Competitive Intelligence: Is My company at Risk?

William Andrew Staszewski
University of Tennessee-Knoxville

Follow this and additional works at: https://trace.tennessee.edu/utk_chanhonoproj

Recommended Citation
Appendix D - UNIVERSITY HONORS PROGRAM
SENIOR PROJECT - APPROVAL

Name: __William Staszewski______________________________

College: Business Administration Department: Accounting

Faculty Mentor: __Dr. Harold Roth__________________________

PROJECT TITLE: Information Protection [Competitive Intelligence: How Is My Company At Risk?]

I have reviewed this completed senior honors thesis with this student and certify that it is a project commensurate with honors level undergraduate research in this field.

Signed: __Harold P. Roth_____________________________, Faculty Mentor

Date: May 2, 2001

Comments (Optional):
Appendix C - UNIVERSITY HONORS PROGRAM
SENIOR PROJECT - PROSPECTUS

Name: William Staszewski
College: Business Admin. Department: Accounting
Faculty Mentor: Dr. Harold Roth

PROJECT TITLE: Competitive Intelligence: How Is My Company At Risk?

PROJECT DESCRIPTION (Attach not more than one additional page, if necessary):

The focus of this project is the development of a generic audit program through which a business can evaluate areas of possible exposure to competitive intelligence threats. In addition to risk evaluation guidelines, an overview of Competitive Intelligence will be included.

Projected completion date: 4/16/01

Signed: [Signature]

I have discussed this research proposal with this student and agree to serve in an advisory role, as faculty mentor, and to certify the acceptability of the completed project.

Signed: Dr. Harold Roth, Faculty Mentor

Date: February 9, 2001

Return this completed form to The University Honors Program, F101 Melrose Hall, 974-7875, not later than the end of your 3rd year in residence.
Information Protection

Competitive Intelligence:
Is My Company At Risk?

William Staszewski

Submitted in partial fulfillment of
University Honors 458

May 2, 2001
## Contents

Overview
- Managing Information 2
- Information Loss 3
- Relevant Fields of Study 4
- Examples of Information Compromise 5
- Types of Sensitive Information 6
- Protection Programs 7
- Economic Espionage Act 10
- Summary 11

Audit Program 12

References 22
End Notes 23

Appendices
- A. ASIS/PWC: Trends in Proprietary Information Loss 24
- B. CI Is and Is Not 43
- C. SCIP: CI profession overview 47
- D. Joint Venture Management of Information 60
- E. SCIP: EEA Analysis 64
- F. Internet Resources 76
Information Protection

Since the advent of the modern "information age," it has become increasingly important for business professionals to recognize the value of information and the need for active protection of valuable information in organizations. This paper seeks to develop a general audit program to help organizations evaluate whether their valuable information is protected. While far from an exhaustive analysis of the subject, the paper brings together a variety of informational sources and presents the key ideas in three main sections. These sections include a general overview of information protection, the actual information protection audit program, and six appendices attached at the end of the paper.

Managing Information

Because information is a valuable resource, it would be ideal to manage information in much the same way that other corporate resources are managed. This, however, has not been the case in recent years. Despite estimates that seventy percent or more of the market value of a typical U.S. company resides in intellectual property assets (IP), information protection is not a security priority of most companies. In fact, formalized valuation and tracking procedures typically do not exist for these assets, and since the value of IP assets is not well established, they are often not well protected (PWC/ASIS p. 4).

Inadequate protection of valuable assets is a business risk, especially if business risk is defined as anything that threatens achievement of business objectives. On the positive side, the majority of business risks are internal, can be easily analyzed, and can be responded to by a company. But in order to increase control over a business risk, a company must first recognize that a problem exists. From the perspective of this paper,
the problem is inadequate information protection leading to information loss and compromise.

**Information Loss**

In 1999, *Fortune 1000* companies sustained losses of more than $45 billion from thefts of their proprietary information (PWC/ASIS p. 3). When the data are compared with prior years, they show that incidents of theft are rising. A 1995 survey of 325 companies reported 32 cases of theft of intellectual information per month in 1995 (losses amounted to $5.1 billion). This was more than three times the rate found in a similar survey in 1992 (Fialka p. 15). Increasing occurrences of information loss are partly due to the unique characteristics of information and to deficient security measures. Unlike physical assets, like buildings or traditional inventory, information can be in more than one place. "Individuals no longer have to physically steal a product, they can simply download information or transmit it electronically to a single accomplice or to tens of thousands of people in an instant – and they can do so with total anonymity." Sensitive information can be lost merely by allowing access to it.

See Appendix A for *Trends in Proprietary Information Loss* prepared by the American Society for Industrial Security and PricewaterhouseCoopers. This appendix provides the results and summary of a 1999 survey showing the extent of proprietary information loss and the lack of appropriate information security measures in corporations. While the summary is repeatedly cited below, the full text is contained in an appendix for a more thorough review.
Relevant Fields of Study

While researching information protection, it is possible to encounter many specific fields of study connecting to the general topic. Competitive Intelligence (CI) and Intellectual Property (IP) are two such fields related to the protection of sensitive, proprietary, or confidential information. These fields warrant short definitions.

Competitive Intelligence can be defined as “information relevant to strategy formulation regarding the environmental context within which the firm competes” (Miller, A. p. 97), but the Society for Competitive Intelligence Professionals thoroughly describes CI as “a systematic and ethical program for gathering and analyzing information about your competitors’ activities and general business trends to further your own company’s goals.”

For further information on CI, see Appendix B and Appendix C. Appendix B contains a list of ten things CI is and is not; this list was written by Leonard Fuld, a pioneer in the CI field. Appendix C contains an overview of the CI profession compiled by the Society for Competitive Intelligence Professionals (SCIP) in the form of PowerPoint slides.

The term Intellectual Property usually refers to patents, trademarks, copyrights, and trade secrets or know-how (Smith & Parr p. 89). Discussions of IP and intellectual property rights (IPRs) usually involve applicable legal and judicial systems. In regard to information protection, both CI and IP resources provide various countermeasures and defensive tactics that can be utilized in the protection of confidential information.

Other fields of study related to information protection include economic intelligence, national security, asset protection, economic espionage, and
counterintelligence. A list of internet links to sites covering these fields can be found in Appendix F.

**Examples of Information Compromise**

The term “information compromise” refers to any incident in which valuable information has reached unauthorized personnel. Information compromise includes any thefts and misappropriation of proprietary information. While statistics on information compromise were presented above in the “Information Loss” section, the following are examples of information compromise (Dutka pp. 295-297):

- The French intelligence placed agents inside French offices of IBM and Texas Instruments to steal trade secrets.

- A CIA document provides case studies of France spying on U.S. military contractors and high-tech firms. The French exposed four CIA spies attempting to uncover French positions on world trade talks.

- A company publicly announced the location of an off-site planning meeting involving high-level executives. A competitor reserved an adjacent room and installed bugging devices to record the proceedings. The competitor created better-quality documentation of the session than the company conducting the meeting.

- An employee of a high-tech company, undaunted by a security system that prevented unauthorized downloading of information, videotaped confidential documents from the computer screen.

- The president of Blue Cross & Blue Shield of Ohio, engaged in a power struggle to control the company, found that his company telephone was tapped.

- A retired Kodak employee pleaded guilty to offering to sell secret company information. The former employee stole blueprints, cost breakdowns, manufacturing reports, analytical studies, and drawings.

- An engineer offered to sell his former employer confidential plans that he had stolen from the company. The engineer was subsequently arrested by the FBI. During the ensuing trial, the defense demonstrated that the company’s employees did not typically follow procedures to secure information. The court ruled that the company had forfeited its claim to classify the information as a trade secret because of its failure to protect the information.
In a press release dated March 21, 2001, it was reported that a contract food services employee at the Purchase, NY headquarters of MasterCard International was arrested for stealing various confidential documents from the credit card company. The defendant allegedly offered to sell sensitive and proprietary information to Visa International and to record high-level meetings within MasterCard if Visa paid and provided him with recording equipment.6

Types of Sensitive Information

The categories listed below may help identify the general types of assets that might be considered sensitive in a U.S. company. Asset information warranting protection may include location, size or capacity, investment, age, etc. The five basic categories include the following:7

- **People**
  - Government personnel
  - Contractors
  - Military personnel
  - Contractors
  - Consultants
  - Specialized employees
  - Suppliers or customers

- **Activities/Operations**
  - Intelligence collection/analysis
  - Sensitive movement of operations/personnel/property
  - Conduct of sensitive training
  - Communications/networking
  - RDT&E and sensitive technology
  - Production of sensitive technology
  - Protection of nuclear/chemical/biological materials
  - Protection of weapons, explosives, and equipment

- **Information**
  - Classified
  - Sensitive compartmented information
  - Top Secret
  - Secret
  - Confidential
  - System designs
  - Intellectual property
  - Patents
  - System capabilities/vulnerabilities
  - Sensitive methods
Protection Programs

Various models for evaluating and protecting informational assets have been developed in response to threats of information compromise. While these general programs sometimes use differing terminology, they are often conceptually similar. Operations Security (OPSEC), originally designed for government use, is one of the typical general information protection programs in security literature and has thus been chosen for further explanation. An example of specific policies and procedures is provided in Appendix D which explains the particular management of sensitive information in a merger or joint venture.

Specifically, the goal of Operations Security is to control information and observable actions concerning capabilities, limitations, activities, and intentions, thus
preventing or controlling their exploitation by an adversary or a business competitor. Overall operational effectiveness is inevitably enhanced by denying an adversary or competitor the opportunity to foresee a corporation’s intentions, thereby providing the opportunity to take measures to nullify any advantage another company may have. Proper application of Operations Security measures can maximize a company’s potential for success.

Operations Security looks at behavior from adversaries’ or competitors’ points of view. Information that they may need to achieve their goals (to the detriment of the target firm) constitutes the critical information of a firm’s business operations or activities. Denying this critical information to adversaries/competitors enhances corporate security and promotes overall effectiveness.

The Operations Security analytical process focuses on the adversarial exploitation of open or public sources and observable actions to obtain evidence of critical information. These sources are generally not designated proprietary information. Consequently, such sources may be more difficult to control than those that are protected as proprietary. Traditional security programs and procedures generally protect classified or proprietary information. The Operations Security process is designed to identify those indicators that contribute to the loss of critical information through sources that are not protected, and to take action to deny or control the availability of those indicators to an adversary/competitor.

Operations Security measures complement physical, information, signals, computer, communications, electronic, and other security measures to ensure a totally
integrated security package. Reviewing the Operations Security process often discloses weaknesses in the application of traditional security practices.

OPSEC furnishes an analytical framework to determine:

1. Profiles of selected competitors or adversaries
2. Information or intelligence that is of greatest value to the competition
3. The likely targets of intelligence or corporate espionage directed against the company
4. The possible and probably mechanisms that can be utilized to collect intelligence against the company
5. The company’s vulnerabilities and safeguard mechanisms that can be instituted to limit or minimize these vulnerabilities

The steps of the OPSEC process are:

1. Identification of critical information
2. Threat analysis
3. Vulnerability analysis
4. Risk assessment
5. Applications of appropriate countermeasures, each equally important
   a. Elimination of indicators subject to exploitation
   b. Disruption of effective adversary collection or processing efforts
   c. Prevention of the accurate interpretation of indicators during their analysis

George Jelen, a former director of Operations Security at the National Security Agency (NSA) states:

Each of these phases is important to the integrity and efficacy of the overall process. Although each of them has value in and of itself, it is only when all five are employed together that the full synergistic value of the Operations Security process accrues. Identification of critical information provides focus; threat analysis assures realism; vulnerability analysis lends objectivity; risk assessment guarantees rationality; and the application of countermeasures ensures utility and value. Together they represent a logical and balanced approach to contending with risk. The approach which is applicable to any competitive or adversarial situation seeks not so much to avoid risk, as this is impossible, but rather to manage it. (Miller, J. pp. 221-224)

By using the Operations Security analytical process, Competitive Intelligence professionals will gain a better understanding of what information may be available to an
adversary or competitor, the impact of information loss, and a better appreciation of ways for its protection. The careful selection of Operations Security measures and their appropriate application contributes to overall corporate effectiveness by protecting critical information against compromise.

**Economic Espionage Act**

A worthy subject to mention in relation to information protection is the Economic Espionage Act (EEA). Many executives mistakenly believe that the EEA automatically protects their company’s valuable information and eliminates the risk of competitive intelligence. A brief explanation of the EEA follows; see Appendix E for a Society of Competitive Intelligence Professionals analysis of the EEA and its influence on the CI profession.

The Economic Espionage Act (EEA) of October 1996 made the theft of trade secrets a federal crime. Specifically, the EEA makes it illegal to steal or “appropriate” rivals’ proprietary information without their authorization. Violators could get up to 15 years in imprisonment and fines up to $10 million (Shaker & Gembicki pp. 217-220).

A *trade secret*, as defined by the EEA, encompasses all types of financial, business, scientific, technical, economic, and engineering information. These can take the form of patterns, plans, compilations, program devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs or codes.

There are two stipulations governing the enforcement of EEA:

1. The owner must have taken “reasonable measures” to keep the information secret, and
2. The information’s value must be derived from not being readily ascertainable through proper means, which is to say it is being kept secret. These stipulations are somewhat broad and their interpretation is debatable.
Review of court cases in which the EEA was applied may be necessary prior to the initiation of litigation or other legal proceedings. The following cases involve application of and rulings based on the EEA:

- Midgard Corp. v. Todd, 1997 U.S. App. LEXIS 3874 (10th Cir. March 5, 1997)

Summary

This concludes the brief overview of information protection and the first section of the paper. As stated above, more information regarding information protection can be obtained through the online resources listed in Appendix F. The following section of the paper contains the information protection audit program. The audit program was developed in response to the increasing risks of sensitive information security compromise. Specifically, the program helps auditors evaluate whether proper organizational policies and procedures are in place to protect sensitive information.
INFORMATION CONTROL AUDIT GUIDE

Last Update: April 27, 2001

<table>
<thead>
<tr>
<th>Location:</th>
<th>Completed by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Auditee(s) interviewed:</td>
<td>Reviewed by:</td>
</tr>
</tbody>
</table>

INTRODUCTION

Generic audit program to evaluate information security within a client company

RESOURCES

Qualified competitive intelligence professional
Intellectual property control expert

A. GENERAL INFORMATION

1. Provide a brief overview of the company's competitive intelligence department, if any (size, responsibilities, output, etc.). In addition, document the position of the information control function within the firm. Attach a general organizational chart if necessary.

Attachment Reference:

2. Document the names and titles of employees who are involved in information control. Evaluate any separation of duties issues.

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Attachment Reference:

B. INFORMATION COUNTERMEASURES

A variety of factors make an active countermeasures program an important addition to the obvious benefits to the company, including (Miller, J. p. 218):

1. A due-diligence requirement to ensure that countermeasures sufficient to deter material as well as intellectual property losses are present in the facility
2. To ensure that such measures are consistent with the changing nature of the threat environment as a required element in the event of any future, potential compromises
3. To ensure that the firm meets those industry standards necessary to demonstrate that the firm has undertaken appropriate security measures to protect itself. Moreover, such reporting as may result from this kind of an effort plays an important role insofar as it serves to document the firm’s proactive stance on securing sensitive and proprietary information—a legal prerequisite whenever seeking redress through the court system at any point in the future.

