International Council For Industrial Security & Safety Management

Newsletter: April 2015

Let's professionalize the professionals...

http://onlineicissm.wix.com/iciss

In past newsletter (March 2015) we discussed on the Insiders' Threat and what are the expectations of the employer from its employees on the privileged information which are entrusted to them or they come across in course of their employment.

We also discussed in the previous newsletter on fiduciary duties related to employees leaving the employment and also provided draft of a letter which could be used with modifications in any organization which feel it can be target of poaching, insiders' threat and leaking of privileged information by ex-employees.

Considering as a logical extension we are focusing on this issue on the business or industrial espionage – how it is done and what to do to be prepared against it. It is dealt at the organization level as well as at individual level.

We are also discussing in this newsletter about what is business or competitive intelligence and how it is different than business or industrial espionage - overarching consideration being that while former is legal and legitimate action, the later one is illegal and criminal act!

Security professional would be better advised to study in-depth on the subject and formulate plans and procedures to combat this menace which is like termite – it is harming you from inside and you will know about it when it is too late!

Pinkerton – FICCI India Risk Survey 2015 is enclosed for our readers' benefit. ICISS supported this survey.

Capt S B Tyagi
For ICISS

What is Industrial or Corporate 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**

There are four faces of Business Espionage:

1. 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.

2. 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.

3. 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.

4. 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.

In following pages we will read as to what makes business intelligence or competitive intelligence different from business espionage? We will also discuss on the key elements of business intelligence? Read on further to know what makes the business intelligence "intelligent"?

Industrial or Business Intelligence

Pramila

Sony Pictures' four movies leaked last year on-line due to hacking by a group behind it calling itself "Guardians of Peace". North Korea is allegedly suspected behind it. Similarly Federal Prosecutors in USA have investigated whether Reuters Analytics (a subsidiary of Reuters Holdings PLC) was guilty of industrial espionage activities which involved break- ins of computers at its competitor Bloomberg.

These 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. Above particular stories pools the two of those together.

Expect more industrial espionage stories from USA and other countries of the world. India has already been in new due to snooping done at various ministries on the behest of the leading corporates. In the months ahead more corporate cracking into other computers may surface. 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.

Pramila has been studying the changing trends in industrial crimes and the malpractices corporates engage for over a decade. She has migrated from the field of education to Corporate Laws even after post-graduate degrees of MA (Hindi) and B.Ed.

After her LL.B; she has been mostly involved in studying, projecting and forecasting the trends in corporate ethics, malpractices and competitive intelligence. Due diligence and background screening is other fields of her expertize.

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.

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.

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 a definition of its information needs, the organization may not be able to deploy its resources 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. Omission, which is the seeming lack of cause for a business decision, raises a question to be answered by a plausible response. Anomalies (data that do not fit) ask for a reassessment of the working assumptions (McGonagle & Vella, 1990). 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 (Vella & McGonagle, 1987).

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 (McGonagle & Vella, 1990). 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.

What are the 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, although it is more expensive. 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.

How can the Competitors Foil Your Competitive Intelligence Program?

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 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, inquiries 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 flattery of organization's employees to encourage disclosure of important facts. In the non-sale sale technique, the competitor pursues the organization's non-employee associates such as distributors and suppliers to elicit information about the organization's pricing structure, customer service, etc.

What are the Information Hazards of Competitive Intelligence Information?

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

In the age of merger and acquisition, the business intelligence has acquired an important dimension. There are very important strategic information which are required to be obtained and gleamed -through for making the decision involving heavy amount that there is no scope of there being wrong or late! The delivery is important and also equally important is trustworthiness. This therefore is not left to unprofessional and it is very logical that security professionals with sound knowledge of finance and operational knowledge of the targeted business entity step-in so that they play the role of decision facilitators of the management. There are also imperatives on them to be ready to counter similar attempts on their own organization ‘cause it is jungle out there!’

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

New Security Technologies in This Decade

'Security technology' was widely considered to be one of the major up-coming industries in past decade. That time is now! The sector's growing significance and generous government aid in leading economies has made the industry one of the winners in the decades to come.

