or expect to initiate as a result of this compromise?

**Principal investigators’ commentary**

Respondents demonstrated a keen awareness for the various actions their organization took in responding to this pivotal question. Most respondents reported their organization: investigated the compromise, reassessed its security controls, and/or performed a formal damage assessment. Still, there were a sizable number of respondents who reported that this information was “not available.”

In addition, smaller numbers of respondents reported that they revised their due-diligence/risk-assessment process and/or brought civil action. Other responses were instructive as well: their organization withdrew from the business transaction, filed criminal complaints, redesigned its product offering, reduced its business commitment to that country, filed a trade complaint, or reduced plans for expansion.

No respondents, however, reported that they “restated financials” as a result of this compromise. In light of the growing global emphasis on valuating intangible assets to accommodate both the Sarbanes-Oxley Act and the Financial Accounting Standards Board mandates to report materiality breaches and losses, the principal investigators found it puzzling that “restated financials” was not listed by any respondents.

**Question:** How long do you estimate it will take for the commercial or government entity acquiring your compromised information to assimilate it and produce a comparable product or service using the acquired technology?

**Principal investigators’ commentary**

Although the responses to this question were instructive overall, the overwhelming majority of respondents reported that this information was not available, the question was not applicable to the type of information compromised, or that they were unable to calculate a specific time frame. Figure 7 presents the results for those providing substantive responses.
Figure 7. Single-Most-Significant Loss Incident Percentage of Respondents by Estimated Time for End User To Assimilate and Apply the Acquired Information

Note: Percentage of the 12 respondents who answered the question with other than 'not available,' 'not applicable,' or 'unable to calculate.'
The responses to this question indicate that, in many cases, it is extremely difficult to determine how quickly an adversary will be able to assimilate and apply information he or she has acquired. Although a few respondents who made an estimate believed that their compromised information assets will be able to be exploited very quickly (in 90 days or less), a larger percentage fall into the categories of 90 days to one year and three to five years. The survey team believes that a major factor in the time required to assimilate and apply information is based on the specific type of information or technology involved in the compromise or the industry affected.

**MONITORING TODAY’S DYNAMIC RISKS**

Risks to information assets (for example, through compromise, misappropriation, infringement, or counterfeiting) are asymmetric and change rapidly—oftentimes instantaneously—and:

- **Stifle an organization’s competitive/economic momentum.**
- **Undermine a transaction or strategic business plan.**
- **Erode (literally evaporate) an asset’s value and projected (future) profitability.**

In the pre-Internet era, when information compromises occurred, a common business continuity strategy was to try to contain the damages or extent of the loss. Today, however, although a containment strategy may be admirable, it does not reflect the reality of “speed” at which valuable information-based assets can be acquired and disseminated globally. Once the asset is gone or compromised, containment—in the conventional sense—is seldom a realistic option.

Today, the value and competitive advantages routinely found in an organization’s information assets—many of which may be targeted for possible compromise—can be quickly discerned and extracted, in whole or part, and instantaneously distributed to a growing labyrinth of skilled and organized information brokers, counterfeitors, and/or economic-competitive adversaries. The consequences in terms of lost economic/competitive advantage can be extremely quick and long lasting.
ABOUT THE PRINCIPAL INVESTIGATORS

PROJECT DIRECTOR AND LEAD INVESTIGATOR

Richard J. Heffernan, CPP, CISM  
President, R. J. Heffernan & Associates, Inc.  
Guilford, Connecticut

Mr. Heffernan is an independent consultant, advisor, and strategist heading a consulting practice that assists organizations in performing assessments to identify, assess, and manage risks to tangible and intangible assets including intellectual property, proprietary competitive advantages, and other organizational assets.

Early in his more than 30-year career, Mr. Heffernan cofounded one of the leading companies that specialized in countering technical and other means of acquisition of information assets, where he was responsible for developing and directing the technical surveillance countermeasures (TSCM) services and information security consulting practice for government and Fortune 1000 clients. In 1988, Mr. Heffernan founded R. J. Heffernan & Associates, Inc., a consulting practice that assists organizations in assessing and addressing risks and enabling business transactions in a global environment.

Mr. Heffernan has been a member of the ASIS Information Asset Protection (IAP) Council since 1986, including five terms as council chairman, and serves as the 2007 IAP Council vice chairman. He is a contributing author for the Protection of Assets Manual, published by ASIS, and vice chairman of the ASIS Information Asset Protection (IAP) Guideline Committee. He served as an instructor for both of the ASIS Asset Protection Course I and II. He provided expert testimony at the request of ASIS at the U.S. House Judiciary Committee hearings concerning the extent of economic espionage targeting, information-security best practices, and the need for U.S. trade-secret legislation.

In addition, Mr. Heffernan is a recipient of the ASIS President’s Award, as well as a citation from the FBI Director for his work to help U.S. businesses to identify, assess, and address threats to information assets. He served as a member of the industry council of the National Counterintelligence Center (NACIC) and as a consultant and lecturer for the National Security Division of the FBI.