<table>
<thead>
<tr>
<th>Yes or No</th>
<th>MEMOREF</th>
<th>#</th>
<th>Primary Control Question</th>
<th>Test Methodology</th>
<th>Control Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>Is an acceptable process in place to identify critical information?</td>
<td>Review information classifications to determine if consistent criteria are used to initiate sensitive information into the protection system. Document procedures to classify information as sensitive.</td>
<td>Sensitivity of information should be evaluated and sensitive information identified and protected (Dutka p. 302).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Does the client company use the proper evaluation techniques to classify information?</td>
<td>Review the criteria for each level of information classification to ensure that they are fitting and up-to-date for the circumstances. Compare the information the company is collecting (or attempting to collect) on its competitors with similar data of the client company.</td>
<td>Protection should encompass information that is most difficult for a competitor to develop without tacit or active cooperation. This includes information on subjects like intentions and goals (McGonagle p. 54). Critical information similar to that desired of a competitor company, information that is critical to the client’s operation as a business, and competitive data crucial to completing a profile of the client company should all be protected.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Is supplemental sensitive information protected?</td>
<td>Examine the data surrounding sensitive information to make certain that it is also placed in the protection process.</td>
<td>A focus should be placed on the subject matter of information already declared sensitive. Component parts that would lead a rival business intelligence function to gain useful insights should be defined (Miller, J. pp. 210-211). Protection should extend to material alluding to confidential information and material from which someone could derive critical elements of the confidential plan (McGonagle p. 54).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>Are adequate procedures in place to “declassify” non-sensitive information?</td>
<td>Review the declassification process and document recent incidents of information declassification.</td>
<td>Information should only be protected as long as necessary (McGonagle p. 54).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>Is accurate, current documentation of the protection process’ policies and procedures readily available?</td>
<td>Request copies of documentation relating to protection procedures.</td>
<td>Documentation is necessary for the formal establishment of policies and procedures (Dutka p. 302) and demonstrates that the client company has taken adequate measures to protect itself (Miller, J. p. 218). Documentation should be current and up-to-date (Shaker &amp; Gembicki pp. 213-215).</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>6.</strong></td>
<td>Does the protection policy begin with upper management?</td>
<td>Determine if protection policy statements are from the company CEO or other appropriate member of top management.</td>
<td>A policy statement from upper management emphasizes the importance of information security and the protection process (Shaker &amp; Gembicki pp. 213-215).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>7.</strong></td>
<td>If of sufficient size, does the company contain a diverse, standing information protection policy committee?</td>
<td>Review company organization and the information security process. Interview appropriate members of management.</td>
<td>In addition to providing accountability, a standing committee of appropriate personnel can form and adjust information protection policy as needed by business operations. The committee should contain representatives from a variety of operational areas (competitive intelligence, legal, public relations, human resources) (Shaker &amp; Gembicki pp. 213-215).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>8.</strong></td>
<td>Are common sources of intelligence regularly monitored for disclosed information on the company?</td>
<td>Determine and evaluate the frequency of official monitoring of common sources of competitive intelligence (database searches, industry publications, internet, etc.).</td>
<td>The client company should be aware of the type and quantity of information about it available to its competitors (McGonagle p. 69). In addition, vulnerability assessments should be conducted on a periodic basis (Miller, J. pp. 210-211).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>9.</strong></td>
<td>Are senior management and the legal department kept apprised of any deception and misinformation activities of the company?</td>
<td>In discussions with management, determine if any deception or misinformation activities have occurred. Confirm any statements with personnel from the legal, security, and competitive intelligence functions.</td>
<td>The damage that can occur from a deception campaign if it is disclosed can far exceed the benefits derived from its use (Shaker &amp; Gembicki p. 217).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>10.</strong></td>
<td>Are new innovations or developments patented or copyrighted when appropriate?</td>
<td>Review R&amp;D procedures. Examine legal department documents and interview personnel from the legal department.</td>
<td>Developments of intellectual property should be protected by law whenever possible (Smith &amp; Parr pp. 89-120).</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>11.</strong></td>
<td>Is there a designated contact within the company for ANSIR email advisories from the FBI?</td>
<td>In discussions with management and security personnel, determine if there are one or more ANSIR internal contacts. Document any individual’s name and position.</td>
<td>The Awareness of National Security Issues and Response (ANSIR) Program is the FBI’s National Security Awareness Program designed to provide unclassified national security threat and warning information to U.S. corporate security directors and executives. The company should take full advantage of any government measures raising awareness of security issues and risks.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## INFORMATION CONTROL AUDIT GUIDE

### C. RELEASE OF INFORMATION

<table>
<thead>
<tr>
<th>#</th>
<th>Primary Control Question</th>
<th>Test Methodology</th>
<th>Control Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Are forms of internal communication (employee newsletters, bulletin boards, displays, etc.) monitored for sensitive information?</td>
<td>Review recent employee newsletters and conduct a walkthrough of the client company’s facilities. Document any incidents or discoveries of sensitive information.</td>
<td>Sensitive information may be compromised if unnecessarily placed in prominent areas or publications (McGonagle pp. 61-66). All release of sensitive information should be controlled.</td>
</tr>
<tr>
<td>2</td>
<td>Is only minimal information provided on forms intended for external audiences?</td>
<td>Inquire about the procedures and personnel that are used to complete required external forms. This may include censuses, surveys, government forms such as regulatory filings, or communication with nonbusiness publications.</td>
<td>Documents intended for any external audience should be reviewed to ensure that they do not contain unnecessary references to sensitive information (McGonagle pp. 61-66).</td>
</tr>
<tr>
<td>3</td>
<td>Are all documents containing sensitive information clearly marked as confidential?</td>
<td>Observe the preparation of sensitive documents or review existing sensitive documents. Verify that such documents are clearly labeled as confidential.</td>
<td>Clear markings define documents as sensitive and confidential to a user uneducated about the informational contents of the documents (McGonagle pp. 61-66).</td>
</tr>
<tr>
<td>4</td>
<td>Is sensitive information only available to necessary internal personnel?</td>
<td>Randomly select a topic of sensitive information and review the dissemination process within the company. Check regularly produced documents and mailing lists. Document any instance of information availability to nonessential personnel.</td>
<td>Sensitive information should only be available to necessary personnel. This includes limiting the knowledge of the competitive intelligence or information protection units in the company and omitting from documents any items no longer relevant to the audience (McGonagle pp. 59, 80-81).</td>
</tr>
<tr>
<td>5</td>
<td>Do email messages include an automatic disclosure (often at the end) stating that information is for intended recipients only?</td>
<td>Examine email correspondence to determine if any such statement is enclosed.</td>
<td>An automatic statement accounts for the possibility that sensitive information may be contained in messages and may encourage message deletion in case of a misdirected message.</td>
</tr>
<tr>
<td>6</td>
<td>Is information on the company website screened and monitored for sensitive information?</td>
<td>Review website posting policy and interview the company’s webmaster. Search the company’s website for any unnecessary disclosures of sensitive information.</td>
<td>Sensitive information should not be disclosed unnecessarily. Extensive job listings or executive changes and profiles may provide insight into the company’s strategies, goals, or objectives (Dutka p. 88).</td>
</tr>
<tr>
<td>7</td>
<td>Is information reviewed and filtered by appropriate personnel before it is released for research at universities?</td>
<td>Inquire about any recent permitted university research or projects involving the company. Review joint research policy, if any.</td>
<td>Sensitive information can be compromised if it is carelessly distributed under the pretense of university research (Dutka pp. 306-307). Sensitive material should not be released.</td>
</tr>
</tbody>
</table>
D. SECURITY

<table>
<thead>
<tr>
<th>Yes or No</th>
<th>MEMO REF</th>
<th>#</th>
<th>Primary Control Question</th>
<th>Test Methodology</th>
<th>Control Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>Does the company have a trained security staff?</td>
<td>Interview appropriate management personnel; review organizational chart.</td>
<td>The company should have trained security personnel on staff to provide professional expertise and accountability (PWC/ASIS p. 15).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Is access to areas containing sensitive information controlled and limited to necessary personnel?</td>
<td>Review security procedures and policy. Examine any entry or security logs of the company.</td>
<td>Access to facilities or areas containing sensitive information or material should be limited (Dutka p. 300; PWC/ASIS p. 27).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Are employees required to register their entry into areas where sensitive information is stored?</td>
<td>Review security procedures and policy. Examine any entry or security logs of the company.</td>
<td>Access to facilities or areas containing sensitive information or material should be limited (Dutka p. 300; PWC/ASIS p. 27).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>Are the company's extremely sensitive facilities regularly inspected for eavesdropping, wiretapping, or alteration of telecommunication system programming?</td>
<td>Determine if and how often inspections occur. Review procedures and interview personnel to determine who completes the inspection.</td>
<td>Eavesdropping, wiretapping, or alteration of telecommunication system programming should be detected (PWC/ASIS p. 21).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>Are all documents containing sensitive information disposed of in an acceptable manner?</td>
<td>Inquire about document disposal process. Observe disposal of documents containing sensitive information.</td>
<td>Rifling garbage in an attempt to cull valuable information is believed to be the number one method of business and personal espionage (McGonagle p. 55). Documents should be securely and consistently destroyed (preferable shredded or incinerated).</td>
</tr>
</tbody>
</table>

E. OPERATIONS

1. HR, Employee education
## INFORMATION CONTROL AUDIT GUIDE

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong></td>
<td>Are employees advised and/or reminded of information control procedures prior to any trade show, interview, or meeting where competitors may be present?</td>
<td>Inquire about the preparation procedures for any such event. Review any preparation documents to verify that they contain general lists of information that is too sensitive for specific discussion.</td>
</tr>
<tr>
<td><strong>2</strong></td>
<td>Do employees deal with incoming solicitations of information in an appropriate manner?</td>
<td>Review company policy to confirm that procedures are in place for employees to: 1. Get name, firm, and contact information of the caller 2. Ask precisely what kinds of information is desired and the deadline, if any, and 3. Report the contact to a specific individual in the security department for follow-up. Interview and observe employees to ensure that policy is followed.</td>
</tr>
<tr>
<td><strong>3</strong></td>
<td>Are appropriate employees required to sign official secrecy and associated (non-disclosure) agreements?</td>
<td>Randomly select and review the personnel files of employees to determine if any such agreement is utilized. These should include agreements pledging no competition against current company programs for a specified period of time should the employee leave, no raiding of company personnel to accompany a departed employee, and invention covenants.</td>
</tr>
<tr>
<td><strong>4</strong></td>
<td>Are thorough background checks conducted of all employees?</td>
<td>Review hiring procedures and personnel files to determine if thorough background checks were performed and documented.</td>
</tr>
<tr>
<td><strong>5</strong></td>
<td>Are complete background investigations completed on the company's non-traditional workers (especially temporary and contract staffs)?</td>
<td>Review procedures for hiring temporary and contract workers. Examine work contracts.</td>
</tr>
<tr>
<td><strong>6</strong></td>
<td>Are temporary workers, including interns, not assigned to projects or work areas containing sensitive information areas?</td>
<td>Interview HR personnel and review recent assignments for temporary workers.</td>
</tr>
<tr>
<td><strong>7</strong></td>
<td>Do employees undergo information security training upon employment?</td>
<td>Review the agenda for new-hires and discuss training policies with HR personnel.</td>
</tr>
</tbody>
</table>
### INFORMATION CONTROL AUDIT GUIDE

Last Update: April 27, 2001

<table>
<thead>
<tr>
<th>Memo #</th>
<th>Primary Control Question</th>
<th>Test Methodology</th>
<th>Control Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>Does the company provide employees with continued information security training and awareness?</td>
<td>Interview HR personnel and policies concerning continued security training. Examine the schedules of key employees to ensure that they have undergone additional security training.</td>
<td>In order to safeguard sensitive information, employees should remain informed about proper security procedures and any new developments in sensitive information control (PWC/ASIS p. 15).</td>
</tr>
<tr>
<td>9</td>
<td>During exit interviews, are employees reminded of obligations to the company regarding sensitive information?</td>
<td>Review the exit or termination procedures of HR. Interview personnel to ensure that proper exit interviews are conducted.</td>
<td>Exit or termination interviews reminding employees of their continuing obligation to safeguard the trade secrets and proprietary information to which they had access during the course of their employment are effective at preventing many problems and are another method of communicating the organization’s vigilance in defending its intellectual property rights (PWC/ASIS p. 27).</td>
</tr>
</tbody>
</table>

#### 2. Travel

<table>
<thead>
<tr>
<th>Yes or No</th>
<th>Memo REF</th>
<th>#</th>
<th>Primary Control Question</th>
<th>Test Methodology</th>
<th>Control Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>YES/NO</td>
<td></td>
<td>1</td>
<td>Are travel plans of key company officials treated as sensitive information when necessary?</td>
<td>Evaluate internal access to the travel plans of executive personnel and the release of travel plans to the public.</td>
<td>Travel plans of key company officials could indicate an impending merger or acquisition (Shaker &amp; Gembicki p. 206). Access to the travel plans of key executives should be restricted to necessary personnel.</td>
</tr>
<tr>
<td>YES/NO</td>
<td></td>
<td>2</td>
<td>Is the discussion of sensitive information restricted to secure telephones only?</td>
<td>Review travel and communication procedures for sensitive information. Interview traveling personnel to ensure that proper procedure is followed.</td>
<td>Public and cellular telephone conversations may be overheard or intercepted. Discussion of sensitive information in this manner should be limited or avoided (McGonagle pp. 78-79).</td>
</tr>
<tr>
<td>YES/NO</td>
<td></td>
<td>3</td>
<td>Are travelers encouraged to avoid the use of hotel fax machines?</td>
<td>Review travel and communication procedures for sensitive information. Interview traveling personnel to ensure that proper procedure is followed.</td>
<td>Because information can be easily seen by hotel staff or sent to an unauthorized party, the use of hotel fax machines for outgoing and incoming messages containing sensitive information should be avoided (McGonagle pp. 78-79).</td>
</tr>
<tr>
<td>YES/NO</td>
<td></td>
<td>4</td>
<td>Are laptop computers used only in secure locations?</td>
<td>Review travel and communication procedures for sensitive information. Interview traveling personnel to ensure that proper procedure is followed.</td>
<td>Sensitive information on computer screens can be compromised if a laptop computer is operated in plain view in a public place (hotel lobby, airplane, airport concourse, etc.) (McGonagle pp. 78-79).</td>
</tr>
</tbody>
</table>
### INFORMATION CONTROL AUDIT GUIDE

**Last Update:** April 27, 2001

<table>
<thead>
<tr>
<th></th>
<th>Primary Control Question</th>
<th>Test Methodology</th>
<th>Control Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>Is sensitive information not left unattended in hotel rooms?</td>
<td>Review travel procedures for personnel carrying sensitive information. Interview traveling personnel to ensure that proper procedure is followed.</td>
<td>Foreign hotel rooms occupied by visiting business executives are common targets (Dutka p. 299).</td>
</tr>
<tr>
<td>6</td>
<td>Is sensitive information transferred only through secure lines of communication?</td>
<td>Review travel and communication procedures for sensitive information. Interview traveling personnel to ensure that proper procedure is followed.</td>
<td>Fax transmittals and electronic data interchanges are routinely monitored in some countries (Dutka p. 299).</td>
</tr>
</tbody>
</table>

#### 3. General, purchases

<table>
<thead>
<tr>
<th></th>
<th>MEMO REF</th>
<th>#</th>
<th>Primary Control Question</th>
<th>Test Methodology</th>
<th>Control Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Are appropriate precautions taken to conceal or disguise especially sensitive purchases?</td>
<td>Review or observe procedures for such purchases to determine if protection measures are sufficient. Procedures may include purchasing through several captive companies or staggering purchases over a period of several months.</td>
<td>Important aspects of sensitive information should be protected. Measures should be appropriate based on sensitivity of the purchase (Miller, J. pp. 210-211).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Is sensitive material eliminated from plant or facility closing sales?</td>
<td>Determine policy and procedure for facility closings.</td>
<td>Proprietary information, especially advanced technical material, should be kept confidential or sold to appropriate buyers only (Fialka pp. 29-49).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Are sensitive negotiations held in a secure, unannounced location?</td>
<td>Review procedures for arranging important or confidential negotiations. Determine that recent negotiations conformed to policy.</td>
<td>For security purposes, the location of sensitive negotiations should be kept confidential (Dutka pp. 295-296).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Does the company have a safe system in place to receive competitive bids?</td>
<td>Examine procedures for receiving bids and review recent bidding processes.</td>
<td>Bidding information and the bidding process should be free from any unauthorized tampering (Fialka pp. 130-131).</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Is a thorough background investigation completed on major suppliers and original equipment manufacturers (OEMs)?</td>
<td>Review procurement procedures. Determine if investigations are conducted prior to contract or order assignments.</td>
<td>Suppliers and original equipment manufacturers are often exposed to a large amount of sensitive company information (Fialka p. 15; PWC/ASIS p. 3). These entities should be investigated before information is released.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Does the company assess the security of partners and vendors?</td>
<td>Inquire about security procedures for the original establishment of partner or vendor status. Review current partner and vendor policies concerning the transfer of sensitive information.</td>
<td>The security of partners and vendors should be assessed prior to entering into any relationship in which sensitive material may be transferred (PWC/ASIS p. 15).</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### F. PROTECTION COMPROMISES

