THE DOCUMENT COMPANY
XEROX | GLOBAL SERVICES
CONSULTING • IMAGING • CONTENT MANAGEMENT • OUTSOURCING

**White Paper**

# Economic Espionage and Trade Secret Theft:

## Defending against the pickpockets of the new millennium

"Economic espionage is the unlawful or clandestine targeting or acquisition of sensitive financial, trade, or economic policy information; proprietary economic information; or critical technologies."

U.S. Attorney General's Office
The 2002 Annual Report to Congress on Foreign Economic Espionage and Industrial Espionage

Dave Drab,
Director, Information Content Security Services
August 2003

# Table of Contents



**Pickpockets are opportunists who work the streets with a keen eye for a good mark. They are masters of the art of diversion and often work in teams, executing a series of precision tactics to make the score. They are long gone before their victims know what happened.**

# Introduction

Any organization competing today is in the business of using its knowledge and expertise to drive new revenue and gain advantage in the marketplace. Maintaining the secrecy of a unique business method, strategy, or process—a trade secret—may be the difference between success and failure. How well a company protects its competitive advantage is largely dependent on its ability to identify, manage, and protect its intellectual capital. Herein lies the problem.

Many companies define information security requirements on a traditional "perimeter" approach. Companies make huge investments to secure their physical properties and information infrastructure. And while this approach may be effective in preventing unauthorized persons from gaining access from the outside, it does little to prevent the theft or loss of critical information by those on the inside. Viable security architectures must therefore be implemented that account for this deficiency and offer holistic solutions that reduce the risk of theft or loss of trade secrets during the course of routine business activities.

The value of trade secret information is ever increasing as the result of globalization, the rapid advancement in technology and telecommunications, and employee mobility in the workplace. At the same time, however, these factors combine to create an unprecedented opportunity for the commission of economic espionage and trade secret theft. Companies victimized by economic espionage experience the loss of competitive advantage, erosion of market share, reduction in revenue streams, and the loss of shareholder confidence. A strategic plan to manage and protect intellectual assets and property is essential to building and maintaining competitive advantage in the new global economy.

**The definition of a trade secret, according to the Economic Espionage Act of 1996, 18 U.S.C. § 1839 (3)**

"All forms and types of financial, business, scientific, technical, economic, or engineering information, including patterns, plans, compilations, programmed devices, formulas, designs, prototypes, methods, techniques, processes, procedures, programs, or codes, whether tangible or intangible, and whether or how stored, compiled, or memorialized physically, electronically, graphically, photographically, or in writing."

There is a broad spectrum of espionage activity that impacts corporations. At one end of the spectrum is the opportunity seized by a trusted employee or person with access and consummated through a simple act or series of acts over a short period of time. At the opposite end of the spectrum is the sophisticated collection operation of a foreign government or corporation initiated through a targeting strategy and executed through a complex sequence of acts over a protracted period of time.

Whichever the case, Congress recognized the importance of securing intellectual assets and enacted the Economic Espionage Act of 1996 (EEA).This law makes it illegal to steal trade secret information, provided the information has actual or potential economic value and the owner has taken reasonable measures to protect it. Through mid-2003, there have been approximately 40 prosecutions levied by the Department of Justice under the EEA with hundreds more under investigation by the FBI.

## Is economic espionage on the rise?

The past decade has seen a significant increase in the number of businesses immersed in economic espionage—either as a victim or as the target of a federal investigation. The motives for stealing critical business information are the same as they ever were and can be traced back thousands of years. From the secret processes of China's silk industry, to the Cartwright loom of Britain's textile industry of the 1800s, and now to the chips of Silicon Valley in the new millennium—nothing has changed. It's just that now, the opportunity to act is much easier. The payoff is high, and the risk of getting caught is low.

Advances in technology, the advent of the Internet, and political changes have transformed the ways in which information is captured and presented for use in the global economy. The document—the means bu which information is most often transferred—has evolved considerably, and today U.S. courts generally hold that documents include not only the 8.5" x 11" paper version, but also e-mail, files on computer disk, voice mail, handwritten notes, audio recordings, video, and draft versions of paper and electronic communications. These "documents" are created, stored, shared, and distributed differently than traditional paper documents, meaning new workflows have been established to keep the information moving reliably. The new technology and new workflows certainly make employees more productive, but they also leave business information more vulnerable to theft and loss than they have been in the past.

