



**ÆGIS** e-journal

***Addressing threats that affect your bottom line***

Volume 3 Number 4, April 2000

From the case files of

The LUBRINCO Group  
<http://www.lubrinco.com/>

and

Financial Examinations and Evaluations, Inc.  
<http://www.feeinc.com/>

**Intellectual property being stolen or at risk? Call us!**

**This month's features:**

- 1. Due Diligence — Reputational risk**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — How do you know what your CI needs may be?**
- 3. Executive Protection — The protective agent abroad**
- 4. Technical Issues — E-mail and privacy**
- 5. Real Stories from the Field — Echelon**
- 6. Book and Product Reviews — Financial Investigations & Forensic Accounting**
- 7. Free-Subscription/Unsubscription/Copyright Information**

## **1. Due Diligence — Reputational risk**

Reputational risk is the potential risk that negative publicity regarding an institution's business practices, whether true or not, will cause a decline in the customer base, costly litigation, or revenue reductions.

Is reputation everything? In some cases the answer is "YES, IT IS!" Johnson & Johnson very effectively handled a poison scare after a disturbed man began tampering with Tylenol bottles and placing poison in them. Johnson & Johnson ordered a US wide recall and re-introduced the product later. They were widely acclaimed on how they handled the product recall and re-introduction.

Can you imagine an on-line tax preparation firm that has hundreds of thousands of names on its server and the web site is hacked? This business would — or at least should — be gone within minutes.

Can you imagine a rumor spread about a bank that might fail? What happens? There is a run on a bank. In one instance a bank manager reported to the police that a person on the inside had embezzled money and pushed for prosecution. That bank lost 8% of its deposits over the next several days.

How important is reputation to your business? Ask your customers. Use a quality group of customers and proposed "hypothetical" publicly disclosed problems. If what appears to you (the insider) to be relatively minor problems cause an adverse reaction in 5% or more of your customer base, then your reputation is very important.

Have a team assess your weak points; have a group initiate or identify a Public Information Officer (PIO) who is associated with the firm or your advertising agency, if they specialize in this type of "crisis communication" and begin role playing. Use several "what if" scenarios and test them on your customers again. This will help you assess your weak points and take measures to eliminate them. Through trial and error you will get the PIO's message correct. With professional assistance in crisis communication you will get to the correct answers faster.

Why is this a due diligence issue? Because any case in which you face risk or civil liability for negligence actions is a due diligence issue.

What could be more important than to protect than your reputation? And you protect your reputation through proper exercise of due diligence.

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — How do you know what your CI needs may be?**

CI is a process intended to assist in maintaining or developing a competitive advantage. It allows a company's management team to assess change in its industry, as well as the capabilities of current and potential competitors. CI exists to ensure that the organization has accurate, current information about its competitors, and a plan for using that information to its advantage.

Effective implementation of its CI requires not only information about the competitors, but also information on other trends in an industry: legal and regulatory, international, technological, political, and economic. The relative strength of the competitor can be judged accurately by assessing it against the factors listed above. As the speed of change increases external factors assume greater importance in effecting organizational change. Thus, the determination of CI information needs is based upon the company's competitive advantage over the competitor assessed, and further assessed against both internal and external factors.

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

One of the most important roles in CI is that of educating the organization on change. Once needs have been defined, the CI group is responsible for collection, evaluation, and analysis of raw data, and the preparation, presentation, and dissemination of the intelligence gathered. The CI-group 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-group has to decide upon the choice of sources of raw data. Should it use government sources or on-line databases, interviews or surveys, drive-bys, or on-site observations? It also has 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.

The purpose of CI is to gather accurate and reliable information. The groundwork for the CI is done by beginning with a review of the organization's operations to determine what is actually known about the competitors and their operations.

When an organization has some knowledge about its competitors and its own CI needs, it proceeds to the stage of gathering data. Based upon the needs, relevant data can be gathered from the organization's own sales force, customers, industry periodicals, competitor's promotional materials, its own marketing research staff, analysis of competitor's products, competitor's annual reports, trade shows, and distributors. Specific techniques include querying government resources and on-line 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 (determining what your competitors are trying to find out about you), competitive bench marking, 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 beg for a check of the working assumptions. 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 is a major source of incorrect interpretation. Challenge what you have learned. If the information doesn't fit the model or fact you have, then what model or hypothesis does it fit?