#### 1. General

<table>
<thead>
<tr>
<th>Yes or No</th>
<th>MEMO REF</th>
<th>#</th>
<th>Primary Control Question</th>
<th>Test Methodology</th>
<th>Control Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>Does protection policy define what constitutes an informational security compromise?</td>
<td>Make sure that protection policy procedures contain an appropriate definition of a security compromise.</td>
<td>Personnel should be able to accurately recognize when sensitive information has been misappropriated (Shaker &amp; Gembicki pp. 213-215).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Are reaction procedures outlined for situations involving the compromise of information?</td>
<td>Review policy and protocol to determine that contingency plans are in place for compromises of security. Interview employees to determine if policy has been followed in recent incidents of compromise, if any.</td>
<td>The protection policy should specify what procedures should be taken upon discovery of compromises and what legal actions and remedies the company will take. Employees should be aware of and follow procedures (Shaker &amp; Gembicki pp. 213-215).</td>
</tr>
</tbody>
</table>

#### 2. Court Action – Keep in mind that once a trial has begun, everything that is introduced as evidence and all the transcripts of the trial are generally (and usually automatically) a part of the public record...While you cannot control what your opponent introduces into evidence, you can ask the court, in advance if possible, to take special measures to keep such matters in confidence – and out of the public record. (McGonagle 74)

<table>
<thead>
<tr>
<th>Yes or No</th>
<th>MEMO REF</th>
<th>#</th>
<th>Primary Control Question</th>
<th>Test Methodology</th>
<th>Control Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>If court action is initiated, does the company have the other side sign an agreement (stipulation) to keep certain documents or information in confidence?</td>
<td>Review the company’s procedures for court action. Discussion with the company’s attorneys or legal department may be necessary.</td>
<td>Disclosure of sensitive information should be limited in court proceedings (McGonagle p. 74).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Is a request made of the judge to enter a protective order controlling who sees the discovery and under what circumstances?</td>
<td>Examine the client company’s procedures for court action or interview appropriate personnel in the legal department. Review recent court cases, if applicable.</td>
<td>Sensitive information in court rulings should be controlled if possible. A protective order of the judge supervising the discovery may have the parties place discovery documents in a location where they are subject to inspection only, but not copying, if they are very sensitive (McGonagle p. 74).</td>
</tr>
</tbody>
</table>
### G. INFORMATION TECHNOLOGY

<table>
<thead>
<tr>
<th>Yes or No</th>
<th>MEMO REF</th>
<th>#</th>
<th>Primary Control Question</th>
<th>Test Methodology</th>
<th>Control Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1</td>
<td>Are sensitive files encrypted within the company’s computer system?</td>
<td>Review the company’s computer security policies and procedures. Interview system personnel to ensure that policy is adhered to.</td>
<td>Sensitive information should be protected in electronic format. Encryption provides an additional level of protection for information contained in computer files (Fialka p. 15).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>2</td>
<td>Is the company’s computer security equipment installed and updated on the computer system?</td>
<td>Review the company’s computer security policies and procedures. Interview system personnel to ensure that policy is adhered to. Examine computer files to verify that security software is in use and current.</td>
<td>Sensitive information should be protected in electronic format. Security equipment aids in protection only if it is installed and used properly (Fialka p. 15).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3</td>
<td>Are employee passwords kept secure and changed at least once a month?</td>
<td>Review the company’s computer security policies and procedures. Interview system personnel to ensure that policy is adhered to.</td>
<td>Access to the company’s computer system should be limited to authorized personnel (Fialka pp. 101-112).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4</td>
<td>Are one-time password generators used for important computer entries and alterations?</td>
<td>Review the company’s computer security policies and procedures. Interview system personnel to ensure that policy is adhered to.</td>
<td>Providing a new password for each important computer entry ensures that entries will not be duplicated (Fialka pp. 101-112).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5</td>
<td>Does the company require screen saver passwords on all computer terminals?</td>
<td>Examine one or more computer terminals to determine if screen saver passwords are standard. Interview IT personnel and review policy.</td>
<td>Screen saver passwords reduce the risk of unauthorized access to sensitive information on unattended computers (PWC/ASIS p. 15).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>6</td>
<td>Does the company encrypt data transmitted over the internet?</td>
<td>Review the company’s computer security policies and procedures. Interview system personnel to ensure that policy is adhered to.</td>
<td>Sensitive information should be protected in electronic format. Encryption provides an additional level of security assurance (PWC/ASIS p. 15).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7</td>
<td>Does the company use only licensed software?</td>
<td>Examine installed software on computer terminals to ensure that only official, licensed versions are installed.</td>
<td>The use of licensed software limits the risk of file corruption or compromise by illegal or altered software code. (PWC/ASIS p. 15).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>8</td>
<td>Are digital forms of sensitive information secured comparable to hard forms?</td>
<td>Review the company’s computer security policies and procedures. Interview system personnel to ensure that policy is adhered to.</td>
<td>Sensitive information should be protected in electronic format with the same enthusiasm that it is protected in paper format (PWC/ASIS p. 15).</td>
</tr>
</tbody>
</table>


End Notes

1In a 1985 proposal of Information Resource Management (IRM), Diebold (p. 41) states that IRM means “Managing information as a resource in much the same way that other corporate resources are managed.”

2Tritter (p. 14) asserts, “…a business risk is anything that threatens achievement of business objectives. Such risks could be environmental, such as the strength of national economy... The majority of business risks, however, are internal... Business risks can be easily analyzed in CSA [Control Self-Assessment] sessions, and proper solutions can be put in place to strengthen the company’s responses to them.”

3This information is found at the Federal Bureau of Investigations website: Intellectual Property Crimes section <http://www.fbi.gov/programs/fc/fifu/about/about_ipc.htm>

4This quote is found on the website of the Society of Competitive Intelligence Professionals (SCIP) <www.scip.org> and in Appendix C, an overview of the Competitive Intelligence field compiled by the SCIP.

5For information on legal strategies for protection of IP rights, see Simensky 15.1-15.54. For information on proactive auditing of IP, see Simensky 7.1-7.9. An intellectual property audit is an internal review of the intellectual property rights (IPRs) of a business and how those rights are managed.

6The press release for this final incident is found on the U.S. Department of Justice website at <http://www.usdoj.gov/criminal/cybercrime/Estrada.htm>

7The majority of this list is found at the Defense Security Service’s counterintelligence website <http://www.dss.mil/cithreats/protect.htm>. The added points were discovered through additional research.

8The following Operations Security (OPSEC) information is compiled from information found in Shaker & Gembicki pp. 206-207 and Miller, J. pp. 221-224.

9For further information on the Awareness of National Security Issues and Response (ANSIR) program of the Federal Bureau of Investigation (FBI), see the FBI website at <http://www.fbi.gov/programs/ansir/ansir.htm>
Appendix A:

PricewaterhouseCoopers LLP and the American Society for Industrial Security, International

Trends in Proprietary Information Loss
Survey Report
Trends in Proprietary Information Loss
Key Survey Findings

- In 1999, Fortune 1000 companies sustained losses of more than $45 billion from thefts of their proprietary information.1

- Forty-four companies of the total 97 that responded reported a total of over 1,000 incidents of thefts. Of these, 579 incidents were valued with a total estimated loss of nearly $1 billion dollars. The average company responding reported 2.45 incidents with estimated losses per incident of over $500,000. The vast majority of the reported incidents were in High Technology (360) and Services organizations (356). Although Manufacturing reported only 98 incidents, the acknowledged losses of manufacturing companies accounted for the majority of losses reported in the survey, and averaged almost $50 million per incident.

- The global Internet and proliferation of information systems have significantly increased the risks to corporate proprietary information.

- The greatest known losses to American companies are in manufacturing processes and research and development information.

- The number of reported incidents per month has increased dramatically within the last 17 months.

- Forty-five percent of companies responding to the American Society for Industrial Security/PricewaterhouseCoopers ("ASIS/PricewaterhouseCoopers") survey indicate one or more incidents of information loss, theft and/or misappropriations.

- On-site contractor employees and original equipment manufacturers (OEMs) are now perceived by companies responding to the survey to present the greatest threat to corporate proprietary information.

- The majority of companies responding to the survey have not effectively met the challenges of providing a framework in which to safeguard proprietary information.

- Consistent mechanisms and processes for determining the value of proprietary information are not in place at most Fortune 1000 companies.

1For the purposes of this survey we are limiting our definition of proprietary information to that information which is not within the public domain and which the owner has taken some measures to protect. While commonly referred to as "trade secrets," this information is typically protected under both State and Federal law.
The Nature of the Proprietary Information Loss Problem

Over the past few years this annual report has highlighted the fact that documented losses of trade secrets and other proprietary information cost US companies tens of billions of dollars annually. Recent high profile incidents involving major U.S. companies illustrate that misappropriation of sensitive proprietary information has become a serious problem afflicting many business organizations. This year, PricewaterhouseCoopers joined with ASIS to conduct the Trends in Proprietary Information Loss Survey in an effort to raise awareness of these important strategic issues throughout the business community and among corporate counsel and senior management. In particular,

Although 70 percent or more of the market value of a typical US company resides in intellectual property (IP) assets, typically formalized valuation procedures do not exist and thus these assets are not tracked in corporate accounting systems. Since the value of IP assets is not well established, they are often not well protected, thereby contributing to the current problems associated with theft of trade secrets and proprietary information.

Proprietary information protection differs significantly from the other security disciplines. It differs from computer and network security services, as the focus is on managing and protecting the intangible assets in whatever medium or form they exist, which may not be limited to computerized forms. It also differs from the classic physical security services even though it may involve guard forces and alarm systems. The challenge facing security professionals is to improve proprietary information protection through more systematic cooperation with the corporate legal department, compliance, human resources and the business units to address the many forms of "non-physical" harm to the enterprise. The primary focus of these coordinated efforts should be on preventing and responding to theft, misappropriation or infringement of the client's intellectual property rights in the physical world as well as addressing the new challenges arising from the vast increase in electronic commerce and operations in cyberspace.

Proprietary information assets are vital to the success of many, perhaps most businesses at the end of the 20th Century. The importance of these assets, while often not formally "valued" by many companies, cannot be underestimated. In today's highly competitive environment, it is essential for American businesses to recognize that the intellectual assets of every business are highly sought-after commodities.

Competitive intelligence gathering has become an essential part of international business. Many organizations are fearful they will be left behind if they don't use every means at their disposal to gain a competitive edge over their rivals. This has resulted in many companies forming specialized intelligence gathering units, to ensure timely and accurate information is available. While some "ethical" intelligence practitioners, such as the members of the Society of Competitive Intelligence Professionals (SCIP) adhere to professional codes of conduct, the field is also populated with practitioners concerned solely with achieving results. Some practitioners, such as "retired" personnel from foreign governmental clandestine intelligence services, may resort to predatory illegal means to obtain information.

The loss of proprietary intellectual assets through unethical or illegal means costs businesses significant amounts of lost profits and reduces new opportunities for future business success. In extreme cases it may result in the total loss of the business. Information gathered through the ASIS/PricewaterhouseCoopers Trends in Proprietary Information Loss Survey suggest that monetary losses and other negative business impacts from theft, misappropriation and infringement will increase in the foreseeable future.
Survey Question Responses

The Survey Instrument will be available on the ASIS web site at www.asisonline.org. The questions and responses have been summarized and charts provided where appropriate to highlight significant findings and observations. To facilitate the analysis of the responses, organizations have been allocated to four main groups: Manufacturing, High Technology, Financial/Insurance or Services.

1. For each of the items listed, how high or low is the potential threat to your company's intellectual property (IP)?
   (1 — highest, 4 — lowest)

<table>
<thead>
<tr>
<th>Insiders</th>
<th>Score</th>
<th>Outsiders</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Employees</td>
<td>2.66</td>
<td>Domestic Competitors</td>
<td>2.82</td>
</tr>
<tr>
<td>On-site Contractors</td>
<td>2.29</td>
<td>Foreign Competitors</td>
<td>2.53</td>
</tr>
<tr>
<td>Former Employees</td>
<td>2.74</td>
<td>Computer Hackers</td>
<td>2.75</td>
</tr>
<tr>
<td>Vendor/Suppliers</td>
<td>2.81</td>
<td>The Media</td>
<td>3.28</td>
</tr>
<tr>
<td>Strategic Partners</td>
<td>2.64</td>
<td>Intelligence Services</td>
<td>3.28</td>
</tr>
<tr>
<td>OEMs</td>
<td>2.27</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average</td>
<td>2.53</td>
<td>Average Score</td>
<td>3.01</td>
</tr>
</tbody>
</table>

The threat posed by persons within the organization is still considered to be a primary threat to corporate information. Responses to this question were consistent with each of the previous surveys. This year OEMs (original equipment manufacturers) — the companies that provide components, sub-assemblies and the like — edged out current and former employees as the top concern. OEMs are perceived to represent the greatest threat to both Financial/Insurance and Manufacturing while on-site contractors are perceived to be the greatest risk for High Technology and Services firms.

The average score for all insider relationships was 2.53, suggesting a higher than average threat. The common factor in these relationships is that these groups are privy to the trade secrets and proprietary information of the company using their services. The levels of concern expressed by respondents suggest that more efforts may be appropriate to manage these risks.

Outsiders were, at best, considered to pose only a medium to low level of threat. Interestingly, intelligence services (whether governmental or private) are not, according to the respondents, considered to be a significant threat. Only High Technology respondents expressed significant concerns about foreign competition, the other industry groups apparently finding them to be an average threat. The media was a below average concern to virtually all respondents.

2. Please rank each in terms of the GREATEST RISK of losing this type of information.

(1 — Greatest Risk, 10 — Least Risk)

<table>
<thead>
<tr>
<th>Information Category</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Lists</td>
<td>4.16</td>
</tr>
<tr>
<td>Financial Data</td>
<td>4.46</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>4.72</td>
</tr>
<tr>
<td>Merger/Acquisition</td>
<td>4.84</td>
</tr>
<tr>
<td>Strategic Plans</td>
<td>4.96</td>
</tr>
<tr>
<td>Unannounced Product Specs</td>
<td>4.92</td>
</tr>
<tr>
<td>2nd Party Information</td>
<td>5.07</td>
</tr>
<tr>
<td>Prototypes</td>
<td>5.50</td>
</tr>
<tr>
<td>Manufacturing Data</td>
<td>5.80</td>
</tr>
</tbody>
</table>

High Technology companies consider the greatest risk is associated with losing new product specifications (4.05) and research and development (4.18). Loss of such information early in a high tech product's lifecycle could result in a competitor gaining sufficient time to bring to market an equal or superior product with similar features and performance.

Financial/Insurance respondents were most concerned about loss of customer lists (2.75) and second-party information (3.35). Financial/Insurance organizations demonstrate priority concern with losses of second party information. Customers/clients of such organizations often entrust personal and private information to the company, and such organizations are privy to credit reports, medical and other forms of information loss or unauthorized disclosure of which could subject the company to liability, as well as adversely impact customer confidence.

Manufacturing companies were most concerned about research and development information (4.18). Services companies were most concerned about financial data (4.00). Manufacturing concerns about the loss of R&D information may indicate that the longer lead times required to bring a new manufactured product to market is significant, so greater losses could be expected from that type of information. Services firms are apparently most concerned that their greatest risks derive from loss of failure to safeguard their financial data. Lacking physical or tangible products, they may be most harmed by loss of their financial forecasts, metrics used to cost services or other activities.
3. During the past year, (i) approximately how many times has your company lost the specified information and (ii) what was the approximate dollar value of the actual loss?

<table>
<thead>
<tr>
<th>Industrial Category</th>
<th>Dollar Lost (Reported)</th>
<th>Total Number of Companies</th>
<th>Number of Companies Reporting Incidents</th>
<th>Number of Incidents</th>
<th>Number of Incidents Valued</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Technology</td>
<td>$119,825,000</td>
<td>20</td>
<td>9</td>
<td>33</td>
<td>252</td>
</tr>
<tr>
<td>Financial/Insurance</td>
<td>$2,055,000</td>
<td>20</td>
<td>7</td>
<td>41</td>
<td>8</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>$871,295,000</td>
<td>31</td>
<td>18</td>
<td>96</td>
<td>39</td>
</tr>
<tr>
<td>Services</td>
<td>$5,252,000</td>
<td>26</td>
<td>13</td>
<td>358</td>
<td>280</td>
</tr>
</tbody>
</table>

The average company responding reported 2.65 incidents with estimated losses per incident of over $500,000.

The Survey responses indicate that manufacturing companies experienced the largest losses, due to loss of research and development information and manufacturing data. Manufacturing organizations reported losses of nearly $900 million in 39 incidents. Significantly, these same companies only indicated the risk to such information was average (5.23).

Most frequent reported losses were to high technology companies that lost customer lists and data. Survey respondents reported more than 250 incidents of loss of such data. Small companies (under $5 billion) suffered losses of research and development information. Due to their smaller size, losses experienced by smaller companies may be much more harmful to their survival and future success. High tech companies reported their largest losses from "unauthorized distributions of product specifications." This may explain why they noted the greatest concern about such losses because a loss of this sort would allow competitors to rush to market equivalent products.