Another factor contributing to the rise of economic espionage involves employee mobility and shifting allegiance. The hallmarks of virtue in the workplace—trust, loyalty, and dedication—are not what they once were. Today, employees give little more than a passing thought to walking out with innovation and ingenuity—bought and paid for by a company—and using it as a bargaining chip to climb the job ladder, possibly with a competitor.

## What is the cost of economic espionage?

Fortune 1000 companies reported losing proprietary information and intellectual property valued at between $53 and $59 billion dollars during the period beginning July 1, 2000 and ending June 30, 2001. This finding was based on a survey entitled *Trends in Proprietary Information Loss*, sponsored by the American Society of Industrial Security Foundation (ASIS), PricewaterhouseCoopers and the U.S. Chamber of Commerce.[1]

*FBI Director Robert S. Mueller III claims an even higher number—as much as $200 billion—is lost annually to economic espionage.*[2]

[1] Based on 138 companies that responded to the survey
[2] William Mcquillen, *Bloomberg News*, June 21, 2003; quote from a speech at the National Press Club, Washington, D.C., Friday, June 20, 2003.

Despite these findings, it is still unclear as to exactly how much is truly lost to economic espionage. We know that it is a serious problem, and we know it's on the rise, but it is difficult to accurately assess the impact and long-term consequences of this activity. This may be attributed to several factors:

### Failure to detect sophisticated espionage activity

Sophisticated espionage attacks on commercial enterprises may go undetected. The highly technical covert operations of intelligence services can accomplish their collection objectives and leave little or no evidence of the intrusion. Loss of market share may be the only indicator—and it may not be discovered for years. However, as companies educate employees as to the motivation, tactics, and techniques of economic espionage, such activities will be more easily detected and prevented.

### Failure to report espionage activity

Victims often face the choice of reporting violations, risking broader disclosure of their trade secrets, or not reporting their loss, thereby minimizing public exposure of their trade secrets, but allowing the wrongdoers to go unpunished. Companies may also allow espionage to go unreported because of the fear of public embarrassment and eventual loss of shareholder confidence. A company victimized by economic espionage is obligated under the law to report such offenses, but because of the risk of losing more trade secret information in civil or criminal proceedings, no one can accurately determine how much corporate theft is actually occurring.

### Failure to accurately assess the long-term impact of espionage activity

A single, accurate calculation of monetary losses directly and indirectly linked to economic espionage on an annual basis cannot be made and is not readily available. Speculations have been made, however, and range from $53 billion to $1 trillion. Losses may only reflect inventory "snapshots" on the day the audit was performed. Such reporting does not account for lost sales activity and jobs that may extend over a period of years.

### What types of information are targeted?

Sensitive business information is divided into five primary categories, including financial, organizational, marketing, technical, and scientific. The following list identifies some of the types of information protected as trade secrets in cases thus far prosecuted under the Economic Espionage Act of 1996.

- Access card control information
- Project information
- Pricing information/sales forecasts
- Financial information
- Computer source code
- Test material/prototypes/design specifications
- Customer business info
- Engineering plans and drawings
- Formulas
- Research
- Blueprints/diagrams
- Confidential documents
- Software
- Implementation methodology
- Technical records
- Biomedical research
- Sales forecasts

## Who is involved?

Any company is susceptible to trade secret theft and loss. Of course, mid- to large-size organizations are especially vulnerable because their boundaries are wider, they have more employees to manage, and many operate internationally. These large organizations can potentially be targeted by competitive commercial enterprises and foreign governments.

### Commercial enterprises

Competitive organizations are the most obvious source of economic espionage. In fact, of the approximately 40 cases that were prosecuted under the Economic Espionage Act of 1996 thus far, nearly all were corporate-on-corporate, where one company targeted another. Only two cases involved foreign government sponsorship. Lacking required funds to launch a new product R&D program, many corporations elect to level the playing field by stealing time-intensive and costly research results from competitors. In some cases, they actually use

the information to incorporate the same or similar processes or products into their own organizations. In other cases, they simply review the trade secret information to see how their competitors operate. In either case, the victims of economic espionage have lost their competitive advantage and experience a weakened position in the marketplace.

