International Council of Industrial Security & Safety Management

http://onlineicissm.wixsite.com/ Newsletter: July 2017

Industrial espionage or corporate spying ....

Inside this issue:

For as long as there has been commerce, there has been espionage. The methods for spying on competitors have changed over time, but the desire to uncover a rival's secrets has not.

In this Information Age, protecting trade secrets and critical and sensitive information from loss through business espionage is an increasingly important management function.

Industrial espionage, economic espionage, corporate spying or corporate espionage is a form of espionage conducted for commercial purposes instead of purely national security. Economic espionage is conducted or orchestrated by governments and is international in scope, while industrial or corporate espionage is more often national and occurs between companies or corporations.

Competitive intelligence is the legal gathering of information by examining corporate publications, websites, patent filings and the like, to determine a corporation's activities.

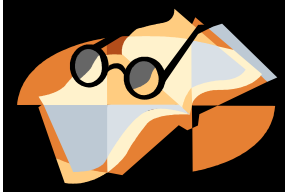
On the other hand industrial espionage is the covert and sometimes illegal practice of investigating competitors to gain a business advantage. The target of investigation might be a trade secret such as a proprietary product specification or formula, or information about business plans. In many cases, industrial spies are simply seeking any data that their organization can exploit to its advantage. There's no end to the skullduggery that businesses will get involved in with the aim of making a quick buck, or trying to keep up with their competitors.

Security professionals with sound knowledge of finance and operational knowledge of the targeted business entity must step-in so that they play the role of decision facilitators of the management. It is also imperatives on them to be ready to counter similar attempts on their own organization!

Remember – what you do unto others – others can do unto you too!

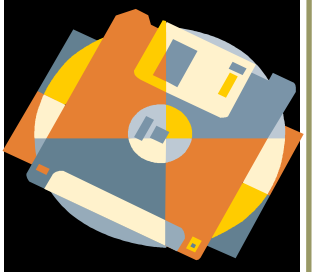
Capt. SB Tyagi

For ICISSM



Industrial or Business espionage is the covert and sometimes illegal practice of investigating competitors to gain a business advantage.

The target of investigation might be a trade secret such as a proprietary product specification or a formula, or information about business plan and strategies.



The Four Faces of Business Espionage:

1. Delphi and Other Pretext Attacks.

Sophisticated pretext interviews and/or "surveys" are often the first steps in a spy operation. Pretext interviews may take place on the phone, at seminars and trade shows, in bars, in bed, or anyplace else the target is available. The questions used are worked out in advance, often by someone other than the surveyor. The people hired to ask the questions (college students, private investigators, retirees, etc.) may or may not know the real objectives of the survey. Pretext attacks through Internet newsgroups, chat lines and direct e-mail help hide the true identity of the attacker.

2. Computer Abuse.

Computer abuse takes many forms. It may take only a few seconds for a spy to break into your computer system if your computer access codes are known around the office. Other attacks may be much more complex and take place both on and off site.

3. Technical Surveillance.

Basic electronic "bugging" is quick and easy. A spy can buy a legal wireless microphone or other listening device, and then plant it illegally by simply walking through your home or place of business and tucking it out of sight. It took less than 30 seconds to plant a bug in one of the demonstrations author witnessed.

4. Undercover Attacks

These attacks are performed by spies inside the targeted organization, including people on the target's payroll. Undercover spy operations may go on for months - or even years - depending on the spy's objectives.

What makes business intelligence or competitive intelligence different from business espionage? What are the key elements in business intelligence? What makes the business intelligence "intelligent"?

Let's look at the definitions of "intelligence" and "espionage." As defined by Merriam-Webster, intelligence is the ability to apply knowledge to change one's environment or to think abstractly as measured by objective criteria (as tests), also the act of understanding.

"Espionage" is the practice of spying or using spies to obtain information about the plans and activities especially of a foreign government or a competing company.

"From these definitions it appears as if one could infer that "business intelligence" is directed at your own organization (what is the company doing that could be changed to improve its ability to function in the environment), while espionage is directed outside the organization to those companies that are in competition with your organization.