The disparity in both numbers of incidents and financial impact between the Manufacturing/High Technology companies and the Services/Financial/Insurance groups is significant. Financial companies are governed by strict rules that are derived from governmental regulations about information security and as such would be expected to have better systems in place to detect and deter such losses. The majority of incidents where respondents provided a specific value for a loss in the Services group involved copyright infringements.

The data looks more consistent when sorted by revenue size.

<table>
<thead>
<tr>
<th>Revenue Category</th>
<th>Dollar Lost (Reported)</th>
<th>Total Number of Companies</th>
<th>Number of Companies Reporting Incidents</th>
<th>Number of Incidents</th>
<th>Number of Incidents Valued</th>
</tr>
</thead>
<tbody>
<tr>
<td>$5 Billion or Less</td>
<td>$196,112,000</td>
<td>38</td>
<td>18</td>
<td>441</td>
<td>324</td>
</tr>
<tr>
<td>$6-$15 Billion</td>
<td>$400,280,000</td>
<td>33</td>
<td>18</td>
<td>108</td>
<td>77</td>
</tr>
<tr>
<td>Over $15 Billion</td>
<td>$196,035,000</td>
<td>28</td>
<td>11</td>
<td>474</td>
<td>178</td>
</tr>
</tbody>
</table>

Medium sized companies appear to have sustained the most significant losses. Regardless of how the data is sorted, proprietary information losses are far greater than any other type of security-related loss to the company.

4. How much did loss of information contribute to the identified problems for your company between January 1, 1997 and June 1, 1998?

<table>
<thead>
<tr>
<th>Corporate Issue</th>
<th>High Technology</th>
<th>Financial/Insurance</th>
<th>Manufacturing</th>
<th>Services</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Loss of Competitive Advantage</td>
<td>2.41</td>
<td>2.15</td>
<td>2.36</td>
<td>2.29</td>
<td>2.30</td>
</tr>
<tr>
<td>Loss of Market Share</td>
<td>2.53</td>
<td>2.10</td>
<td>2.36</td>
<td>2.38</td>
<td>2.35</td>
</tr>
<tr>
<td>Loss of Revenue</td>
<td>2.17</td>
<td>2.00</td>
<td>2.35</td>
<td>2.19</td>
<td>2.18</td>
</tr>
<tr>
<td>Increased R&amp;D Costs</td>
<td>2.12</td>
<td>2.10</td>
<td>2.42</td>
<td>2.78</td>
<td>2.35</td>
</tr>
<tr>
<td>Embarrassment</td>
<td>2.41</td>
<td>1.95</td>
<td>2.35</td>
<td>2.05</td>
<td>2.19</td>
</tr>
<tr>
<td>Increased Legal Costs</td>
<td>2.00</td>
<td>2.10</td>
<td>2.19</td>
<td>2.05</td>
<td>2.10</td>
</tr>
<tr>
<td>Increased Insurance Costs</td>
<td>2.41</td>
<td>2.20</td>
<td>2.59</td>
<td>2.33</td>
<td>2.41</td>
</tr>
<tr>
<td>Average Score</td>
<td>2.29</td>
<td>2.09</td>
<td>2.30</td>
<td>2.29</td>
<td>2.27</td>
</tr>
</tbody>
</table>

It appears that there are two major consequences of loss of information to many companies (especially High Tech and Services). The first is embarrassment, which is tied with increased legal costs for the problems created for companies. It is difficult to place a monetary assessment on intangibles such as embarrassment or adverse publicity but the potential consequences can translate into very tangible financial losses if, for instance, shareholders abandon a publicly traded company based upon a publicized information loss incident.

The second major consequence, legal costs are very real and represent costs to litigate or prosecute for known or suspected cases of theft or infringement. Legal costs also include any supplemental efforts to protect existing patents, copyrights and

Embarrassment and legal costs were reported as the two major consequences of loss of information to many companies.
trademarks against infringements. Given that legal costs to litigate a single patent suit may exceed $1 million dollars, it is obvious that litigation is a very expensive means of enforcement, especially when an organization may have dozens to hundreds of patents and other IP to defend.

Increased insurance costs were the least important consequence of information loss. Information losses tend not to be covered by business insurance, at least in part because there is a lack of effective mechanisms to consistently value information. Insurance companies may also be reluctant to issue policies for assets that are not valued or do not have firmly established guidelines on how to safeguard them.

5. Rank each of the types of information to indicate the GREATEST POTENTIAL DOLLAR LOSS from losing this type of information.

(1 — Greatest Risk, 10 — Least Risk)

One purpose of this question was to determine any consistency between the information loss experience of the respondent companies and their internal assessments of what could impact them the most.

<table>
<thead>
<tr>
<th>Information Category</th>
<th>High Technology</th>
<th>Financial/Insurance</th>
<th>Manufacturing</th>
<th>Services</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer List/Data</td>
<td>5.12</td>
<td>2.78</td>
<td>4.08</td>
<td>4.30</td>
<td>4.22</td>
</tr>
<tr>
<td>Financial Data</td>
<td>5.76</td>
<td>2.22</td>
<td>4.62</td>
<td>4.18</td>
<td>4.44</td>
</tr>
<tr>
<td>R&amp;D</td>
<td>5.47</td>
<td>6.28</td>
<td>3.87</td>
<td>5.36</td>
<td>4.52</td>
</tr>
<tr>
<td>Mergers/Acquisitions</td>
<td>5.00</td>
<td>3.09</td>
<td>4.86</td>
<td>4.14</td>
<td>4.25</td>
</tr>
<tr>
<td>Strategic Plans</td>
<td>4.11</td>
<td>4.94</td>
<td>4.21</td>
<td>3.82</td>
<td>4.27</td>
</tr>
<tr>
<td>Unannounced Product Specs</td>
<td>2.94</td>
<td>5.28</td>
<td>4.43</td>
<td>4.82</td>
<td>4.36</td>
</tr>
<tr>
<td>2nd Party Information</td>
<td>5.17</td>
<td>3.39</td>
<td>5.59</td>
<td>6.23</td>
<td>5.34</td>
</tr>
<tr>
<td>Prototypes</td>
<td>5.06</td>
<td>6.61</td>
<td>4.79</td>
<td>5.59</td>
<td>5.51</td>
</tr>
<tr>
<td>Manufacturing Data</td>
<td>5.53</td>
<td>6.94</td>
<td>4.38</td>
<td>6.18</td>
<td>5.76</td>
</tr>
<tr>
<td>Average Score</td>
<td>4.79</td>
<td>4.71</td>
<td>4.81</td>
<td>4.96</td>
<td>4.74</td>
</tr>
</tbody>
</table>

While customer lists/data were thought to pose the greatest risk to revenue loss they in fact accounted for just one percent of reported losses. There were 296 incidents of customer lists/data loss, however, the total value assigned to those losses was only $13,190,000.

It would appear that companies in Manufacturing perceive the revenue impact greater, but that is deceiving. When only information types directly related to their business are included in the assessment, the Financial/Insurance group potential goes from 4.71 to 3.47.

High Technology respondents believe their greatest potential losses derive from unauthorized disclosure of proprietary product specifications. The greatest potential losses for Financial/Insurance respondents, are considered to be from customer lists and data. Manufacturing noted substantially more concern over research and development information rather than manufacturing data itself, even though actual losses were nearly three times higher for manufacturing data than R&D information. Services firms were most concerned about losses of strategic plans and roadmaps.

Companies with revenues over $15 billion and companies with very high percentages of temporary employees generally seemed more concerned about losses of research and development. Companies with revenues less than $5 billion were most concerned about losses of financial data.

6. During the past year, please indicate the approximate number of times that your company engaged in each of the following activities:

1) Litigation to enforce IP rights;
2) Inspecting competing products to determine if they infringe on IP rights;
3) Hiring an outside firm to evaluate potential infringements;
4) Hiring a firm to determine if the organization was infringing on others IP rights.

Most respondents did not report any engagements in IP litigation, although High Technology organizations seemed to have a higher propensity toward IP litigation than the other Industry segments. Likewise, only High Technology was reported to have engaged in inspecting a competing product to determine whether it infringed on patents or other IP rights. None of the industry segments were especially likely to hire outside firms to evaluate potential infringements or to determine if the company was infringing on others IP rights.

7. What percent of all IP lawsuits involving your company are currently pending?

The responses indicate that of those who reported IP litigation, most organizations have between 0-25 percent of all IP lawsuits currently pending. This may indicate that the majority of suits have been settled.
8. What percent of all IP lawsuits does your company generally settle before trial?
The responses indicate that about half of the IP lawsuits involving the company are settled before trial.

9. How many IP negotiations does your company currently have underway to avoid litigation?
Most respondents, regardless of industry segment had few pending suits and reported they generally settled between 26-50 percent of IP lawsuits prior to trial. High Technology companies were more likely than others to engage in IP negotiations to avoid litigation, but this did not appear to be a widespread practice.

10. How often does your company value intellectual property?
(1 — never, 2 — rarely, 3 — once a year, 4 — more than once a year)

<table>
<thead>
<tr>
<th>Industry Category</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Technology</td>
<td>2.33</td>
</tr>
<tr>
<td>Financial/Insurance</td>
<td>1.89</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>2.61</td>
</tr>
<tr>
<td>Services</td>
<td>2.37</td>
</tr>
<tr>
<td>Average</td>
<td>2.30</td>
</tr>
</tbody>
</table>

Few organizations engage in any sort of regular review of their intellectual property valuations. The most common answers were that IP is never or rarely valued. Somewhat surprisingly, Manufacturing organizations appeared more likely to engage in a more formal and scheduled process than High Technology companies. Large organizations (those over $15 billion in revenues), were more likely to have a process whereby on at least an annual basis IP is valued.

11. Which item MOST FREQUENTLY causes a valuation of intellectual property?
(1 — Most Frequent, 4 — Least Frequent)

<table>
<thead>
<tr>
<th>Industrial Category</th>
<th>Litigation</th>
<th>Transactions</th>
<th>Transfer Pricing</th>
<th>Licensing Agreements</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Technology</td>
<td>2.06</td>
<td>2.06</td>
<td>2.18</td>
<td>2.81</td>
<td>2.15</td>
</tr>
<tr>
<td>Financial/Insurance</td>
<td>2.39</td>
<td>2.39</td>
<td>2.28</td>
<td>2.38</td>
<td>2.38</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>1.84</td>
<td>2.32</td>
<td>1.87</td>
<td>2.03</td>
<td>2.02</td>
</tr>
<tr>
<td>Services</td>
<td>2.32</td>
<td>2.32</td>
<td>1.74</td>
<td>2.63</td>
<td>2.45</td>
</tr>
<tr>
<td>Average</td>
<td>2.13</td>
<td>2.27</td>
<td>2.02</td>
<td>2.46</td>
<td>2.33</td>
</tr>
</tbody>
</table>

Litigation and transactions (such as mergers and acquisitions or divestitures) are the most common factors cited by respondents for events that trigger an IP valuation. Manufacturing respondents appeared to value information for cause more frequently than the other three groups.

12. Who is responsible for valuing intellectual property in your company?
Attorneys, especially in-house counsel, are more than twice as likely to be responsible for valuing IP as either the CFO or outside experts. Although this appears to be a common practice, attorneys may not have all the necessary training, experience or tools to perform the more complex methodologies that are now generally available to generate accurate IP valuations.

13. The THREE most important factors considered when valuing intellectual property.

<table>
<thead>
<tr>
<th>Industrial Category</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Technology</td>
<td>Competitive Advantage</td>
<td>Incremental Profit</td>
<td>R&amp;D Costs</td>
</tr>
<tr>
<td>Financial/Insurance</td>
<td>Competitive Advantage</td>
<td>Incremental Profit</td>
<td>Other licensing agreements</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>Competitive Advantage</td>
<td>R&amp;D Costs</td>
<td>Royalties earned from licensing</td>
</tr>
<tr>
<td>Services</td>
<td>Competitive Advantage</td>
<td>Incremental Profit</td>
<td>R&amp;D Costs</td>
</tr>
</tbody>
</table>
In valuing IP, respondents indicated that the most important factor considered is how much it contributes to competitive advantage. In descending order of importance, respondents indicated the following when asked to rank the most important factors in valuing IP: the incremental profit associated with the IP; research and development costs in creating the IP; royalties that could be earned by licensing out the IP; and the benefits the IP would bring to other license agreements covering similar technology.

14. The THREE most important factors considered when valuing damages associated with the theft of IP:

<table>
<thead>
<tr>
<th>Industrial Category</th>
<th>1st</th>
<th>2nd</th>
<th>3rd</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Technology</td>
<td>Loss of Competitive Advantage</td>
<td>Loss of Market Share</td>
<td>Loss of Sales</td>
</tr>
<tr>
<td>Financial/Insurance</td>
<td>Loss of Competitive Advantage</td>
<td>Loss of Market Share</td>
<td>Loss of Sales</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>Loss of Sales</td>
<td>Loss of Market Share</td>
<td>Loss of Competitive Advantage</td>
</tr>
<tr>
<td>Services</td>
<td>Loss of Competitive Advantage</td>
<td>Loss of Market Share</td>
<td>Loss of Sales</td>
</tr>
</tbody>
</table>

Respondents indicated that when valuing IP thefts, the most important factor they consider is loss of competitive advantage; loss of market share is second; and loss of sales was the third most common response.

15. Which regulatory groups require your company to protect information?

(Multiple answers are permitted)

The U.S. Federal Government appears to have the largest impact on companies from a regulatory perspective, being cited more than twice as often as the other choices. However, in the very near future this issue will become much more complex as new and more extensive privacy laws impact the information flow facilitated by electronic commerce. This is an especially important issue for US companies doing business in the European Union. Notably, 31 respondents indicated that no regulatory authority required them to protect their company's proprietary information.

<table>
<thead>
<tr>
<th>Industrial Category</th>
<th>Federal</th>
<th>State</th>
<th>Local</th>
<th>None</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Technology</td>
<td>11</td>
<td>4</td>
<td>2</td>
<td>7</td>
</tr>
<tr>
<td>Financial/Insurance</td>
<td>15</td>
<td>11</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>15</td>
<td>4</td>
<td>1</td>
<td>12</td>
</tr>
<tr>
<td>Services</td>
<td>11</td>
<td>8</td>
<td>2</td>
<td>10</td>
</tr>
<tr>
<td>Totals</td>
<td>53</td>
<td>27</td>
<td>8</td>
<td>21</td>
</tr>
</tbody>
</table>

16. How often does company take the precautions listed below to prevent information loss?

(1 - Always; 2 - Sometimes; 3 - Rarely; 4 - Never)

To facilitate discussion, answers in these areas were grouped into administrative, physical and information systems security as follows:

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Security Training upon Employment</td>
<td>Prevent Unauthorized Access to Physical Spaces</td>
<td>Use Screen Saver Passwords</td>
<td></td>
</tr>
<tr>
<td>Prevent Unauthorized Access to Physical Spaces</td>
<td>Use Screen Saver Passwords</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use Screen Saver Passwords</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

This was not meant to be an exhaustive list of information protection measures, but a representative sampling. Based on these groupings, respondents are most likely to implement information systems security measures to protect information and least likely to consider physical measures listed above.

<table>
<thead>
<tr>
<th>Industrial Category</th>
<th>Administration</th>
<th>Physical</th>
<th>IS</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Technology</td>
<td>1.85</td>
<td>1.84</td>
<td>1.74</td>
<td>1.74</td>
</tr>
<tr>
<td>Financial/Insurance</td>
<td>1.85</td>
<td>1.88</td>
<td>1.66</td>
<td>1.73</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>1.74</td>
<td>1.88</td>
<td>1.69</td>
<td>1.77</td>
</tr>
<tr>
<td>Services</td>
<td>2.04</td>
<td>1.80</td>
<td>2.02</td>
<td>1.95</td>
</tr>
<tr>
<td>Averages</td>
<td>1.82</td>
<td>1.85</td>
<td>1.72</td>
<td>1.79</td>
</tr>
</tbody>
</table>

Financial/Insurance respondents took slightly more precautions while the Services group took the least.
17. For each of the following statements, indicate whether you strongly agree (1), somewhat agree (2), somewhat disagree (3), strongly disagree (4), or have no opinion (5).