The dawn of this year promised to bring a bevy of new products and innovations to the physical security industry. End users continue to migrate away from legacy security systems towards technologies that enable them to be more proactive in mitigating their risks.

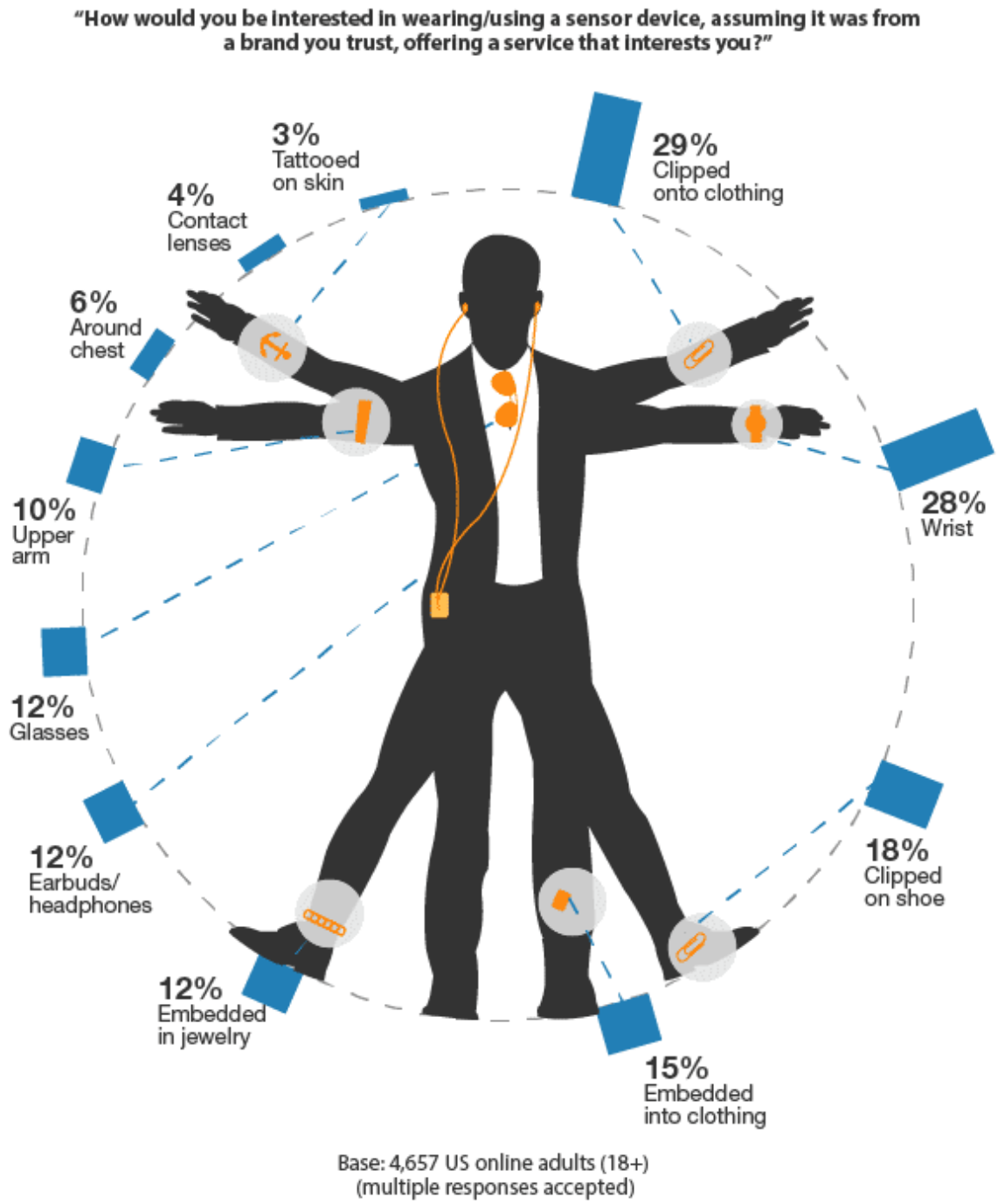
Last year's investigation into the bombing at the Boston Marathon showed the potential waiting to be unlocked in using big data analytics to comb through troves of video evidence. The ability to remotely access and control security systems from mobile devices also continues to rise in prominence.