Evaluation and analysis of raw data are critical steps. Data that lacks accuracy and reliability may be marginally correct, a mixture of very good data and bad data, or even disinformation. All data is produced or released for some specific purpose. In CI, reliability of data implies the reliability of the ultimate source of the data, based upon its past performance. Accuracy of data implies 'correctness' of data. Evaluation of 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 may mask (this is disinformation) its 'real' intentions. The analysis should be conducted not only by the CI group, but by as broad a range of professionals in the firm as the CI-group can muster. The resulting CI information and its

analysis can then be integrated into the company's internal planning and operations for developing alternative competitive scenarios, structuring attack plans, and evaluating potential competitive moves.

Some suggest you should not build the mother of all databases, because A), no one is there to feed it, so maintenance becomes a nightmare, and B) it is so poorly focused, there are a jillion things in there, most of which are worthless, and no one can figure out what is good and what is worthless.

For some, the term "competitive intelligence" evokes images of computer hacking, dumpster diving, and other cloak-and-dagger activities. But there is enough information available from good sources to make questionable practices unnecessary.

Most of the information you *need* (not *want*) is publicly available. CI professionals frequently call a client's competitors seeking information. The darndest thing is that most of the people called answer the questions. Some will ask on whose behalf they are calling. Even when the CI professional names the company, and even if unable to name the specific client, most will still answer.

Keep in mind that no one involved in modern decision making needs 100% of the information to make good decisions. Not even historians get 100% of the information.

### **3. Executive Protection — The protective agent abroad**

In many third world environments a combination of poverty, corruption, organized (and unorganized) crime makes operating conditions for western multi-national organizations fraught with difficulties and sometimes dangerous. However, it isn't necessary for the environment to be threatening for companies and their senior people to require advice and protection.

A distinction needs to be made between body-guarding in general and the work of executive protection in particular. Competence in a comprehensive range of combative skills is essential and maintenance of those skills a necessity, but in terms of importance in corporate security, they come well down the list: Going about equipped with a range of weaponry, handcuffs, and specially designed suits to conceal a range of covert kit is just not the real world of protection.

The protective services world is about management, logistics, detailed planning, detailed advance work, and the ability to operate amongst the most

senior people of international business, without intruding on them, and without your actions drawing attention to them.

There are certain places in the world where, given the potential level of threat, a protective detail may need to be armed. But the people who are armed will be the indigenous security personnel escort team members. Often they will be off-duty police officers licensed to carry weapons. It is the height of folly to carry a weapon in a foreign country, irrespective of who has authorized it: The person who jails you for carrying one may have more authority than the one who approved it.

Most EP details follow a similar formula. The CEO of a multi-national operation, probably American in origin, is making a trip to one or more countries, to visit his company's operations there. The individual whilst in the States faces no threat, but the combination of the third world environment, anti-U.S. sentiment, and the profile of the visit justify security planning for the visit.

The company's head of security, or the protective detail team leader, will be charged with organizing the operation, usually at arm's length, by contracting with an agency he has used before and who themselves have a network of international links through which local manpower and material can be supplied, or by utilizing his own contacts in the country to be visited.

The reality is that often all that is required is one or two operators who will carry out all the planning, detailed advance planning, liaison work and ultimately act as the personal bodyguard to the principal. In any foreign country you need local drivers and people who are familiar with the environment.

The initial brief will be just that – brief – and is likely to contain little more than the dates (which will invariably change) and the resources felt to be appropriate (which will also change)

In the textbook world of protective work, the tasks would be the *security advances*, which includes the detailed planning and pre-visits that go into any travel arrangements. As with any operation, advances are budget driven, but if the threat demands and budget is no deterrent, then the stages are as follows:

- Pre-advances (planning stage)
- Trip advances (arrangement finalization)
- Visit advances (immediately before the party arrives)
- The aim of the above is:

- To avoid all surprises
- Plan contingencies
- Avoidance of hazards and vulnerable situations
- The object of the advance is:-
- To arrange all accommodation
- Transport arrangements
- Special events arrangements
- Security and law enforcement liaison
- Assessment of emergency / evacuation services

It has to be remembered that in the preparation stage you have a tradeoff of having to disclose the identity of the principle. Often you will not get the best of what is available, particularly with hotels, unless they believe that the visitor is truly a VIP. If the company you are working for has an operation on the ground you will be working in close liaison with them, which in the majority of cases will be a positive experience. However, their imperatives in organizing affairs may be in direct conflict with your requirements, both in terms of security and in what is possible to achieve in a trip of only a few days.