Mr. Heffernan is a frequent media contributor often quoted in leading business publications, as well as a frequent guest on programs including CNBC Power Lunch and The NewsHour with Jim Lehrer.
OTHER PRINCIPAL INVESTIGATORS

Michael D. Moberly
President, Knowledge Protection Strategies
Memphis, Tennessee

Mr. Moberly is the founder and president of Knowledge Protection Strategies, a business-transactions consulting firm that utilizes value-risk-forensic assessments and due diligence to protect, preserve, and monitor intellectual property, intangible assets, and proprietary competitive advantages in mergers and acquisitions, corporate-university research alliances, early stage/venture capital, and research and development programs. Previously, he served in academia and is a past chair of the ASIS Council on Academic Programs in Colleges and Universities. A longtime member of ASIS, he is the 2007 chairman of the ASIS Information Asset Protection Council. Mr. Moberly speaks regularly throughout the United States on issues pertaining to the protection of intangible assets and corporate competitive advantage.

Kevin E. Peterson, CPP
Principal Consultant, Innovative Protection Solutions LLC
Herndon, Virginia

Mr. Peterson serves as an independent consultant in security-risk management and information protection for commercial and government clients. He has more than 28 years of experience including a career in the United States Air Force, where he managed counter-intelligence programs and efforts to protect militarily critical technologies. Following his military career, Mr. Peterson worked in the defense industry protecting sensitive research and development programs, leading vulnerability assessments, and implementing information-assurance and critical infrastructure-protection initiatives. In June 2000, he established Innovative Protection Solutions as a full-time consulting practice. Mr. Peterson is also an adjunct faculty member at Webster University, teaching in its graduate-level Business & Organizational Security Management program, both in the classroom and online.

Within ASIS, Mr. Peterson has served as a vice chairman of the Information Asset Protection Council from 2001-2007. In addition, he is a member of the Council on Academic Programs in Colleges and Universities, past regional vice president, and past chapter chairman. Mr. Peterson recently chaired the ASIS Information Asset Protection Guideline Committee and is a contributing author to the Protection of Assets Manual. He also served as a member of the Board of Directors for the Operations Security Professionals Society (OPS) from 2000 until 2007.
Larry Runyon, CPP  
Director of Counterintelligence, Pacific Northwest National Laboratory  
Richland, Washington

Mr. Runyon has more than 28 years of professional experience in conducting and managing criminal and counterintelligence/counterespionage investigations, operations, and programs in the United States and overseas. He possesses extensive experience in developing and managing effective security and counterintelligence programs directed at protecting classified and sensitive information relating to technology research and business development initiatives.

He has been board certified as a Certified Protection Professional since 1987 and has served in a number of leadership roles within ASIS to include service as the 2005 and 2006 chairman of the ASIS Information Asset Protection Council. He is a graduate of the University of Nebraska at Omaha and is the recipient of four security-related U.S. patents.
Glossary of Terms

The following terminology and definitions were used in the survey and this report.

**Business impact of incidents** - Financial or other current or anticipated impacts to the organization from the suspected, unsuccessful, or successful compromise of proprietary and trade-secret information.

**Compromise incidents** - Suspected, unsuccessful, or successful attempts of the compromise of proprietary and trade-secret information.

**Common ethnic background** - Used to specifically indicate an identified commonality between the background of the perpetrator and recipient relating to national or cultural background.

**Export control** - U.S. government controls on the export, sharing, or exposure of certain types of information deemed critical to U.S. national interests to individuals and entities other than the United States.

**Information assets** - Proprietary information, trade secrets, trademarks, patents, and copyrights including the information systems hardware, software, and networks on which they are generated, stored, or shared.

**Intellectual property rights (IPR)** - Legal rights or protections conferred to an owner by proprietary information, trade secret, trademark, copyright, or patent status.

**Likelihood of occurrence of threats** - A determination of the probability of a specific threat action to occur.

**Perpetrator(s)** - The individual or individuals that committed the compromise incident.

**Proprietary information** - There is no general definition for proprietary information in the U.S. legal code. The Federal Acquisition Regulation (48 CFR 27.402 Policy) does, however, provide a definition: “A property right or other valid economic interest in data resulting from private investment. Protection of such data from unauthorized use and disclosure is necessary to prevent the compromise of such property right or economic interest.”

**Risk** - A security risk is the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset.

**Threat** - A deliberate or inadvertent action, which has the potential to cause an unwanted incident where harm may result.
**Trade secret** - “All forms and types of financial, business, scientific, technical, economic, or engineering information, including plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing if (A) the owner thereof has taken reasonable measures to keep such information secret; and (B) the information derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable through proper means by the public.” The Economic Espionage Act of 1996 (USC 1831, 1832).

**Vulnerabilities** - Weaknesses or organizational practices that may be exploited by a threat.
**ASIS International**

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 35,000 members worldwide. 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 and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, governmental entities, and the general public. 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 advanced and improved security performance. For more information, visit [www.asisonline.org](http://www.asisonline.org).

**ASIS Foundation**

The ASIS International Foundation, a 501(c) (3) charitable organization, provides funding and manages endowments for a wide range of academic, strategic, and professional development activities. The purpose of the Foundation is to enhance the security profession worldwide by establishing, developing, delivering, and promoting programs that advance security through education, research, and training. The Foundation, through the awarding of scholarships, ensures that those pursuing a career in security management are able to realize the highest academic achievements. Support for the Foundation is achieved through financial contributions from individuals, chapters, and companies employing ASIS members, and corporations with an interest in security.