17(a). Information security is a priority within my company.
No group of respondents answered that they "strongly agree", and thus no group claimed very strong management support. However, the High Technology respondents indicate that information security is more of a priority than in the other three groups. This group had the largest number of reported incidents for the survey, which may have influenced the score. Financial/Insurance companies were a close second. Services respondents indicated that they only somewhat agree that this is a priority.

17(b). The Internet, networks and computers have created significant new threats.
Regardless of the industry, many respondents indicated that they "strongly agree" that the Internet, networks, and computers have created significant new threats. It seems that respondents acknowledge that the drive to computerize and connect company systems to the global Internet is a new risk factor that deserves serious attention from those responsible for protecting the organization's intellectual property and sensitive proprietary information. Although all industry groups displayed a high degree of concern, the Services group showed incrementally more agreement. This may derive from a concern that the "product" of such an organization may be dependent on reports, models, and other computerized intangibles rather than physical product.

17(c). Information losses are always reported to law enforcement.
There appears to be almost universal agreement on this issue. Given the relatively strong results above (where 1 represents always and 5 never) it appears that law enforcement is not receiving many of the information loss incidents that are known to the responding organizations. This could be due to many factors. Perhaps local, state and federal agencies are perceived as being ill-equipped to handle the magnitude of the problem. The complexity and immediate nature of these issues create a quandary for those responsible for protecting the organization's intellectual property and sensitive information.

17(d). My company's temporary and contract staffs have complete background investigations.
While on-site contractors are considered to be one of the greatest threats to organizational information, most companies did not require these people to undergo background checks. Background investigations represent a level of "due diligence" easily available to US-based organizations. The failure to ensure consistency between standards applied to the regular and temporary/contract staffs creates a gap that could expose the organization's key IP and proprietary information to people who have a history of committing illegal acts.
17 (cont'd). For each of the following statements, indicate whether you strongly agree (1), somewhat agree (2), somewhat disagree (3), strongly disagree (4), or have no opinion (5).

17(a). Management takes necessary precautions to prevent information loss.

There is a significant divergence between these responses and the ones in 17(a). The difference indicates that existing programs probably have some degree of management support, but that in practice, precautions to prevent information loss may not always be followed. Taken together these two responses seem to show that even large companies have yet to link strong management commitment to protection and consistent compliance with precautions needed to safeguard that information and prevent loss of their proprietary information and intellectual property.

17(b). OEM/partner companies provide adequate safeguards for my company's information.

These responses indicate how complicated the world of business has become. This score was seven percent lower than the earlier one about precautions within the company itself. The new on-line and increasingly outsource business environment is moving rapidly to global supply chains that involve tens or hundreds of companies working transparently to design, manufacture, and deliver goods and services to consumers around the world. Most respondents apparently believe that business partners are not doing as much to protect the company's information as they themselves do. This gap could develop from failure to communicate and/or enforce the standards of the owning company as a condition of the business relationship.

17(c). My company has effective guidelines for safeguarding proprietary information.

Guidelines designed to protect proprietary information are viewed as effective at most companies, but may not be fully implemented throughout the corporation. Consistent company-wide implementation is likely to become more difficult as corporations increasingly globalize their operations and must contend with diverse legal as well as cultural and sociological factors.

17(d). Law enforcement effectively responds to information loss incidents.

Survey respondents apparently believe that law enforcement agencies need to become more effective at investigating information loss incidents. However, information loss incidents are inherently very difficult to investigate. Without the complete cooperation of the injured party, a well-trained staff (for both the law enforcement agency and the business), and the ability to quickly respond, these investigations are virtually impossible to conduct.
17 (cont'd). For each of the following statements, indicate whether you strongly agree (1), somewhat agree (2), somewhat disagree (3), strongly disagree (4), or have no opinion (5).

17(i). Recent (within 12 months) information loss incidents could seriously affect my company.

There were fairly consistent responses indicating information loss incidents were not considered to be a serious problem. However, losses due to misappropriation or theft of trade secrets are typically much higher than losses that can be attributed to thefts of tangible products. The discrepancy may indicate there is a lack of appreciation for the extent of the problem of information loss. It seems that even security professionals do not fully appreciate that information loss is a significant issue. One danger of this ambivalent response is that information protection measures may not receive strong advocacy during budget processes. This could mean that the meager resources indicated in the last survey, (<3 percent of security budgets spent on information safeguarding), may be at serious risk of reduction if the need arises to cut budgets.

17(i). My company has effective information systems security procedures.

The respondents uniformly believe that information systems security is not completely effective in their companies. The overall score indicates a neutral position. Information systems security consists of policies, procedures, hardware, software, audits, and monitoring. One essential element not yet mentioned is administrative sanctions for not following the program. If there is no downside risk to ignoring such procedures then the entire program suffers and vulnerabilities often increase.

17(k). My company has detected eavesdropping, wiretapping or alteration of telecommunication system programming.

Eavesdropping, wiretapping or alteration of telecommunications system programming was not detected at a significant number of the responding companies. It is possible that incidents are occurring but are not detected. If respondents do not perform regular inspections, or if the inspections do not utilize equipment, procedures and personnel that are technically up-to-date, they may not detect attacks.

17(l). Temporary/contract employees are not assigned to projects or work areas containing sensitive information.

The respondents indicate that contractors and temporary workers may have nearly the same access to sensitive information as regular employees. The same problem arises with the contractors and temporaries that work for other companies such as major suppliers, vendors or sub-contractors that have access to your company sensitive data. When these comments are combined with 17(d) (which indicate few temporary or contract employees receive background investigations) it is possible that a major risk to a typical organization's critical IP and sensitive proprietary information arises from the lack of controls over the hiring and deployment of the "contingent" workforce.
17 (cont’d). For each of the following statements, indicate whether you strongly agree (1), somewhat agree (2), somewhat disagree (3), strongly disagree (4), or have no opinion (5).

17(m). Sensitive information is seriously at risk in my organization.

Finance/insurance respondents were the most concerned about their current information environment. Their concerns may stem from the governmental oversight they face. Service companies were again the least concerned. Notably, Manufacturing companies reported that they sustained the greatest proprietary information losses, yet they appear to be relatively unconcerned.

17(n). Government intelligence/business intelligence/competitive intelligence staffs have successfully targeted my company.

The respondents clearly indicate that intelligence gathering threats are of considerable concern to their companies. These answers support the proposition that known information losses remain principally an insider threat.

18. To which of the following industry groups does your company belong?

To facilitate better analysis the survey respondents were assigned to one of 4 main groups: Transportation was grouped into Manufacturing, and Wholesale or Retail Trade was grouped into Services. High Technology and Finance/Insurance remained as originally identified. The table to the right gives the numbers in each group.

19. Approximately what are your company’s annual revenues?

The responses show that the companies in this survey represent a wide range of organizations with 38 indicating they were $5 billion or less in revenues, 33 were between $6 and $15 billion and 26 were over $15 billion.
20. Approximately what percentage of your company's total workforce is comprised of full-time regulars, temporary/regular part-time staff?

The responses to this question show that the average company has about 80 percent of employees as regular full-time staff, with nearly 10 percent temporary work force as well as about 11 percent as regular staff who work a part-time schedule. A related response in question 17(b) shows that many, perhaps most, companies do not yet ensure background investigations are conducted on temporary staff. Similarly, the responses to 17(b) indicate many organizations make no effort to avoid assigning temporary or contractor employees to projects or work areas containing sensitive proprietary information. The combination of these three elements—a significant number of contract/temporary staff; with unverified backgrounds/credentials; assigned to work in an organization's most critical or sensitive areas, or projects, could ultimately be disastrous.

21. Approximately what percentage of your company's total workforce is located outside the US?

The responses to this question show that about 79 percent of the workforce of the respondent companies work in the United States, while six percent work in North America (Canada and Mexico) and 15 percent are located elsewhere in the world. This demonstrates the increasing importance of the globalization of business. It is important to consider that most global organizations support their overseas operations with a global network. This connectivity from remote non-US locations poses additional challenges to the security of sensitive proprietary information and especially for the digital forms of intellectual property. The "weakest link" in the safeguards for critical proprietary information may well be in a small representative office in another country where employees enjoy easy access to the company Intranet.

Is the Loss of Proprietary Information a Serious Problem?

While reported thefts of proprietary information and the level of concern about the threats are low, companies and the professionals dedicated to protecting their ideas should not underestimate the impact that a single incident can have on a company. If a company has just one proprietary information loss incident but that incident affects the bottom line of the organization, this can create serious competitive and financial challenges that extend far into the future.

In addition, Survey respondents are likely to under-report incidents for at least two main reasons. First, many organizations lack the means to detect such losses and procedures to investigate or document incidents when they do occur. Second, there may also be concern that reporting losses could only adversely impact the reputation of the organization if it ever became publicly known.

Forty-five percent of responding companies indicate known incidents of information loss. As such, the potential losses deriving from incidents of information loss for all respondents may exceed $4.4 billion and the potential losses may reach nearly $45 billion by straight-line extrapolation of these results to the Fortune 1000.

The types of information and the estimated losses by industry segment are also instructive. In Manufacturing, the loss of manufacturing information comprised nearly three-fourths of the total losses ($610 million of $871 million) with research and development information as the next most substantial losses in the amount of a little over $215 million.

High Technology companies reported nearly $120 million in direct losses, but the respondents reported the greatest average number of incidents with nearly 67 incidents per company with average loss per incident of about $15 million.

Services companies exhibited a more uniform distribution of losses with customer lists/data comprising about half the known losses followed by nearly equal losses from merger/acquisition and strategic planning types of information. Interestingly, the Services companies reported many incidents (356), more than three times the manufacturing incidents, but the average losses per incident were less than $20,000 per event.
The number of reported incidents per month has increased dramatically within the last 17 months.

Financial/Insurance companies reported the smallest total number of incidents but the average losses per event were nearly $350,000.

If the reported figures are accurate, then the estimated dollar loss in US-based companies from these types of events may exceed $40 billion annually. This estimate tracks closely with numbers that the Federal Bureau of Investigation (FBI) and other authorities have prepared. This is a large number and should be a major concern for any company. However, it is important to appreciate that this precise number of the losses is much less important than the fact that losses occur in every industry and that many may be preventable.

The most surprising result revealed by this survey is that many, perhaps most, American companies do not appear to be taking steps to value their information and intellectual properties. In the absence of some sort of assessed value, it is difficult to know how much of corporate assets are at risk or whether the organization is making appropriate investments in protecting proprietary information and other valuable intellectual properties.

At present, random circumstances, such as mergers and acquisitions, appear to drive most valuation efforts. Although at present, there is no commonly available procedure for valuing IP, it is frequently required and accomplished during licensing negotiations, as well as for litigation when it is known or suspected valuable IP may have been stolen or misappropriated.

**What Should Be Done to Protect Proprietary Information?**

A well-executed safeguarding proprietary information (SPI) protection program should commence with an inventory of the key intellectual assets of the organization, as well as valuation of these assets. Once this is accomplished, the organization should perform a risk assessment and determine which assets are adequately protected and which may be at risk. In the inventory and risk assessment it is important to consider the impact of the global Internet and the increasing digitalization of critical proprietary assets.

Basic protection measures remain necessary. All employees (permanent, contract and regular staff) should be subject to background investigations and required to sign non-disclosure agreements that clearly enumerate the organization's ownership rights over all forms of proprietary information. Physical restrictions, especially over visitors and other outsiders, which limit access to organization facilities and to areas containing valuable proprietary information, especially trade secrets, are essential. Exit or termination interviews reminding employees of their continuing obligation to safeguard the trade secrets and proprietary information to which they had access during the course of their employment are effective at preventing many problems and are another method of communicating the organization's vigilance in defending its intellectual property rights. These reminders should parallel efforts to prevent terminating staff, and others, from physically taking hard copy documents, notebooks, prototypes and other tangible proprietary materials belonging to the organization.

The advent of the fully networked enterprise where intranets, extranets and the Internet are all used to gain competitive advantage has significantly increased the importance of integrating digital and information systems security measures into the SPI program. The corporate security professional must now work even more closely with the CIO (Chief Information Officer), the systems security staff as well as the organization law department to ensure the organization's IP protection measures address the increased risks from connectivity and the Internet. These protective measures must include efforts to identify and safeguard digital intellectual assets inside the networked enterprise. However, given the speed and propagation of information, internal security measures must be supported by an external monitoring and surveillance function.

In Question 16 of the Survey we provided 18 common precautions that a company could implement to prevent information loss, and we asked the Respondents to indicate how frequently they actually used such measures. Although the result showed that most organizations are using most of these measures at least some of the time, this is alarming because it is not enough. A well-executed SPI program would use all of these measures most of the time. As a group, the Services firms generally appear to have the most work to do, while Financial Services/Insurance organizations arguably claim the best compliance.
Conclusions from the 1998 Survey

The loss of proprietary information is a serious threat facing American industry.

This threat applies in both global and domestic marketplaces. Loss of intellectual property and sensitive proprietary information is a continuing threat to the health and competitiveness of the American economy. The current survey identifies nearly $45 billion worth of proprietary information lost in a 17-month period.

Those with a trusted relationship to the company pose a serious threat.

In contrast to our previous surveys, this Survey reveals that it is not current or former employees that are considered to be the greatest threat to an organization’s proprietary information and intellectual property. This year, outside contractors and OEMs have been identified as posing the most serious threat to proprietary information. This result parallels many of the cases brought under the Economic Espionage Act of 1996. In several of these cases the individuals indicted have been either a contracted staff member or a temporary employee of the victimized company.

The Internet and associated technologies are perceived as significant threats to every company’s ability to protect the confidentiality of their proprietary information.

Respondents strongly agreed that the Internet, networks and computers and related technologies have created significant new threats to sensitive proprietary information. It is now common that 50 percent or more of the value of companies derives from their intangible assets, primarily their proprietary information, trade secrets and proprietary knowledge. Since 90 percent or more of these assets can be found in digital form in the enterprise, the advent of the fully networked organization can create huge risks to these digital assets.

Businesses of all sizes are affected.

Even though the majority of the reporting businesses are relatively large, having $6-15 billion or greater annual revenues, smaller companies were also affected by information loss. This multifaceted issue affects them all because every size and type of business has sensitive proprietary information such as customer lists, customer preferences, pricing information, innovations, future business plans, and projected sales and revenues figures that are at risk of theft or misappropriation.

About the Respondents

The survey received responses from 97 qualified companies, which equals to nearly a 10 percent response rate for the Fortune 1000. There were 26 Services, 21 Finance/Insurance, 20 High Technology, and 30 Manufacturing companies. The typical responding company has 80 percent of its staff working in the United States.

The annual revenue breakdown of respondents is as follows: 40 percent had revenues of less than $5 billion, 33 percent had revenues between $6 billion and 15 billion, and 27 percent were over $15 billion.)

As in past surveys, larger companies submitted the preponderance of responses. Because the survey forms are sent to Fortune 1,000 companies, the survey is prejudiced toward companies with large revenues.

Employees

Full-time personnel average 80 percent versus 9.2 percent part-time employees and 11.2 percent contract staff. One of the details that emerges upon close study of the responses is that there are some areas where temporary and contract workers may be creating avoidable risks for company. When considering threats to trade secrets and efforts to manage risk to proprietary information, distinctions between kinds of workers are increasingly important.

Acknowledgments

This survey is the latest in a continuing series sponsored by ASIS International and is the first to have been conducted with PricewaterhouseCoopers LLP. The ASIS Safeguarding Proprietary Information Committee members wish to thank ASIS, PricewaterhouseCoopers LLP, the Society’s membership, and especially the companies that participated in the survey. In addition, Dan Swartwood deserves special recognition for his contribution to the analysis and interpretation of the survey responses.

This survey seeks to broaden and deepen the understanding of security professionals, the government, and the business community concerning the importance and methods of safeguarding critical intellectual properties and proprietary information. This survey is designed to provide benchmark data on proprietary information loss, its impact, or methods of managing risk to proprietary information. Most of the material reported in these surveys is extremely sensitive. We appreciate the continued support of security professionals who candidly assessed their own companies’ performance and shortcomings. Without this candid reporting, the value of these surveys would be substantially diminished. According to the PricewaterhouseCoopers Survey Center, the Survey results are statistically valid plus or minus 10 percent. The reader should be cautious in extrapolating from only the responses received to specific conclusions for every company in the Fortune 1000.
Survey Methodology

The survey was conducted under the direction of William C. Boni, of PricewaterhouseCoopers Investigations LLC, and the members of the ASIS Standing Committee on Safeguarding Proprietary Information led by Mr. James O'Neil from United Technologies Corporation. Technical support was provided by the PricewaterhouseCoopers Survey Center in Bethesda, Md. Dan Sweattwood and Bill Boni with the assistance of the PricewaterhouseCoopers Survey Center drafted the survey instrument and solicited suggestions to improve it from the Committee members.