"Espionage" also implies the act of gathering information that is not readily or openly available, whereas business intelligence focuses on making better use of the readily available data within your organization or readily available in the marketplace."
- Anne Marie Smith

Industrial Espionage and Business Intelligence

"Federal prosecutors have been investigating whether Reuters Analytics (a subsidiary of Reuters Holdings PLC) is guilty of industrial espionage activities which involve break-ins of computers at its competitor Bloomberg."

... This one could be an indicator of the crime of the new century, the electronic break in. What makes this news is that computer break-ins are involved on a corporate basis.

This kind of information

stealing and espionage has been the norm for years in highly competitive industries. So has cracking computers to get at the information inside.

Expect more industrial espionage stories in the months ahead, and more corporate cracking into other computers. Industrial espionage is one of a few buzzwords that are starting to crop up more frequently in the business press and on TV.

EMERGING BUZZWORDS: competitive intelligence, business intelligence, industrial espionage, information warfare

Competitive Intelligence is sometimes referred as "**competitor intelligence**" after the seminal book by Leonard Fuld. In 1985 he defined it as **"highly specific and timely information about a company."**

How can Industrial or Corporate Espionage be compared to Competitive Intelligence? Competitive Intelligence (CI) research can be distinguished from industrial espionage, as CI practitioners in general abide by local legal guidelines and ethical business norms.

Business intelligence" refers to the practice of collecting and analyzing competitive information in the marketplace to assist an enterprise in self-analysis and redirection of its resources to maintain and improve competitiveness. There is a severe code of ethics followed by honest competitive intelligence practitioners, laid down by the **Society of Competitive Intelligence Professionals (SCIP)**. This includes the terms that CI professionals

Must abide by all applicable laws - whether domestic or international. Thus bugging, bribery, and other such illegal practices would be a serious breach of the ethical code.

Must accurately disclose all relevant information, including one's identity and organization, prior to all interviews. This ensures that primary research is conducted ethically without twisting. As such it also limits what can be done - and attempts to gain information through lies about one's identify would be viewed as industrial espionage. At the same time, the code of ethics recognizes that it may not be in the interests of the research to declare the final purpose for which the information is being gathered - hence it is only required to reveal relevant information to sources such as one's identity, organization, etc. It is not a requirement to say who the ultimate client is, and so many organizations employ consultants who can be absolutely honest about who they are while keeping their client's name confidential. Such consultants will say that the information is being collected as part of a benchmarking or industry study, for example. What is not said is that the benchmarking study is being done only on competitors to the client!

Must provide honest and realistic recommendations and conclusions in the execution of one's duties. Competitive Intelligence can sometimes expose unpleasant truths that companies would prefer not knowing. At the same time, not knowing could lead the organization to failure. Competitive Intelligence professionals need to communicate both the good and the bad - strengths and weaknesses - even in cases when management would rather stay in lack of knowledge.

Further, the CI professional should use their understandings to provide suggestions and recommendations for action. If the intelligence gathered is not used but ignored it has no value. As a result, competitive intelligence is a key discipline in enabling company's preserves and expands competitive advantage in their business environment.

Driving Competition

In 1993, General Motors accused Volkswagen of industrial espionage.

It was after Jose Ignacio Lopez, the chief of production for GM's Opel division, left to join the rival German automaker, along with seven other executives.

GM claimed its corporate secrets were used at VW.

In the end, the companies agreed to one of the largest settlements of its kind: GM would drop its lawsuits in exchange for VW's pledge to buy $1 billion of GM parts over seven years.

In addition, VW was to pay GM $100 million.

Oracle's Trash Talk

In June 2000, Oracle Chief Executive Larry Ellison said it was doing its "civic duty" by hiring a detective agency to investigate groups that supported Microsoft.

Oracle employed Investigative Group International to look into actions by two research organizations, the Independent Institute and the National Taxpayers Union, that were releasing studies supportive of Microsoft.