In the melee, 'wearable technology' is creating its niche. It will be used for hordes of security applications, major being –

- Personal Security – for individuals' own security
- Used by Security personnel
- Biometrics Identification for logging-in and other authorisations
- Data storage and data sharing / migration
- Access control System
- Remote Access to CCTV and data transfer through Smartphones
- Asset Monitoring and inventory Control
- Alarm Notifications & Verifications

During 2014, we expected to see the first phases of mobile access deployments in which smartphones will function similar to that of a card transaction today, with limitations due to technology and business ecosystems. In subsequent phases, the phone's onboard computing power and multimedia capabilities will be leveraged to overcome limitations and provide a more functional and rich user experience.

In 2015, while looking forward, the connectivity of smartphones will now be used to perform most tasks that today are jointly executed by card readers and servers or panels in traditional access control systems. This includes verifying identity with rules such as whether the access request is within a permitted time and, using the phone's GPS capability, whether the person is actually in the vicinity of the door. The user can then be validated using a cloud application and granted access via a trusted message over secure communication to the door.



To do this, many leading industry players are spending an increasing amount of time in the world's innovation centers looking for technology partners to power the next generation of products and services, while at the same time staffing up their own innovation efforts to at least keep pace with the table stakes in the industry - think iPhone apps! For instance, one technology offering allows homeowners to arm and disarm their home security system, light control, and climate via their iPhone; it also sends notifications to smartphones if alarms are triggered.

Students invent a sound wave fire extinguisher -

Students invent a sound wave fire extinguisher - CNN Video...

A duo of undergraduates at George Mason University in Virginia crea ed a device that they say puts out fires with nothing but sound.

Handheld gadget uses pressure waves to remove oxygen from the flames - Students at George Mason University, Fairfax, Virginia, made the device. It works because low frequency noise separates oxygen from fuel. Students likened the noise to 'the thump-thump bass in hip-hop'.

The 20lb (9kg) device, which would not look out of a place in Ghostbusters film, was created by engineering students Seth Robertson and Viet Tran from George Mason University.

Device could potentially replace traditional fire extinguishers. The thumping bass lines that go along with rap songs may exasperate some reluctant listeners, but such low noises can be used to put out fires.

Two engineering students have built a handheld device that uses sound to extinguish flames - and the breakthrough could one day revolutionise fire-fighting. It works because the low frequency noise, which they liken to the 'thump' of hip-hop music, separates oxygen from fuel to stop a fire from burning.

Read more: http://www.dailymail.co.uk/sciencetech/article-3012955/How-fires-extinguished-using-SOUND-Handheld-gadget-uses-pressure-waves-remove-oxygen-flames.html#ixzz3Vxh5Z1Bi

Better be despised for too anxious apprehensions, than ruined by too confident security.

- Edmund Burke

"You shouldn't overestimate the I.Q. of crooks."

- Stuart A. Baker, General Counsel for the NSA

Dates to Remember!

Ways to register

Fax: +91 22 6144 5999
Tel: +91 22 6757 5980
Email: info@india.messefrankfurt.com
Post: Conference Department, Messe Frankfurt India, 215 Atrium, B – Wing, 2nd Floor, Andheri Kurla Road, Andheri (E), Mumbai 400 093, India

ICISS International Council For Industrial Security And Safety Management

messe frankfurt

ICISS at LinkedIn: http://www.linkedin.com/groups?gid=4413505&trk=hb_side_g
ICISS at Google Group: https://groups.google.com/forum/?fromgroups#!forum/icissm

---

Suggestions & feedback may be sent to us on e-mail: onlineicissm@gmail.com

---

P.S. - If you don't like to receive our newsletter, we apologize for bothering you. Please let us know your mail address and we will move it out from our contact list, thank you!