ASIS provided a mailing list of Fortune 1,000 companies and a PricewaterhouseCoopers list of General Counsel of the Fortune 500 companies. The surveys were mailed to the senior security professional and General Counsel by name. If there was no known name for the security director or general counsel it was sent generically to the security director or senior security professional of the organization. A card was provided to allow survey participants to acknowledge their participation in the survey while keeping their responses anonymous and private.

PricewaterhouseCoopers statistical and research expertise has been essential to complete this report, and to support the validity of the survey findings. As in any survey, the numbers presented do not reflect 100 percent of the respondents. Most respondents declined to answer at least some of the 21 questions.

As in the past, there was no way to identify any response with any company. The PricewaterhouseCoopers Survey Center received the survey instruments and created the survey spreadsheet. After the data was entered and validated, the surveys were destroyed. The authors were then provided the data in Microsoft Excel. The confidential list of participating companies is maintained by ASIS.

The survey covered a 17-month period, January 1, 1997, through June 1, 1998.

© Copyright 1999 American Society for Industrial Security, International and PricewaterhouseCoopers LLP.

Selected References

Web Sites:

The following web sites, although not all inclusive, are excellent resources that offer security practitioners a wealth of information on counterintelligence, economic espionage, counterterrorism, security, legal and infrastructure protection.

Defense Security Service — www.dss.mil
Extranet for Security Professionals — www.xsp.org
Embassy Page — www.embpage.org
FBI AN/ISR — www.fbi.gov/programs/ansis/ansir
Intellectual Property Owners Association — www.ipo.org
National Counterintelligence Center — www.ncic.gov
National Security Institute — www.nsi.org
National Infrastructure Protection Center — www.nipc.gov
Naval Criminal Investigative Service — www.ncbi.gov
Overseas Security Advisory Council — www.dss.state.gov
PricewaterhouseCoopers — www.pwcglobal.com
Travel Warnings and Consular Information Sheets — www.travel.state.gov
U.S. Department of State Bureau of Consular Affairs — www.travel.state.gov

Selected References

Web Sites:

The following web sites, although not all inclusive, are excellent resources that offer security practitioners a wealth of information on counterintelligence, economic espionage, counterterrorism, security, legal and infrastructure protection.

Defense Security Service — www.dss.mil
Extranet for Security Professionals — www.xsp.org
Embassy Page — www.embpage.org
FBI AN/ISR — www.fbi.gov/programs/ansis/ansir
Intellectual Property Owners Association — www.ipo.org
National Counterintelligence Center — www.ncic.gov
National Security Institute — www.nsi.org
National Infrastructure Protection Center — www.nipc.gov
Naval Criminal Investigative Service — www.ncbi.gov
Overseas Security Advisory Council — www.dss.state.gov
PricewaterhouseCoopers — www.pwcglobal.com
Travel Warnings and Consular Information Sheets — www.travel.state.gov
U.S. Department of State Bureau of Consular Affairs — www.travel.state.gov

Selected References

Web Sites:

The following web sites, although not all inclusive, are excellent resources that offer security practitioners a wealth of information on counterintelligence, economic espionage, counterterrorism, security, legal and infrastructure protection.

Defense Security Service — www.dss.mil
Extranet for Security Professionals — www.xsp.org
Embassy Page — www.embpage.org
FBI AN/ISR — www.fbi.gov/programs/ansis/ansir
Intellectual Property Owners Association — www.ipo.org
National Counterintelligence Center — www.ncic.gov
National Security Institute — www.nsi.org
National Infrastructure Protection Center — www.nipc.gov
Naval Criminal Investigative Service — www.ncbi.gov
Overseas Security Advisory Council — www.dss.state.gov
PricewaterhouseCoopers — www.pwcglobal.com
Travel Warnings and Consular Information Sheets — www.travel.state.gov
U.S. Department of State Bureau of Consular Affairs — www.travel.state.gov

Selected References

Web Sites:

The following web sites, although not all inclusive, are excellent resources that offer security practitioners a wealth of information on counterintelligence, economic espionage, counterterrorism, security, legal and infrastructure protection.

Defense Security Service — www.dss.mil
Extranet for Security Professionals — www.xsp.org
Embassy Page — www.embpage.org
FBI AN/ISR — www.fbi.gov/programs/ansis/ansir
Intellectual Property Owners Association — www.ipo.org
National Counterintelligence Center — www.ncic.gov
National Security Institute — www.nsi.org
National Infrastructure Protection Center — www.nipc.gov
Naval Criminal Investigative Service — www.ncbi.gov
Overseas Security Advisory Council — www.dss.state.gov
PricewaterhouseCoopers — www.pwcglobal.com
Travel Warnings and Consular Information Sheets — www.travel.state.gov
U.S. Department of State Bureau of Consular Affairs — www.travel.state.gov

Selected References

Web Sites:

The following web sites, although not all inclusive, are excellent resources that offer security practitioners a wealth of information on counterintelligence, economic espionage, counterterrorism, security, legal and infrastructure protection.

Defense Security Service — www.dss.mil
Extranet for Security Professionals — www.xsp.org
Embassy Page — www.embpage.org
FBI AN/ISR — www.fbi.gov/programs/ansis/ansir
Intellectual Property Owners Association — www.ipo.org
National Counterintelligence Center — www.ncic.gov
National Security Institute — www.nsi.org
National Infrastructure Protection Center — www.nipc.gov
Naval Criminal Investigative Service — www.ncbi.gov
Overseas Security Advisory Council — www.dss.state.gov
PricewaterhouseCoopers — www.pwcglobal.com
Travel Warnings and Consular Information Sheets — www.travel.state.gov
U.S. Department of State Bureau of Consular Affairs — www.travel.state.gov

Selected References

Web Sites:

The following web sites, although not all inclusive, are excellent resources that offer security practitioners a wealth of information on counterintelligence, economic espionage, counterterrorism, security, legal and infrastructure protection.

Defense Security Service — www.dss.mil
Extranet for Security Professionals — www.xsp.org
Embassy Page — www.embpage.org
FBI AN/ISR — www.fbi.gov/programs/ansis/ansir
Intellectual Property Owners Association — www.ipo.org
National Counterintelligence Center — www.ncic.gov
National Security Institute — www.nsi.org
National Infrastructure Protection Center — www.nipc.gov
Naval Criminal Investigative Service — www.ncbi.gov
Overseas Security Advisory Council — www.dss.state.gov
PricewaterhouseCoopers — www.pwcglobal.com
Travel Warnings and Consular Information Sheets — www.travel.state.gov
U.S. Department of State Bureau of Consular Affairs — www.travel.state.gov

Selected References

Web Sites:

The following web sites, although not all inclusive, are excellent resources that offer security practitioners a wealth of information on counterintelligence, economic espionage, counterterrorism, security, legal and infrastructure protection.

Defense Security Service — www.dss.mil
Extranet for Security Professionals — www.xsp.org
Embassy Page — www.embpage.org
FBI AN/ISR — www.fbi.gov/programs/ansis/ansir
Intellectual Property Owners Association — www.ipo.org
National Counterintelligence Center — www.ncic.gov
National Security Institute — www.nsi.org
National Infrastructure Protection Center — www.nipc.gov
Naval Criminal Investigative Service — www.ncbi.gov
Overseas Security Advisory Council — www.dss.state.gov
PricewaterhouseCoopers — www.pwcglobal.com
Travel Warnings and Consular Information Sheets — www.travel.state.gov
U.S. Department of State Bureau of Consular Affairs — www.travel.state.gov

Selected References

Web Sites:

The following web sites, although not all inclusive, are excellent resources that offer security practitioners a wealth of information on counterintelligence, economic espionage, counterterrorism, security, legal and infrastructure protection.

Defense Security Service — www.dss.mil
Extranet for Security Professionals — www.xsp.org
Embassy Page — www.embpage.org
FBI AN/ISR — www.fbi.gov/programs/ansis/ansir
Intellectual Property Owners Association — www.ipo.org
National Counterintelligence Center — www.ncic.gov
National Security Institute — www.nsi.org
National Infrastructure Protection Center — www.nipc.gov
Naval Criminal Investigative Service — www.ncbi.gov
Overseas Security Advisory Council — www.dss.state.gov
PricewaterhouseCoopers — www.pwcglobal.com
Travel Warnings and Consular Information Sheets — www.travel.state.gov
U.S. Department of State Bureau of Consular Affairs — www.travel.state.gov
ASIS Safeguarding Proprietary Information Committee Members

The following persons are SPI Committee members:

James M. O'Neil (Chairman)
Manager, Security
United Technologies Corporation
860-728-5681

Stephen F. Argubright
Staff Officer
National Counterintelligence Center
703-874-4073

William C. Boni, Jr.
Director, Information Protection Services
PricewaterhouseCoopers Investigations
213-356-9647

Donald R. Charlesworth, CPP
Security Manager
Sandia National Laboratories
925-294-3537

Donald E. Greenwood
Director, Security Consulting Services
Swales, Sheridan, Stade & Associates
713-361-4750

William Halliday
Corporate Security
Manny Alas
Partner
New York
212-596-5882

Jonny Frank
Principal
New York
212-596-8390

Thomas Golden
Partner
Chicago
312-940-2799

Chuck Huxter
Partner
New York
212-598-8680

Mac Henderson
Partner
Washington, D.C.
202-822-4035

Neal Hochberg
Partner
Miami
305-373-6218

James Hunt
Partner
Los Angeles
213-236-4520

Jo Ann Jury
Partner
New York
212-598-7519

Larry Kantor
Partner
Dallas
214-794-5238

Orlando Yarbrough
Partner
Chicago
312-540-2960

Robert Lindquist
Partner
Washington, D.C.
202-822-5590

ASIS Safeguarding Proprietary Information Committee Members

The following persons are SPI Committee members:

James M. O'Neil (Chairman)
Manager, Security
United Technologies Corporation
860-728-5681

Stephen F. Argubright
Staff Officer
National Counterintelligence Center
703-874-4073

William C. Boni, Jr.
Director, Information Protection Services
PricewaterhouseCoopers Investigations
213-356-9647

Donald R. Charlesworth, CPP
Security Manager
Sandia National Laboratories
925-294-3537

Donald E. Greenwood
Director, Security Consulting Services
Swales, Sheridan, Stade & Associates
713-361-4750

William Halliday
Corporate Security
Manny Alas
Partner
New York
212-596-5882

Jonny Frank
Principal
New York
212-596-8390

Thomas Golden
Partner
Chicago
312-940-2799

Chuck Huxter
Partner
New York
212-598-8680

Mac Henderson
Partner
Washington, D.C.
202-822-4035

Neal Hochberg
Partner
Miami
305-373-6218

James Hunt
Partner
Los Angeles
213-236-4520

Jo Ann Jury
Partner
New York
212-598-7519

Larry Kantor
Partner
Dallas
214-794-5238

Orlando Yarbrough
Partner
Chicago
312-540-2960

Robert Lindquist
Partner
Washington, D.C.
202-822-5590

PricewaterhouseCoopers Investigations LLC

United States

Manny Alas
Partner
New York
212-596-5882

Jonny Frank
Principal
New York
212-596-8390

Thomas Golden
Partner
Chicago
312-940-2799

Chuck Huxter
Partner
New York
212-598-8680

Mac Henderson
Partner
Washington, D.C.
202-822-4035

Neal Hochberg
Partner
Miami
305-373-6218

James Hunt
Partner
Los Angeles
213-236-4520

Jo Ann Jury
Partner
New York
212-598-7519

Larry Kantor
Partner
Dallas
214-794-5238

Orlando Yarbrough
Partner
Chicago
312-540-2960

Robert Lindquist
Partner
Washington, D.C.
202-822-5590

PricewaterhouseCoopers Investigations LLC

United States

Manny Alas
Partner
New York
212-596-5882

Jonny Frank
Principal
New York
212-596-8390

Thomas Golden
Partner
Chicago
312-940-2799

Chuck Huxter
Partner
New York
212-598-8680

Mac Henderson
Partner
Washington, D.C.
202-822-4035

Neal Hochberg
Partner
Miami
305-373-6218

James Hunt
Partner
Los Angeles
213-236-4520

Jo Ann Jury
Partner
New York
212-598-7519

Larry Kantor
Partner
Dallas
214-794-5238

Orlando Yarbrough
Partner
Chicago
312-540-2960

Robert Lindquist
Partner
Washington, D.C.
202-822-5590

PricewaterhouseCoopers Investigations LLC

United States

Manny Alas
Partner
New York
212-596-5882

Jonny Frank
Principal
New York
212-596-8390

Thomas Golden
Partner
Chicago
312-940-2799

Chuck Huxter
Partner
New York
212-598-8680

Mac Henderson
Partner
Washington, D.C.
202-822-4035

Neal Hochberg
Partner
Miami
305-373-6218

James Hunt
Partner
Los Angeles
213-236-4520

Jo Ann Jury
Partner
New York
212-598-7519

Larry Kantor
Partner
Dallas
214-794-5238

Orlando Yarbrough
Partner
Chicago
312-540-2960

Robert Lindquist
Partner
Washington, D.C.
202-822-5590
Appendix B:

Written by Leonard Fuld, a pioneer in the Competitive Intelligence (CI) field and founder/president of Fuld & Company, a Cambridge, MA consulting firm.

Competitive Intelligence Is and Is Not:
Ten descriptions of what CI is and does for a company and ten common misconceptions about CI; found at <www.fuld.com>.
### Competitive Intelligence Is...

| 1 | Information that has been analyzed to the point where you can make a decision. |
| 2 | A tool to alert management to early warning of both threats and opportunities. |
| 3 | A means to deliver reasonable assessments. Competitive intelligence offers approximations and best views of the market and the competition. It is not a peek at the rival's financial books. Reasonable assessments are what modern entrepreneurs such as Richard Branson, Bill Gates, and Michael Dell need, want, and use on a regular basis. They don't expect every detail, just the best assessment at the time. |
| 4 | Comes in many flavors. Competitive intelligence can mean many things to many people. A research scientist sees it as a heads-up on a competitor's new R&D initiatives. A salesperson considers it insight on how his or her company should bid against another firm in order to win a contract. A senior manager believes intelligence to be a long-term view on a marketplace and its rivals. See our Strategic Intelligence Organizer tool on fuld.com for examples of the many flavors of competitive intelligence and tips on how to develop it. |

### Competitive Intelligence Is Not...

| 1 | Spying. Spying implies illegal or unethical activities. While spying does take place, it is a rare activity. Think about it; corporations do not want to find themselves in court, nor do they want to upset shareholders. For the most part, you will find spies in espionage novels, not in the executive suite. |
| 2 | A crystal ball. There is no such thing as a true forecasting tool. Intelligence does give corporations good approximations of reality, near- and long-term. It does not predict the future. |
| 3 | Database search. Databases offer just that — data. Of course it is wonderful to have these remarkable tools. Nevertheless, databases do not massage or analyze the data. They certainly do not replace human beings who need to make decisions by examining the data and applying their common sense, experience, analytical tools, and intuition. |
| 4 | The Internet or rumor chasing. The Net is primarily a communications vehicle, not a deliverer of intelligence. You can find hints at competitive strategy, but you will also uncover rumors disguised as fact, or speculation dressed up as reality. Be wary of how you use or misuse the Net. Its reach is great, but you need to sift, sort, and be selective on its content. |
A way for companies to improve their bottom line. Companies, such as NutraSweet, have attributed many millions of dollars in earned revenue to their intelligence usage. See our CI Success Stories on fuld.com for over 100 excerpts telling how companies have used CI successfully.

Paper. Paper is the death of good intelligence. Think face-to-face discussion or a quick phone call if you can, rather than paper delivery. Never equate paper with competitive intelligence. Yes, you must have a way to convey critical intelligence. Unfortunately, many managers think that by spending countless hours on computer-generated slides, charts and graphs, and footnoted reports, they have delivered intelligence. All they have managed to do is to slow down the delivery of critical intelligence. In the process, they have likely hidden the intelligence by over-analyzing it. Remember: Paper cannot argue a point — you can.

A way of life, a process. If a company uses CI correctly, it becomes a way of life for everyone in the corporation — not just the strategic planning or marketing staff. It is a process by which critical information is available for anyone who needs it. That process might be helped by computerization, but its success rests upon the people and their ability to use it.

A job for one, smart person. A CEO might appoint one individual to oversee the CI process, but that one person cannot do it all. At best, the CI Ringmaster, the coordinator of the program, keeps management informed and ensures that others in the organization become trained in ways to apply this tool within each of their SBUs.