Oracle said it sought evidence that the groups were receiving financial support from Microsoft during its antitrust trial.

Oracle admitted ties to Investigative Group after news reports said the detective agency had tried to buy trash from two cleaning women at the Association for Competitive Technology, a research group that Microsoft backed.

Industrial Espionage

Industrial espionage and corporate espionage are phrases used to describe espionage conducted for commercial purposes instead of national security purposes. Espionage is sometimes called the dark sister of competitive intelligence.

Espionage is more than the legal and ordinary methods of examining corporate publications, web sites, patent filings, and the like to determine the activities of a corporation. In business language the term covers more the illegal methods such as bribery, blackmail, technological surveillance and even occasional violence. In addition to spying on commercial organizations, governments can also be targets of commercial espionage – for example, to determine the terms of a tender for a government contract so that another tenderer can underbid.

"Industrial espionage" refers to the clandestine methods of obtaining competitive information that is not publicly available. As a legal matter, this distinction can have serious consequences. This case study of Boeing Company offers some suggestions for staying on the right side of the law not only in business intelligence but also for internal audit controls and business ethics.
-Bierce & Kenerson

How to Determine Competitive Intelligence Information Needs?

Effective implementation of its CIP requires not only information about the competitors, but also information on other environmental trends such as industry trends, legal and regulatory trends, international trends, technology developments, political

Counter Intelligence Program ...

developments and economic conditions. The relative strength of the competitor can be judged accurately only by assessing it with respect to the factors listed above. In the increasingly complex and uncertain business environment, the external [environmental] factors are assuming greater importance in effecting organizational change. Therefore, the determination of CI information needs is based upon the firm's relative competitive advantage over the competitor assessed within the 'network' of 'environmental' factors.

What are the General Uses of Competitive Intelligence Information?

The competitive intelligence information obtained using CIP can be used in programs that supplement planning, mergers and acquisitions, restructuring, marketing, pricing, advertising, and R&D activities.

What is the Role of the Organization's Internal Competitive Intelligence Unit?

Despite the increasing sophistication of CI tools and techniques, the most important role in a CIP remains that of the organization or its internal Competitive Intelligence Unit. Once the CI needs have been defined, the CI-unit is responsible for collection, evaluation and analysis of raw data, and preparation, presentation, and dissemination of CI. The CI -unit may handle all the activities itself, or it may assign some tasks to an outside contractor. Often, decisions have to be made on assignments of data collection, and data analysis and evaluation.

The CI-unit has to decide upon the choice of sources of raw data. Should it use government sources or online databases, interviews or surveys, drive-bys or on -site observations? It has also to decide if and when to deploy 'shadowing' and defensive-CI. Other decisions may involve choice of specialized interest groups (such as academics, trade associations, consumer groups), private sector sources (such as competitors, suppliers, distributors, customers) or media (such as journals, wire services, newspapers, financial reports) as the sources of information. Very frequently, such issues involve balancing various constraints, such as those of time, finances, staffing, etc. and therefore are based upon individual judgment.

Are there any Methods/ Methodology for a Competitive Intelligence Program?

The purpose of CIP is to gather accurate and reliable information. The groundwork for the CIP is done through an internal Competitive Intelligence Audit which is primarily a review of the organization's operations to determine what is actually known about the competitors and their operations. As a starting point for obtaining CI data, the organization generally has some knowledge of its competitors, and its own CI needs.

In absence of definition of its information needs, the organization may not be able to deploy its

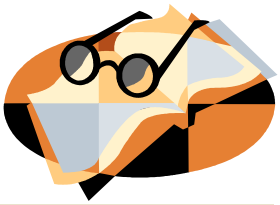
Gillette: Razor Burn

In 1997, an engineer who worked with Gillette to help develop its next generation shaver system disclosed confidential information to the company's competitors.