### Foreign governments

Companies tend to underestimate the risk factor of foreign intelligence operations because the activity is difficult to detect and its impact may not be known for years—if ever. But Supervisory Special Agent Donald Przybyla, of the FBI's Palo Alto, California, Office in Silicon Valley stated,

*"In Silicon Valley, at least 20 foreign nations have tried repeatedly to steal U.S. trade secrets over the past five years."*[3]

Many "cold warriors" of the former KGB pose a serious threat to commercial enterprises worldwide because of their high level of technical skills training and expertise in information gathering, human asset development, use of advanced technologies, and global networks. Furthermore, many of them are now seated in the boardrooms of international corporations as decision makers.

The collection tactics of allied nations tend to be more discreet and subtle out of fear of public embarrassment and injuring diplomatic relations. Hostile nations, on the other hand, can be highly aggressive and indiscreet in their collection tactics and operations.

## How are trade secrets accessed?

A company's trade secrets are maintained in computer files, formal or draft documents, working papers (including notes and actions lists), scrap papers, appointment calendars, internal correspondence, newsletters, policy documents, meeting minutes, legal and regulatory filings including annual reports and patent applications, travel documents, and other official records. All too often, collectors are successful in recovering clues to trade secret information from trash receptacles and Dumpsters in and around the building. Trade secrets are also located in the memory banks of employees and are often the topics of discussion at a local pub.

Commercial enterprises and foreign governments have a number of methods and techniques to access trade secrets—both legally and illegally. Economic espionage, like traditional espionage, is rarely committed through the use of a single collection technique. Experienced collectors and their enterprises are often affiliated with global networks and are masterful in combining legal and illegal means. They will seek a balanced collection approach—human versus technical and direct contact versus indirect contact.

### Legal means

*Review of publicly available records*

Nearly all espionage attacks will rely upon publicly available information or open-source information in some manner to design a collection strategy. Public libraries have always been a reliable source, but the World Wide Web and Internet have expanded the accessibility of even more information to the entire world.

*Internet*

Between 1990 and 1995 alone, acts of economic espionage increased 300% as the result of the ease with which trade secret information can be misappropriated and disseminated over the Internet.[4] The use of e-mail is clearly the method of choice to solicit information, though the use of postcards and letters continues. Requests are usually in response to information posted on Internet Web sites, trade journals, advertisements, and in marketing materials at trade shows and conferences. Non-threatening requests for price lists, product lists, published papers, assistance in research, and employment inquires are most common.

The Internet may be used by collectors and spies to gather valuable information and at the same time hide their true identity, affiliation, and location. Public-access Internet locations at libraries, colleges, and universities, for example, offer excellent cover and a degree of legitimacy to such requests.

[3] Edward Iwata, *USA Today*, "More U.S. trade secrets walk out door with foreign spies."

[4] *Protecting Your Company's Intellectual Property, A Practical Guide to Trademarks, Copyrights, Patents & Trade Secrets*, Deborah E. Bouchoux, AMACOM (American Management Association), 2001.

*Employment solicitation*
A common information gathering technique is the "phantom interview." A third-party recruiter is hired by Company A to elicit information from employees of Company B during the course of bogus job interviews. Because there is no hiring intent, this tactic is clearly unethical and, combined with other circumstances, could also constitute espionage activity.

*Joint ventures and acquisitions*
Trade secret information and protected technologies are subjected to security risk in joint venture scenarios. Employees from Company A working in close proximity to employees and technology from Company B for extended periods of time may be accepted as partners and security becomes lax. A simpler, legal, but more expensive means for Company A to obtain information from Company B is to actually acquire the company or business unit.

*Conferences and visitors*
The audiences of conferences, seminars, exhibits, and trade fairs include scientists and engineers. Because of their knowledge and expertise, corporate entities and foreign governments may task them with identifying and exploiting information.

Similarly, facility visitation has long been a valuable information gathering technique of commercial enterprises. Delegates have received specialized training to aggressively gather information, including breaking away from their escort to access restricted areas, taking unauthorized photographs, and asking questions beyond the scope of the tour.