Part of all best-in-class companies. In my 20 years of consulting in this arena, I have witnessed that high-quality, best-in-class corporations apply competitive intelligence consistently. The Malcolm Baldridge Quality Award, the most prestigious total quality award for American corporations, includes the gathering and use of external market information (a.k.a. CI) as one of its winning qualifications.

An invention of the 20th century. CI has been around as long as business itself. It may have operated under a different name, or under no name at all, but it was always present. Just review the story surrounding 19th century British financier Nathan Rothschild, who managed to corner the market on British government securities by receiving early warning of Napoleon's defeat at Waterloo. He used carrier pigeons, the E-mail of his day. He knew the information to watch and how to make sense of it; in the end, he used this intelligence to make a killing in the market.
Directed from the executive suite. The best-in-class intelligence efforts receive their direction and impetus from the CEO. While the CEO may not run the program, he dedicates budget and personnel; most important, he promotes its use.

Software. Software does not in and of itself yield intelligence. The CI market is hot, and numerous software houses are producing products for the intelligence marketplace. Many more are repositioning existing software — in particular, data warehousing and data mining packages — for use in intelligence. Software has become an important weapon in the CI arsenal, but it does not truly analyze. It collects, contrasts, and compares. True analysis is a process of people reviewing and making sense of the information.

Seeing outside yourself. Companies that successfully apply competitive intelligence gain an ability to see outside themselves. CI pushes the not-invented-here syndrome out the window.

A news story. Newspaper or television reports are very broad and are not timely enough for managers concerned with specific competitors and competitive issues. If a manager first learns of an industry event from a newspaper or magazine report, chances are others in the industry already learned of the news through other channels. While media reports may yield interesting sources for the CI analyst to interview, they are not always the most timely, or specific enough for critical business decisions.

Both short- and long-term. A company can use intelligence for many immediate decisions, such as how to price a product or place an advertisement. At the same time, you can use the same set of data to decide on long-term product development or market positioning.

A spreadsheet. "If it's not a number, it's not intelligence." This is an unspoken, but often thought of, refrain among managers. "If you can't multiply it, then it is not valid." Intelligence comes in many forms, only one of which is a spreadsheet or some quantifiable result. My firm has completed numerous strategic assessments, where the numbers only address one aspect of the problem. Management thinking, marketing strategy, and ability to innovate are only three among a host of issues that rely on a wide range of subjective, non-numeric intelligence.
Appendix C:

Compiled by the Society of Competitive Intelligence Professionals.

An Overview of the Competitive Intelligence (CI) Field
This PowerPoint presentation is available at <www.scip.org>.
What is Competitive Intelligence (CI)?

CI is a systematic & ethical program for gathering and analyzing information about your competitors' activities and general business trends to further your own company's goals.

What Intelligence Can Be Obtained Legally and Ethically?

80%-90% of all information is public knowledge.
What is the CI Function and Process?

Communicate

Adapted from William Y. Wilson, NextStep and Timothy W. Powell, InfoStrat.

What Principles and Skills are Needed for the Function?

Intelligence Value Creation System

Developed by SCIP in association with the Monitor Company
Where Are the Sources For CI?

Sources of CI (by extent of use)

**High use**
- Trade journals
- External (on-line) data bases
- External hard copy documents
- Employees
- Industry experts
- Trade organizations

**Moderate use**
- Sales representatives
- Customers
- Internal documents
- Internal databases/CD-ROM
- Telephone interviews

**Low use**
- Government records
- Direct observation
- Clipping services
- Security analysis
- Competitors (contact directly)
- Personal interviews
- Suppliers

**Very little use**
- Product purchasing
- Freedom of information act
- Focus groups
- Case studies
- Mail questionnaires

Based on the Society of Competitive Intelligence Professionals 1997 Salary Survey
Who Are the Best Internal Clients For CI?

Based on the Society of Competitive Intelligence Professionals 1997 Salary Survey

What Methods Are Available to Gather CI?

- Reading newspapers
- Ad hoc, reactive
- Comparative profiles
- TQM
- Benchmarking
- Baselining
- CI systems
- Fully-integrated custom field research
- Fully-utilized tracking systems
How Are Organizations Using These Methods?

- 7% of companies with dedicated CI professionals at corporate & divisions.
- Department specialists focusing on developing & using their own intelligence.
- Dedicated staffs for information organization.
- Part-time responsibility of corporate librarians; 90% of companies.

What is the Framework For Accessing, Sharing, and Utilizing CI Across the Organization?

- Decision Makers
- Collect
- Analyze
- Plan
- Apply
- Compile

CI TEAM
How Can Companies Have the Right Intelligence, But Not Share or Utilize it Effectively?

Analysis and Results Must Be:
- Responsive to Management’s Needs (even when they don’t know them)
- Focused
- Timely
- In a Usable Format

How Can You Create Structures For Using CI Effectively Within a Company?

Modes of Dissemination (In order of perceived effectiveness)
- Custom reports
- Personal communications
- Presentations
- Special memos
- E-mail
- Competitor files
- Computerized databases
- Newsletter
- Regular meetings
- Training Seminars
- Bulletin Boards
- Special Retreats

Based on the Society of Competitive Intelligence Professionals 1997 Salary Survey
How is Information Made Available But Improperly Employed at High Levels?

- Decision makers don't act in a timely manner
- Information is incorrect or incomplete
- Information is misinterpreted
- Decision makers misunderstand CI

Organizations Don't Make Decisions, People Do.

What Should You Consider When Setting Up and Maintaining an On-Going CI Process?

- Where Should CI Programs Be Located and Should There Be a Centralized CI Effort?
- What Large Should the CI Staff Be?
- What Budget Should Be Allocated to the CI Function?
- Who Do the CI Professionals Report to and Who Are Their Primary Users?
- What is the Objective of the Program and How Is It Operationalized?
How Do You Ensure That CI is Strategy Driven?

CI professionals must work for decision makers

Decision makers need to be educated on the purpose & benefits of CI

CI Professionals’ Roles Within Organizations

- Market Planning & Research: 13%
- CII Analysis: 10%
- Strategic Planning: 14%
- Info Center/Services: 12%
- R&D, Business Development, Product Planning: 25%
- Financial Planning/Counterintelligence: 26%

Based on the Society of Competitive Intelligence Professionals 1997 Salary Survey
### Who is in the CI Field?

<table>
<thead>
<tr>
<th>Type:</th>
<th>Work in:</th>
<th>Doing:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Practitioners</td>
<td>A corporation</td>
<td>Ad Hoc requests (50%) to tracking (50%)</td>
</tr>
<tr>
<td>76.8%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Vendors or</td>
<td>Independent consultants or</td>
<td>Strategy applications of developed CI on project &amp;</td>
</tr>
<tr>
<td>Consultants</td>
<td>consulting practice</td>
<td>subscription basis seminars</td>
</tr>
<tr>
<td>17.5%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Academics</td>
<td>A university or college</td>
<td>Teaching research methods. Authoring books in CI</td>
</tr>
<tr>
<td>2.1%</td>
<td></td>
<td>business. Project consulting.</td>
</tr>
<tr>
<td>Students</td>
<td>A university or college</td>
<td>Full-time studies.</td>
</tr>
<tr>
<td>3.6%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Based on the membership of the Society of Competitive Intelligence Professionals*

### CI Professionals’ Demographics

<table>
<thead>
<tr>
<th>Years in CI profession:</th>
<th>52% 1-3 years</th>
<th>17% 4-5 years</th>
<th>23% 6-12 years</th>
</tr>
</thead>
<tbody>
<tr>
<td>Professional work</td>
<td>10% 1-5 years</td>
<td>16% 6-10 years</td>
<td>42% 11-20 years</td>
</tr>
<tr>
<td>experience:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Median salary:</td>
<td>$63,000</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Size of CI staff:</td>
<td>73% 1-3 per unit</td>
<td>22% 4-10 per unit</td>
<td></td>
</tr>
<tr>
<td>Education:</td>
<td>93% university education</td>
<td>65% advanced degrees</td>
<td></td>
</tr>
</tbody>
</table>

*Based on the Society of Competitive Intelligence Professionals 1997 Salary Survey*
SCIP Membership
Growth Trend

The Industries of SCIP Members

Based on the Society of Competitive Intelligence Professionals 1997 Salary Survey
"Advantage is a better soldier than rashness."

*William Shakespeare,*
*King Henry V*

society of competitive intelligence professionals

---

"The model for management that we have right now is the opera ... yet business should be emulating a good jazz group ... you have to develop the score as you go along."

*Peter F. Drucker,*
*author and management consultant*
“We are drowning in information but starved for knowledge.”

*John Naisbitt,*
Chairman of the Naisbitt Group

“You don’t just set your compass and head south — or you will quickly run aground. Instead, you steer from point to point according to how the river is running and the obstacles that appear in your path.”

*Abraham Lincoln*
on how to govern as one would steer a riverboat
Appendix D:

Managing Sensitive Information in a Joint Venture

This overview contains specific recommendations for documentation and management of confidential information in a joint venture.

Compiled from information found in Wolf pp. 230-233.
The confidentiality agreement

The confidentiality agreement appears when the parties, even operating with the clear understanding that they are in an exploratory phase, are asked to exchange or give access to information of a confidential nature, trade secrets that should not be known by competitors. It would not be unusual for a confidentiality agreement to be executed after considerable negotiations between the parties and it is an agreement naturally prepared by legal counsel.

The confidentiality agreement has become an important complement particularly in industries or services where the secret of the business is not in patented rights or technology licenses but in trade secrets, commercial practices that cannot receive formal, written protection, such as a copyright, but that nevertheless are crucial to the success of the enterprise. A typical example is a specialized mailing list built up through the years and that is productive for mail-marketing purposes.

No information should be disclosed without a proper agreement defining the responsibility of all parties. It is not that the law requires a written agreement. A verbal agreement may be perfectly enforceable. However, if the information is of serious commercial value, the vagueness and ambiguities that characterize verbal agreements are sufficient for choosing a formal agreement instead. The agreement should be reduced to writing and the solemnity of its terms emphasized. This will contribute to its being voluntarily implemented.

Breach of a confidentiality agreement subjects the defaulting party to a claim for damages. However, this right is more theoretical than practical. When large corporations are involved, the agreement surely has an important moral force. Nevertheless, plaintiffs seeking damages for breach of the confidentiality agreement have a difficult burden of demonstrating what are the damages incurred and, if the information is disclosed to unauthorized third parties, its circulation in the commercial world cannot be prevented easily.

Inserting a statement as to the agreed-on damages for default in the confidentiality agreement may not be a valid clause, a question for local counsel, but in any event, unless the amount is very high, out of proportion to the value of the secret, it is an invitation to disclosure if the information gained is worth more than the penalty to pay.

There is a serious dilemma in confidential transactions for the seller. For the buyer to request to have access to the records and information of the seller is a normal solicitation. It may not even be possible to seriously consider a joint venture without having more information. There thus arises a conflict: If information is not revealed, there can be no further progress; if information is revealed but negotiations fail, valuable information has been given away. How can this be resolved? Two suggestions are a clear delineation as to what is the
confidential information and then its managed disclosure according to some simple rules. The possibility of damages should be considered as a last resort.

**Defining the subject matter of confidential information**

The most important subject matter is what it is that is being considered confidential. Merely stating that all information given is confidential does not contribute to clarity; nor stating that all information of a commercial nature constitutes a trade secret; nor claiming all confidential information belongs to the seller. A serious effort must be made to define as well as possible what is meant by confidential information; such a description then can be followed by general clauses of confidentiality. The more detailed the description, the more important will seem the material sought to be protected.

**The management of confidential information**

Negotiations begin. An interest is confirmed. Further information is requested. Even with an agreement, there is no need to rush to deliver all confidential information available. Certain guidelines can be established subsequent to the signing of the confidentiality agreement:

- Management should separate vital knowledge from information that is a natural activity in most companies. How to make a product is very different from where you purchase the materials. The latter is also important but not critical. Insider information then should be divulged in harmony with the advance of negotiations. As negotiations become more close to a contract, the quality of the knowledge being given can also increase, become more unique in its application.

- Information should be given only after a certain level of agreement is reached on major issues. One does not reveal confidential information merely because another party may have interest. The level of interest is difficult to determine but there surely should be agreement on price and the equity contribution of each party.

- The information can be given initially in written summaries. This establishes a reference for what areas are considered confidential and the buyer is put on notice.

- Representative information can be given. It is not necessary to furnish a copy of an entire client list broken down by city and products. Sample information can be given.

- The buyer or potential partner should have to channel his requests in a formal procedure, and if possible to the same party. This tends to make personal the assumption of the confidentiality obligation and also establishes a simpler method of proof should the condition be broken.
- For the same reason, releasing the information should be done in the same room and in a formal manner. This emphasizes the seriousness of the information being given. A rapport may develop between the participants, which contributes to honoring the promises of confidentiality given.

- A point often overlooked is a failure to place a limitation on the copies of information made and in general controlling the copy process. The more there are formalities, the more serious the information received will be considered. It would be perfectly advisable to record how many copies have been made of any item, to whom given, and when.

- The entities entitled to receive the information should be defined as narrowly as possible, for example, auditors, financial officers, attorneys, and specified categories of key personnel.

- A decision has to be made as to the consequences of a misuse of the information received. Two options are to make all parties responsible who misuse the information and the other is to have one primary party responsible, the buyer who must take the necessary precautions with third parties, such as employees. It is simpler to place the responsibility on the inquiring buyer as this is likely to be a corporation and be able to respond in damages.
Appendix E:

Competitive Intelligence and the Economic Espionage Act:
An overview of the EEA and its impact on the CI field.

Prepared by the Society for Competitive Intelligence Professionals (SCIP).
Competitive Intelligence and the Economic Espionage Act

A Policy Analysis Adopted by the SCIP Board of Directors

Society of Competitive Intelligence Professionals
1700 Diagonal Road, Suite 600
Alexandria, VA 22314 USA
www.scip.org

Copyright © 1999 by SCIP

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by and means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher.
Introduction

In October 1996, the U.S. president signed into law the Economic Espionage Act (EEA). The EEA makes stealing or obtaining trade secrets by fraud (and buying or receiving secrets so obtained) a U.S. federal crime. Upon passage of the EEA, some members of the competitive intelligence (CI) community expressed concern that the EEA could have implications for the conduct of CI.

After the passage of the EEA, SCIP organized two symposiums, one in February 1997 and another in February 1998, on the topic of CI, ethics, and law. The purpose of these events, and of several publications and articles published by SCIP, was to promote education and understanding of the law and its implications for the CI profession among SCIP’s membership and in industry at large.

Many members of the Society felt it was important to develop a clear statement to define the impact of the EEA on the CI profession and clear up any confusion about the relationship between the EEA and CI. This policy statement, the result of extensive research and consultation, addresses that relationship. The policy statement was prepared by Richard Horowitz, a SCIP member who is an attorney and private investigator. It was subsequently adopted by the SCIP board of directors and endorsed by leading legal experts. Their endorsements are also included in this booklet.

Competitive intelligence is the legal and ethical collection and synthesis of data and information to enhance business decision making. SCIP members endorse this definition.

— Ava Harth Youngblood, SCIP ’98-99 president

SCIP Code of Ethics for CI Professionals

• To continually strive to increase respect and recognition for the profession.
• To pursue one’s duties with zeal and diligence while maintaining the highest degree of professionalism and avoiding all unethical practices.
• To faithfully adhere to and abide by one’s company’s policies, objectives and guidelines.
• To comply with all applicable laws.
• To accurately disclose all relevant information, including one’s identity and organization, prior to all interviews.
• To fully respect all requests for confidentiality of information.
• To promote and encourage full compliance with these ethical standards within one’s company, with third party contractors, and within the entire profession.
Introduction to the SCIP
Policy Analysis on
Competitive Intelligence and
the Economic Espionage Act

Richard Horowitz, Esq.
Legal and Investigative Services
400 Madison Avenue, Suite 1411
New York, NY 10017, USA
Tel.: +1.212.829.8196
Fax: +1.212.829.8199
RHESQ@compuserve.com

Under the auspices of the SCIP ethics committee and as requested by the SCIP board of directors, I have prepared this policy analysis, adopted by SCIP's board of directors.