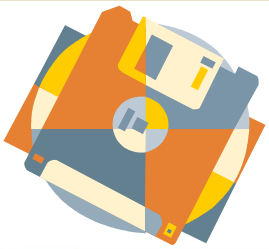
Steven Louis Davis, an employee at Wright Industries Inc., a designer of fabrication equipment that was hired by Gillette, faxed or e-mailed drawings of the new razor design to Warner-Lambert, Bic, and American Safety Razor.

Davis pled guilty to theft of trade secrets and wire fraud and was sentenced to 27 months in prison.

He told the court he stole the information out of anger at his supervisor and fear for his job. In 1998, Steven Louis Davis was sentenced to 27 months in prison and ordered to pay $1.3 million for theft of trade secrets from Gillette.



Business Espionage Controls & Countermeasures Association (BECCA) was brought together by William M. Johnson during research for his book, "Who's Stealing Your Business? - How To Identify and Prevent Business Espionage".



Methodology for a Competitive Intelligence Program?

sources effectively. To avoid such a scenario an organization may conduct a CI audit which is effectively a review of its current operations to determine what is actually known about the competitors and their operations. The CI audit helps in pinpointing the organization's CI needs.

When the organization has some knowledge about its competitors and its own CI needs, it proceeds to the stage of gathering CI data. Based upon the CI needs, relevant data can be gathered from the organization's own sales force, customers, industry periodicals, competitor's promotional materials, own marketing research staff, analysis of competitor's products, competitor's annual reports, trade shows and distributors. Specific CIP techniques include querying government resources and online databases, selective surveys of consumers and distributors about competitor's products, on-site observations of competitor's plant or headquarters, "shadowing" the markets, conducting defensive CI, competitive benchmarking, and reverse engineering of competitor's products and services.

Raw data is evaluated and analyzed for accuracy and reliability. Every attempt is made to eliminate false confirmations and disinformation, and to check for omissions and anomalies.

While the conclusions one draws from the data must be based on that data, one should never be reluctant to test, modify, and even reject one's basic working hypotheses. The failure to test and reject what others regard as an established truth can be a major source of error .

Evaluation and analysis of raw data are critical steps of the CIP. Data that lacks accuracy and reliability may be marginally correct data, concoction of very good data, bad data, or even disinformation. All data is produced or released for some certain purpose. In CIP, reliability of data implies the reliability of the ultimate source of the data, based upon its past performance. In CIP, accuracy of data implies the [relative] degree of 'correctness' of data based upon factors such as whether it is confirmed by data from a reliable source as well as the reliability of the original source of data. Evaluation of CI data is done as the facts are collected and unreliable or irrelevant data is eliminated. Analysis of remaining facts includes 'sifting' out disinformation, studying patterns of competitor's strategies, and checking for competitor's moves that mask its 'real' intentions.

The resulting CI information is integrated into the company's internal planning and operations for developing alternative competitive scenarios, structuring attack plans and evaluating potential competitive moves.

Tools and Techniques for Competitive Intelligence Activities

Different types of CI tools and techniques are available for different requirements of the Competitive Intelligence Program -

Contacting Government Agencies can yield valuable data for the CIP, but may often require excessive lead time.

Searching Online Databases is a faster method of finding competitive information. With increasing sophistication and affordability of information technology, this technique is expected to become less expensive. Database search does not provide information that has not been released to the public or that has not yet been collected.

From Companies and Investment Community Resources Some types of data that are not widely available from databases can be procured by contacting the corporation itself or from investment community sources.

Surveys and Interviews Surveys can yield plenty of data about competitors and products, while Interviews can provide more in-depth perspectives from a limited sample.

Drive-by and On-site Observations of the competitor's [full or empty] parking spaces, new construction-in-progress, customer service at retail outlets, volume and pattern of [suppliers' or customers'] trucks, etc. can yield useful CI information about the state of the competitor's business.

Competitive Benchmarking is used for comparing the organization's operations against those of the competitor's.

Defensive Competitive Intelligence involves monitoring and analyzing one's own business activities as the competitors and outsiders see them.

Reverse Engineering of competitor's products and services may yield important CI information about their quality and costs.