*Dumpster diving*
Generally, office documents and property discarded in trash receptacles are considered abandoned property because the owner has relinquished ownership rights. "Waste archeology" may yield rewarding information, including memos, notes, letters, projects, departments, titles, phone numbers, organization charts, financial information, corporate travel, etc. Dumpster diving becomes illegal if the waste container is in a secure, restricted area.

**Criminal means**

Naturally, executives at commercial enterprises and officials of foreign governments will not directly participate in any criminal activity. To maintain plausible deniability, they may only tell a subordinate (with a wink and a nod) that they need the information "no matter what." The subordinate then does the dirty work by recruiting individuals and groups who perform illegal services for hire, such as independent entrepreneurs or members of organized crime.

*Organized crime* evolves and takes on new, non-traditional forms in response to its environment. Globalization has enabled the emergence of a new type of transnational crime. Mega-global criminals, particularly in the territories of the former Soviet Union, line the pockets of corrupt public officials and muscle their way into commercial enterprises. They often possess more power and wealth than the local or national government of the territory and pose a real threat to business and industry.

*Independent entrepreneurs* include independent or loosely affiliated persons involved in competitive intelligence. In essence, they are private investigators hired by companies to acquire specific business information deemed useful to the corporate decision-making process. Depending on their ethics or penchant for money, they are inclined to bend or break the law to accomplish their mission. People in this category are not to be confused with law-abiding competitive intelligence professionals affiliated with the Society of Competitive Intelligence Professionals (SCIP).

But no matter who actually performs the act, there are several illegal ways corporate enterprises and foreign governments obtain trade secrets:

*Insiders with access*
The number one threat of economic espionage comes from within organizations. Whether willingly or unknowingly, employees, partners, vendors, subcontractors, venture capitalists, and temporary employees with access are the most difficult challenge for companies trying to initiate a secure environment. Temporary employees alone—with no permanent stake in the success of their organizations—are said to comprise an unprecedented 20% of today's workforce.

In some cases, insiders who do not wish to harm their organizations give away trade secrets inadvertently. Competitive commercial enterprises and/or foreign governments will try to gain access to trade secrets using elicitation techniques. Elicitation, commonly referred to as "social engineering," is a learned skill to obtain information through conversation by tactics and concealed purposes not readily identifiable to a person from whom the information was elicited. Through the use of deception and manipulation, the social engineer is able to convince a person in a targeted company to lower his/her guard and divulge information that should not be released. They will study the company's vernacular and use it in a skillful and convincing manner. While not always illegal, social engineering is generally a precursor to criminal activity.

In other cases, commercial enterprises and foreign governments may try to access trade secrets through employee infiltration or employee recruitment:

*Employee infiltration*
It is a relatively simple task to obtain false identification that would enable a collector to gain employee status inside a targeted company. Once on the inside, the capability of the collector to identify and obtain sensitive information is greatly increased.

*Employee recruitment*
The recruitment of an employee of a company is one of the most effective ways to steal a company's secrets. Once an insider or "mole" has been recruited through bribery or other means, s/he can then be tasked to procure specific types of trade secret information. The collector's interest is not limited to corporate executives, business managers, and researchers, but includes secretaries, computer operators, technicians, and maintenance employees. Lower-level employees often have far more access to trade secrets and competitive business information than is necessary and appropriate, and can be invaluable to a collection operation.

Recruiting employees is not as difficult as it may seem. Some employees steal trade secrets for money. Others do it out of revenge for perceived wrongs against them. Disgruntled employees are an excellent target for recruitment and exploitation because they are often predisposed to injure the company.

*Computer intrusions*
Computer "hacking" is on the rise because of the vast software resources available via the Internet. There are hundreds of Web sites that offer downloadable, customizable hacking tools. Many hackers engage in this activity as a sport or conquest to enter a system that is supposed to be secure and impenetrable. Others, though, are often professional criminals that hack into systems with the intent to steal information for economic gain. Both business competitors and foreign intelligence services have been known to task computer "geeks" to attack enterprise systems to gain access.