The question of the EEA's effect on CI has been an issue of concern in the CI industry. I believe that the significant difficulty for many in understanding what effect if any the EEA has on CI is that this issue reflects a confluence of law and security, two topics that are not generally included in a college or graduate school education. For example, the EEA is a statute, and a statute is not prose. Statutes are written without incorporating the underlying legal principles into their wording. The frustration many have felt after reading the EEA and still not understanding how it affects CI is because these underlying legal principles which are essential to understanding the law's application will not emerge from the text, regardless of fonts, graphics, or the statute's layout on the page.

I have always maintained that CI practitioners who act consistently with SCIP's code of ethics should not run afoul of the EEA. It is my hope that this policy analysis will assist members of the CI industry to understand why this is so. For those who would like a more in-depth analysis, see my article "The Economic Espionage Act: The Rules Have Not Changed" in the July-September 1998 volume of Competitive Intelligence Review.

I would like to thank Elkan Abramowitz, Mark Halligan, Peter Toren and the board of directors and staff of SCIP for their assistance in the preparation of this document. A special thanks to Mark, Peter and Hamilton Loeb for their assistance to me since I took an active role in this issue. In case there are any further questions, I can be reached at the address above.

Richard Horowitz

POLICY ANALYSIS
Competitive Intelligence and the
Economic Espionage Act

Prepared by Richard Horowitz, Esq.

For the board of directors of Society of Competitive Intelligence Professionals

Executive Summary

Seeking competitive information in a legal and ethical manner is an integral component of healthy competition. The EEA was enacted in order to enable federal law enforcement to investigate and prosecute acts of economic espionage. It adds federal criminal penalties to activities which were already illegal under state law. The EEA does not interfere with the way corporations are entitled to gain a competitive advantage in the marketplace by seeking information on a competitor in a legal manner.

That the EEA does not materially affect competitive intelligence (CI) does not mean that CI professionals need not be concerned about trade secret law. On the contrary, the EEA has drawn attention to the necessity of insuring that CI activities are within the parameters of trade secret law.

An understanding of trade secret law and the EEA indicates that CI professionals who have been and will continue to conduct their business in an ethical manner and consistent with established trade secret law need not be concerned about the EEA debate.

Companies that have curtailed their CI efforts out of a misplaced fear of the EEA have awarded a competitive advantage to companies whose CI activities continue unimpeded.

Background

The Society of Competitive Intelligence Professionals (SCIP) is the global professional society for practitioners of business or competitive intelligence (CI). Established in 1986, SCIP today has more than 5,000 members and continues to grow substantially year after year.

Seeking information on a competitor is an important component of healthy competition; CI is the term which has developed to describe this profession. Many corporations and executives perform this function without any formal ties to the CI profession, while others employ CI professionals or outside CI firms and practitioners. Many large corporations have established entire CI departments. Competitive intelligence is a recognized,
accepted, and legal way for businesses to gain a competitive advantage in the marketplace. This in turn accelerates the benefits to society of competition in the marketplace.

SCIP encourages its members to abide by its code of ethics; one clause in the code instructs its members to "accurately disclose all relevant information, including one's identity and organization, prior to all interviews."

The Economic Espionage Act of October 1996 (EEA) was enacted by the U.S. Congress in response to attempts by foreign entities to steal American trade secrets. It was not enacted in order to regulate the CI industry nor was it enacted in response to any problems arising out of the activities of CI professionals. Its passage however has led to various and sometimes conflicting opinions regarding the EEA and has created confusion regarding its implications for the practice of CI.

The EEA is a federal criminal law and was passed in order to enable federal authorities to investigate and prosecute acts of economic espionage.

Federal authorities charged with the responsibility of protecting national security and the national economy were confronted with the reality that laws dealing with the theft of trade secrets were state law, and needed a federal law to give them the authority to investigate and prosecute the increasing number of cases of economic espionage conducted by foreign entities. The EEA was passed to do just that.

Congress decided however that the scope of the EEA would include the theft of a trade secret by anyone, for anyone. In other words, the EEA is not limited to theft of a trade secret for a foreign entity, but encompasses theft of a trade secret by and for a domestic competitor.

Herein lies the confusion. While the EEA makes trade secret law a federal criminal matter — this for the first time in U.S. history — the activities it criminalizes had always been prohibited under state law and/or inconsistent with SCIP's code of ethics. In other words, the rules are fundamentally the same but the consequences of violating them are different. An activity that had always been a violation of state trade secret law can now result in not only state civil liability but federal criminal liability as well.

Implications

There are several reasons why the EEA should not have any impact on the practice of competitive intelligence.

First, the act of seeking and collecting information on a competitor is itself legal. Note the following from the Restatement of Torts (1939):

The privilege to compete with others includes a privilege to adopt their business methods, ideas, or processes of manufacture. Were it otherwise, the first person in the field with a new process or idea would have a monopoly which would tend to prevent competition (Section 757, Comment a).

One limitation on this rule cited by the Restatement is: "It is the employment of improper means to procure the trade secret, rather than the mere copying or use, which is the basis of liability in this section."

Information collection performed by CI professionals centers around the sophisticated use of published material, databases, and on-the-record interviews, techniques which themselves are legal and proper means of acquiring information.

Second, properly trained CI professionals who have conducted themselves in an ethical manner were not engaged in legally risky business prior to the EEA. The appropriate legal principles have been instilled into the CI profession over the years of its existence and subsequently adopted as practice by properly trained industry members. The increased penalties for trade secret theft under the EEA will not be applicable to those whose practice has been consistent with the already existing legal standards.

Third, most situations commonly referred to as "gray zone" areas are not trade secret violations at all. Though they raise ethical questions, "gray zone" situations such as finding a lost document in the street, overhearing competitors talk on a plane, having a drink with a competitor knowing you are better at holding your liquor, removing your name tag at a trade show, or even falsely identifying yourself as a student, are situations which alone will not trigger trade secret liability. Properly trained CI professionals should be able to identify and avoid the predicaments that would place them in actual legal risk.

Fourth, the EEA will not be applied to general commercial disputes, but to clear criminal acts of theft. The reason for the EEA's passage was to thwart attempts at stealing American trade secrets which would have an impact on the competitiveness and health of the American economy. That the U.S. Attorney General promised Congress that no charges will be filed under the EEA for the first five years after the law's enactment without the approval of the Attorney General or two of her top deputies indicates that federal authorities have no intention of becoming entangled in the numerous trade secret disputes that do take place in the routine course of business (see Congressional Record, October 2, 1994, S12214).

To summarize, the EEA incorporates into the federal criminal code activities that were already illegal under state law. It does not add new burdens or restrictions to the American workforce.
A Note on Extraterritoriality

About twenty percent of SCIP's membership is outside the USA, making the question of how the EEA affects overseas activity pertinent.

The EEA does have an extraterritoriality clause. In principle, a statute must state that it applies overseas for it to so apply. The extraterritoriality provisions of the EEA apply the statute to a U.S. citizen even abroad, and to a non-U.S. citizen (1) while on U.S. soil or (2) abroad, if the act committed abroad violates the EEA and "an act in furtherance of the offense was committed in the United States."

What this means in practice is that whatever types of activities the EEA prohibits overseas are the same as what is prohibited on U.S. soil, which, as explained, had always been prohibited by state law and/or inconsistent with SCIP's code of ethics.

EEA Compliance Plans

An additional reason for concern regarding the implications of the EEA on competitive intelligence has been the many calls for "EEA compliance plans" based on the Federal Sentencing Guidelines. The Sentencing Guidelines do not instruct, dictate, require, prescribe, or obligate a company to have a compliance plan. The Sentencing Guidelines, the manual by which federal judges must sentence a defendant, allows the judge to deduct "points" from the sentence, i.e., lessen the sentence, if a corporate defendant, not an individual defendant, took measures to "detect and prevent" the criminal activity from occurring. A proper compliance plan can lower the sentence of a corporation convicted of a crime; it has no relevance to the sentencing of an individual convicted of a crime.

The list of seven "must haves" from the Sentencing Guidelines, referred to in EEA compliance plan articles and presentations are not obligatory (i.e., "The organization must have established compliance standards and procedures ... the organization must have taken steps to communicate effectively its standards and procedures to all employees and other agents... "). The document is talking to the judge, not the corporate defendant. The corporate defendant "must have" taken these steps in order for the judge to find that a reasonable plan to "detect and prevent" crime was in place, not that the company "must have" done these things as an independent legal obligation.

The Sentencing Guidelines do not actually use the phrase "compliance plan." This is the term which has developed to refer to the measures to "detect and prevent" violations of law. A company that does not have a compliance plan is not "in violation" of the Federal Sentencing Guidelines, and if not convicted of a particular crime, the lack of a compliance plan for that aspect of law will be of no consequence. Conversely, a company convicted of a federal crime will not be penalized for not having a compliance plan but will lose its chance of receiving a lowered sentence. Though not a legal requirement under the Guidelines, in practice having a compliance plan is the responsible and indeed the expected way for a company to conduct its affairs.

There are no "EEA regulations" to comply with. One is to learn what not to do and not do it. Generally speaking, compliance plans are geared to aspects of law that are industry specific and encompass regulations. Banks will have a compliance plan for Treasury Department regulations, pharmaceutical companies for FDA regulations, securities dealers for SEC regulations, and telecommunications companies for FCC regulations. As the activities the EEA criminalizes are substantially the same activities in which CI professionals should never have been engaged, an EEA "compliance plan" should not be substantially different from the existing professional guidelines a CI firm or professional would be expected to have or abide by.

Answers to Frequently Asked Questions

1. Even if the EEA was not intended to deal with competitive intelligence or general commercial disputes, hasn't it had an impact nonetheless?

Answer: The impact the EEA has had on the CI community has been based on anxiety and confusion. Some companies have mistakenly taken the position that the EEA has placed them in legal jeopardy because of the activities of their CI professionals.

Ironically, companies who curtail the legal and ethical activities of their CI professionals have placed themselves at a competitive disadvantage to companies whose CI activities continue unimpeded.

2. Don't we have to wait to see how the EEA is applied in the courts before determining what it prohibits?

Answer: How courts ultimately interpret statutes is a fundamental part of legal analysis. This does not mean however that one cannot understand the basic prohibitions of a statute. Indeed, a statute can be declared unconstitutional by the courts if it does not provide adequate notice as to what it prohibits.

The intention and purpose behind the EEA was clearly explained by Congress prior to its enactment. This did not include an intention to alter the fundamentals of corporate conduct, but to deter and punish the criminal act of trade secret theft.

3. Can't the EEA be applied to situations it was not intended to cover?
Answer: It is not unusual for some laws to ultimately be applied to unforeseen situations. A law once passed may take on a life of its own. The concern that the EEA will be applied to routine commercial disputes was discussed and dismissed by Congress prior to the EEA's passage, with the Attorney General's letter giving further assurances to this effect (see page 4). Companies who remain concerned are well-advised to study the background of the law.

4. The definition of a trade secret under the EEA is broader than existing trade secret law. What implications does this have on competitive intelligence?

Answer: The wording of the EEA's definition enumerates more types of information considered a trade secret than previous legal definitions. This is because a criminal statute should be written in explicit language so as to give notice as to what it criminalizes, otherwise it risks being declared unconstitutional. This does not mean that prior legal definitions excluded types of information enumerated in the EEA's definition.

In practice, existing legal definitions and case law interpretations cover all sorts of financial, business, and scientific information.

Whether the information stolen is included in the EEA's definition of a trade secret is moot with respect to professionals whose conduct precludes them from engaging in theft.

5. What effect if any does the EEA have on the legal risks one may decide to take in seeking information on a competitor?

Answer: The EEA compounds the legal consequences for one engaged in theft of a trade secret by adding federal criminal penalties to an act which already triggers state civil penalties. This added risk however is of no consequence to one who seeks information on a competitor in a legal manner.

6. What implication does the EEA have on a company's efforts to protect information?

Answer: The EEA focuses primarily on the activities it prohibits. The EEA's definition of a trade secret however, like state trade secret law preceding it, requires the trade secret holder to take reasonable measures to keep that information secret. In practice, the holder of a trade secret must have taken those reasonable measures in order for one who misappropriates that information to be held liable under the EEA or state trade secret law.
January 21, 1999

VIA OVERNIGHT COURIER

SCIP Board of Directors
Society of Competitive Intelligence Professionals
1700 Diagonal Road
Suite 520
Alexandria, Virginia 22314

Re: Competitive Intelligence and the Economic Espionage Act

Dear Board Members:

As you know, I teach trade secrets law at John Marshall Law School and I am an active practitioner and retained expert in trade secret cases around the country. See http://www.execpc.com/~mhallign/resume1.html.

At Richard Horowitz’s request, I have reviewed his (8/17/98) draft entitled "Proposed Policy Analysis: Competitive Intelligence and the Economic Espionage Act."

This is a well written draft and I endorse it. I strongly agree with the basic underlying premise -- The EEA does not materially affect competitive intelligence activities and companies should not curtail competitive intelligence activities based on a "misplaced fear" of the EEA. In fact, just the opposite is true. Companies should increase competitive intelligence activities to meet the challenge of an increasingly global competitive environment.

My summary of "Reported Criminal Arrests Under the Economic Espionage Act of 1996" is the most up-to-date information available on EEA prosecutions and convictions. It is available on the Internet at http://www.execpc.com/~mhallign/indict.html. As you can see, these EEA prosecutions involve trade secret theft and bear no reasonable relationship whatsoever
to legitimate competitive intelligence activities.

If I can be of further assistance to the SCIP Board of Directors, please contact me at 1-312-526-1559.

Very truly yours,

R. Mark Halligan

cc: Richard Horowitz, Esq.
Re:  Economic Espionage Act of 1996

Dear Board Members:

I was formerly a trial attorney with the Computer Crime and Intellectual Property Section of the United States Department of Justice where I was involved in drafting the Economic Espionage Act of 1996 ("EEA"), and was the lead prosecutor on one of the first cases brought under the EEA. In addition, I am a co-author of an article entitled "Understanding the Economic Espionage Act of 1996," 5 Tex. Int. Prop. L.J. 177 (Winter 1997). Currently, I am a Special Counsel in the San Francisco and Palo Alto offices of Heller Ehrman White and McAuliffe.

At Richard Horowitz’s request, I have reviewed SCIP’s “Proposed Policy Analysis: Competitive Intelligence and the Economic Espionage Act” and offer the following comments.

The EEA was intended to address both the general need for a federal criminal deterrent against trade secret theft and the apparent threat of industrial espionage sponsored by foreign countries. The EEA was not intended to impose new restrictions on American businesses. I agree with the Policy Analysis that the EEA was not developed in order to regulate the competitive intelligence community, nor was it developed in response to any problems that might have existed in the competitive intelligence community. Competitive intelligence practitioners who abide by SCIP’s Code of Ethics should not be in violation of the EEA. If I can be of further assistance to the SCIP Board of Directors, please call me at (650) 324-7156 or e-mail me at bmtsdad@AOL.com.

Very truly yours,

Peter J. Toren

Peter J. Toren
March 2, 1999

Re: Economic Espionage Act of 1996

Dear Board Members:


At Richard Horowitz's request, I have reviewed his (1/27/99) draft entitled "Proposed Policy Analysis: Competitive Intelligence and The Economic Espionage Act," particularly the section dealing with the sentencing guidelines and compliance plans.

Mr. Horowitz has written an interesting and informative submission, pointing out the relationship between compliance plans and the Federal Sentencing Guidelines as they relate to corporations. His analysis is incisive and important.
I agree with his analysis that the Federal Sentencing Guidelines do not create a legal obligation for a corporation to create a compliance plan.

If I can be of further assistance to the SCIP Board of Directors, please feel free to contact me at the above number.

Very truly yours,

Elkan Abramowitz

cc: Richard Horowitz, Esq.
Appendix F:

Online Resources:
A list of informational internet resources for competitive intelligence, intellectual property, and general economic and national security
American Society for Industrial Security (ASIS) – www.asisonline.org

Competitive Intelligence Guide by Fuld & Company, Inc. – www.fuld.com


Defense Security Service (DSS) counterintelligence information –
www.dss.mil/cithreats/index.htm

Economic and competitive intelligence links – www.loyola.edu/dept/politics/ecintel.html

FBI’s National Security Awareness Program (ANSIR) –
www.fbi.gov/programs/ansir/ansir.htm

Information Security magazine online – www.infosecuritymag.com


Marketing and competitive intelligence resource focused on the United Kingdom –
www.marketing-intelligence.co.uk/aware/sitemap.htm

National Infrastructure Protection Center (NIPC) – www.nipc.gov


Security Management magazine online – www.securitymanagement.com

Society for Competitive Intelligence Professionals (SCIP) – www.scip.org

U.S. Department of Justice computer crime and intellectual property crime section –
www.cybercrime.gov