Tools and Techniques for all Competitive Intelligence Activities

Not all CIP tools and techniques are suitable for all CI objectives; the CI-unit has to use judgment in determining the relevant CI needs and the most appropriate tools and techniques. Specific tools and techniques are chosen depending upon various factors such as CI needs, time constraints, financial constraints, staffing limitations, likelihood of obtaining the data, relative priorities of data, sequencing of raw data, etc.

The online databases are preferable for faster turnaround time. Whereas surveys may provide enormous data about products and competitors, interviews would be preferred for getting a more in-depth perspective from a limited sample. Therefore, human judgment is an essential element of the decision regarding which CI techniques to deploy in a specific situation.

Teapot with Actresses, Vezzi porcelain factory, Venice, c. 1725.

The Vezzi brothers were involved in a series of incidents of industrial espionage.

It was these actions that led to the secret of manufacturing Meissen porcelainbecoming widely known.

How can the Competitors Foil Your Competitive Intelligence?

Very likely the target competitor would be aware of the organization's CI moves and could make all possible efforts to thwart or jeopardize the organization's CIP.

The competitor may have its own CI activities targeted at the organization. Or it might intentionally generate disinformation to mislead the organization's efforts.

The competitor could also create the problem of false confirmation by releasing similar, but misleading (or incomplete), facts to different media sources. The competitor may also use common ploys to pump information from the organization's employees. Such ploys include "the phantom interview", "the false flag job seeker", "the seduction," and "the non-sale sale."

Phantom Interview The competitor, posing as a potential employer, inquires from the organization's employees about their duties and responsibilities.

False Flag Job Seeker A competitor's trusted employee , in the guise of a potential job seeker, tries to learn about the organization in the course of the employment process.

Seduction involves organization's non-employee associates such as distributors and suppliers to elicit information about the organization's pricing structure, customer service, etc.

Remember - what you do unto others - others can do unto you too!

During testing, automakers commonly disguise their upcoming car models with camouflage pai nt patterns designed to obfuscate the vehicle's lines.

Padded covers, or deceptive decals are also often used. This is also to prevent Motoring Media-outlets from spoiling the model's big reveal.

Information theft and sabotage

Information can make the difference between success and failure; if a trade secret is stolen, the competitive playing field is leveled or even tipped in favor of a competitor.

Although a lot of information-gathering is accomplished legally through competitive intelligence, at times corporations feel the best way to get information is to take it. Economic or industrial espionage is a threat to any business whose livelihood depends on information.

In recent years, economic or industrial espionage has taken on an expanded definition.

For instance, attempts to sabotage a corporation may be considered industrial espionage; in this sense, the term takes on the wider connotations of its parent word.

That the espionage and sabotage (corporate or otherwise) have become more clearly associated with each other is also demonstrated by a number of profiling studies, some government, some corporate.

The United States government currently has a polygraph examination entitled the "Test of Espionage and Sabotage" (TES), contributing to the increasingly popular, though not consensus, notion, by those studying espionage and sabotage countermeasures, of the interrelationship between the two.

In practice, particularly by "trusted insiders," they are generally considered functionally identical for the purpose of informing countermeasures.

Inside Story : Opel Vs Volkswagen

It’s bad enough for a company when their top executives jump ship – but imagine how it must have felt for Opel when their chief of production moved to rival Volkswagen and was followed by not one, not two, but seven other executives.

Opel cried industrial espionage – over an alleged missing bundle of confidential documents – in response to which Volkswagen parried with accusations of defamation.

The four-year legal battle was resolved in 1997 when Volkswagen agreed to pay General Motors, the parent company of Opel, $100 million and place an order for over $1 billion’s worth of car parts.

Volkswagen still refused to apologize, though, showing that even multinational car companies can be as stub-

Freeze Frame: Kodak Vs Harold Worden

Pensioner power was something that Harold C. Worden obviously believed in. After completing 30 years with the Eastman Kodak Corporation he retired and promptly set up a consulting company, brokering the services of over 60 other retired Kodak employees.

In his last five years working for Kodak, Worden was intimately involved with the development of the 401 film machine.