According to the "Computer Crime and Security Survey"[5] from 2002:

- Ninety percent of respondents (primarily large corporations and government agencies) detected computer security breaches within the last 12 months.
- Seventy-four percent cited the Internet as a frequent point of attack.
- Eighty percent acknowledged financial losses due to computer breaches.
- The most serious financial losses occurred through the theft of proprietary information (26 respondents/$170,827,000) followed by financial fraud (25 respondents/$115,753,000).

*Burglary and theft*
Surreptitious entry and break-ins to steal trade secret information may involve the actual removal of documents, computer data storage media, and/or other tangible properties and facilities containing the information. Perpetrators may elect, however, to steal trade secrets without physically removing them from the premises. Sensitive files and documents may be photographed, scanned, or duplicated in a manner that conceals the fact that a theft has

[5] *Computer Security Issues & Trends*, Spring 2002, Vol. VIII, No.1, 2002; Computer Security Institute/FBI Computer Crime and Security Survey. Computer Security Institute (CSI) is an international membership organization serving the information security professional. CSI was established in 1974 and has thousands of members worldwide.

occurred. This affords the collection enterprise the opportunity to continue and even expand the scope of criminal activities based upon the analysis of information acquired in the entry. Such operations are used in consonance with other legal and illegal collection tactics.

*Electronic surveillance*

The potential of electronic surveillance as a means of collecting trade secret information cannot be overstated. Especially now, as technology continues to move toward the wireless market, the threat of intercepting vital information is greater than ever before. Yet until recently, technical "spy" equipment was designed, manufactured, and controlled exclusively by government intelligence services and the military. Today, though, the technology has been successfully commercialized and is sold affordably. For example, micro video and audio recorders designed for concealment may be purchased at an average cost of approximately $175. Even baby monitors can be hidden in boardrooms and meeting areas to capture trade secret information. It has never been easier.

## What can be done to protect trade secrets?

Protecting trade secrets from theft and loss is critical for organizations that want to maintain their competitive advantage in the marketplace. The first active step forward-thinking organizations take is to appoint an information executive and a team who are accountable for capturing and protecting the competitive advantage of the company. This "security team" is responsible for integrating and managing the three traditional silos of security—physical security, IT security, and risk management. Working with the different departments across the entire enterprise, including legal, HR, R&D, finance, engineering, marketing, etc., the team establishes formalized processes to identify, manage, and protect trade secrets.

### Identify

Before trade secrets can be protected, they must first be identified and documented. Once the monetary value of the trade secret is identified, the organization will see the urgency in developing a comprehensive management program to safeguard it. But it is not easy.

A large part of the problem is that many people within organizations are unable to define the intellectual assets that become trade secrets. Patrick H. Sullivan, founding partner of The ICM Group, LLC, stated that

*"Few managers in knowledge firms can define intellectual capital—what it is, where it resides in their firms, and how they manage it to produce the profits for their shareholders."*[6]

Trade secrets that have not been identified still exist within the company, but they are undocumented, unleveraged, and unprotected under the law. Consequently, company know-how and innovative methodologies are highly vulnerable and more easily lost or stolen. It is the responsibility of the security team, therefore, to define and implement formal policies and procedures and, at the same time, develop educational tools to help information workers identify trade secrets and play a more active role in their management and protection.

### Manage

Much of a company's useful knowledge is unstructured and may be found on desktops, filing cabinets, personal e-mails, and internal documents. This makes it difficult to capture, manage, and protect. To effectively protect both structured and unstructured information, the security team must first have a thorough understanding of how trade secrets are used, accessed, and distributed inside and outside the organization. Once they comprehend the trade secret workflow, they may establish a system to classify, declassify, archive, and destroy trade secrets. Once implemented, the team must be given the authority to enforce compliance with the system.

[6] Profiting from Intellectual Capital, Extracting Value from Innovation, Patrick H. Sullivan, John Wiley & Sons, Inc., 1998.

### Protect

Protecting trade secrets is vital to the financial health of an organization. Without a defined, cohesive protection program, employees who leave their companies may take trade secrets with them. Even if the organizations file a civil action to stake their claim of ownership and protect their interests, it becomes a "he-said, she-said" matter in the courts. The results are potentially catastrophic but almost certainly expensive—and these types of disputes can be averted if the companies identify their trade secrets early and notify employees of the value of the information to the company. That is why it is so important the security team establish a trade secret compliance program that outlines company-wide policies and procedures that best serve the objectives of intellectual capital management. Anything short of a documented compliance plan does not exceed good intentions.