Not content with simply bringing with him several thousand confidential documents relating to the machine, he also convinced his successor to provide him with even more.

He was sentenced to one year in prison and fined $30,000, only a little more than he had received for the stolen information, which Kodak held to be worth millions of dollars. One wonders whether Worden pawned his gold watch too…

Evaluation and analysis of raw data are critical steps of the CIP. Data that lacks accuracy and reliability may be marginally correct data, concoction of very good data, bad data, or even disinformation.

What are the Information Hazards of Competitive Intelligence Information?

Very likely the target competitor would be aware of the organization's CI moves and could make all possible efforts to thwart or jeopardize the organization's CIP. The competitor may have its own CI activities targeted at the organization. Or it might intentionally generate disinformation to mislead the organization's efforts. In fact, the organization's CI activities may find data which the competitor has 'planted' to keep the organization "preoccupied" and "off-balance"

The objective of the Competitive Intelligence Program is to gather relevant information that is valid and accurate. Incomplete or inaccurate information may jeopardize the organization's CI efforts.

False Confirmation:

There might be instances of false confirmation in which one source of data appears to confirm the data obtained from another source. In reality, there is no confirmation because one source may have obtained its data from the second source, or both sources may have received their data from a third common source.

Disinformation:

The data generated may be flawed because of disinformation, which is incomplete or inaccurate information designed to mislead the organization's CI efforts.

Blowback:

Blow-back may occur when the company's disinformation or misinformation that is directed at the competitor contaminates its own intelligence channels or information. I

n all such cases, the information gathered may be inaccurate or incomplete.

What ICISSM is All About?

ICISS is purely non-commercial forum for security and safety professionals world-wide! It neither is with any support from any business groups nor is it projected by any business house in the back-ground. All its members have no stake in any solution providing or consultancy firms. Their association with ICISS is totally based on mutual benefit of knowledge sharing and networking.

We welcome all the security and safety professional world over from diverse background and encour-age them to interact freely by asking the questions, replying them or by sharing their knowledge and experience. The council also strives to have strategic alliances with similar forums world over for fur-therance of its objectives. Formed in 2010, the Council is totally apartisan, apolitical and does not rep-resent any pressure group or interest group.

ICISS strives not to provide surrogate platform for anyone to enhance their respective business inter-est. It is thus totally professionals' body aimed at, 'professionalizing the professionals'!

We in ICISS believe that having different view than the majority is not bad! In fact we encourage differ-ence of opinion and take every different views as intellectual stimulus to either convince or get con-vinced – either way both the parties are benefitted! Those who dare to think differently have shown that firstly they can think and secondly they are not overawed by the majority views! Such are the traits of 'Thought Leaders' and they deserve our respect!

For more details on our activities, please visit us at - http://onlineicissm.wix.com/iciss

What ICISSM can do for you?

Consultancy: International Council of Security and Safety Management (ICISS) would be happy in providing consultancy to Corporates on all matters relating to Industrial Security Management from the best security professionals as it has on its panel the very best security professionals from almost all over the world. We have accredited security consultants from India, South Africa, UK, USA, UAE, Belgium, Libya, Yamane and Austria to name few countries. All the security consultants are under oath not to represent any solution provider or system integrator, thus their consultancy and recommendations are most impartial.

On-site Security Survey and Audits: Conducting on-site security surveys and audits is the forte of ICISS. Its specialists have carried out numerous such surveys which were beneficial to clients in improving the security preparedness and also in cost-cutting. .

Contents Delivery: The experts of ICISS help the Clint in developing its plans, prepare manual and prepare various forms and formats to be used for every day security &safety functions. It will also help the Clients to develop the training contents such as write-ups and the presentations. The specific needs of specific niche segment of the industry will also be met by ICISS.

Forthcoming Event

GLOBAL DIGITAL SECURITY FORUM INDIA

Security Best Practices, Technology and Applications

31 Aug – 1 Sep 2017

Shangri-La Hotel, Bengaluru

Event Partner