But while the security team is accountable for developing the processes and implementing the technological tools that protect trade secrets, everyone in an organization is ultimately responsible for making sure those processes and tools are successful.

Global change requires the integration of security concepts and practices to close the gap on real and potential vulnerabilities, offering a more seamless approach to information management and workflow. This includes protection for key corporate processes such as product development, sales, marketing, and business operations. Reasonable security measures must reflect a balance of solutions involving people, process, and technology. Fostering a sense of trust and loyalty in the workplace helps to galvanize a security culture and establish enterprise-wide best practices.

The security team is tasked with initiating a new security culture and mentality, which requires employees buy in at all levels of the company and empowers them to play a part in the trade secret management process. They must receive awareness training to inform them as to the nature and threat of economic espionage. Understanding its motivation, tactics, effects, and cost helps employees accept policies that govern what can and cannot be done in interacting with non-employees such as contractors, vendors, consultants, contractors, and temporary employees in order to protect trade secrets and confidential information. Once they recognize the threat, employees are much better equipped (and willing) to maintain a secure environment by adhering to protection programs established by the security team.

## Conclusion

The ultimate goal of an organization is to be able to leverage intellectual capital to gain a competitive advantage in the marketplace. For this to be possible, the most critical information—trade secrets—must be known solely by that one single organization. As soon as others are able to access the information, the competitive advantage is compromised or lost.

An enormous amount of money is spent annually on IT solutions to combat the theft or loss of information. Yet companies remain highly vulnerable. Each company possesses different characteristics in systems design and architecture, corporate culture, methodologies, and vision. This gives each company a unique blueprint and identity. Bulletproof IT security systems that claim to protect all are merely an illusion because they only address a part of the risk problem.

Too often the weak link in security—the human factor—is overlooked, misunderstood, or ignored. Insiders with access can attack more easily—and with greater success—than outsiders. Corporations must therefore dispense with the "perimeter-only" approach and start focusing within their own organizations. They also need to consider the functionality of Digital Rights Management and XML-solutions that give authors control over who accesses their documents. In so doing, they have a means to manage documents whether they are inside or outside the company.

But perhaps the greatest danger a company faces today in the information age is the erroneous belief that economic espionage only happens to other companies. Organizations can only implement an appropriate trade secret protection program when they recognize that a real threat exists. This is extremely difficult because, like the pickpockets of the last millennium, today's new breed has mastered the art of opportunity and diversion, which leaves their victims unwitting, unsuspecting, and unthreatened.

## Glossary of terms

**Intellectual capital—**Company knowledge that can be leveraged for advantage and profitability.

**Human capital—**The individual employees of a company that possess knowledge, skills, and expertise that the company intends to use in the pursuit of business.

**Intellectual asset—**Company knowledge that can be leveraged for advantage and profitability.

**Intellectual property—**Created when an employee's idea or know-how is written or otherwise committed to any media or documented, thus defining or codifying its existence.

**Economic espionage—**Refers specifically to theft of legally protected trade secrets. Commonly referred to as *Corporate Espionage* or *Industrial Espionage.*

**Trade Secret—**Any knowledge, protected by law, that is determined to have economic value and provides an advantage over competitors who do not have it. Commonly referred to as *proprietary information.*

**Author: Dave Drab**

The Federal Bureau of Investigation has exclusive jurisdiction in investigating crimes of economic espionage. Dave Drab is a 32-year law enforcement veteran. During his 27 years at the FBI, he specialized in the investigation of organized crime and economic espionage.

Xerox Global Services helps companies streamline and digitize their document-intensive business processes—everyday processes like customer communications, billing, training, or record management. Our people work closely with clients to identify, quantify, and realize hidden opportunities to save money, find new sources of value, and simplify how work gets done.

For more information on how Xerox Global Services can apply Six Sigma methodologies in your organization, call 1-800-ASK-XEROX ext. XGS or visit www.xerox.com/contactglobalservices.