You might have to be firm though, even to the point of taking matters out of local corporate hands if they are too much at odds with your requirements.

- The advance should evolve as follows:
- Pre-departure preparations
- Initial duties on arrival
- Transportation arrangements
- Site surveys and route reconnaissance
- Emergency services

With the pre-departure plans we have three broad areas of work to do:

Collect information – Itineraries, dates, times, type of visit, numbers in party, special VIP and medical requirements (if any), proposed transportation, and accommodations, preliminary threat assessment and threat category, visa requirements, immunization needs, language and country data, account billing.

Contacts by telephone – Corporate, either multinational or local security company. Accommodations – hotel or residence. Transportation – ground, air, or other, and vehicle rental or supply. Police or government agencies if personally known or utilized.

Try to make as many appointments as possible by phone (with fax confirmation) before you leave, with all of the above. It is surprising to find that in many third world countries it can prove more difficult to speak to someone on a local land line, when they may be only one mile from your hotel, than it is to speak internationally when you are many thousands of miles away. So if you know that the local communications infrastructure is not good, then make the appointments before you leave. At a minimum, get the names of the people you will need to see when you arrive.

Plan itinerary for the advance: Prioritize tasks, prepare survey itinerary, prepare checklist of all questions, queries, intelligence required. etc.

From bitter experience I will tell you never to believe anything anyone tells you about how something will happen, without interrogating people in detail about the procedure. Doing a route reconnaissance in Paris or in Mexico City on a Sunday gives no impression as to what the traffic is going to be like on Monday at 0830. In some countries people will tell you what they think you want to hear in response to any question, knowing full well that when it doesn't work, they won't be around or on duty anyway.

Of course there are assignments, mainly in Europe, which go off without a hitch, but it is because we leave no stone unturned in brainstorming what could go wrong, however remote, and then putting in place a contingency arrangement. It is the contingency planning that is so critical.

Time constraints, budget restrictions, lack of resources, and client imperatives have far more impact on how we are able to do the job than the threat ever does.

#### **4. Technical Issues — E-mail and privacy**

Let's look at some specific threats. Most Web browsers hide the HTML portion of a link, showing only a highlighted word or two. Many e-mail clients, particularly those embedded in Web browsers, perform this service as well. It is a useful feature, in most cases. After all, HTML code is both bulky and mysterious; and most e-mail users have neither the expertise, time, nor motivation to analyze every incoming bit of HTML. However it can leave a user open to attack.

An e-mail (solicited or unsolicited) can contain a URL address. If just a web site, most visitors assume their visit is anonymous. All the site will get from a visit, in general, is an IP address or perhaps a domain name. The site can't use either of those to send the visitor more e-mail or identify one as a visitor. However, URLs can contain other items, including parameters that can be transmitted back to the URL site. If the visitor visits the site, the visitor's e-mail address, can be put on a e-mail mailing list.

The web site managers had already obtained the e-mail from an existing list, but they didn't know if the recipient address was valid. Now they do. It gets more intrusive. If a Web browser is used to handle e-mail, even opening the e-mail message may be enough to initiate a significant loss of information. Many web browsers are capable of enhancing e-mail messages with all sorts of (possibly invisible) images, retrieving them when a message is opened from any specified URL. The sender is free to include an IMG tag that includes the recipient's e-mail address in a parameter.

How about a cookie? The sender now knows that the sent message has been opened. The sender's website can also return a cookie to the recipient's browser containing the recipient's (possibly disguised) e-mail address. This means that any future visit the recipient makes to sender's site (or other, cooperating sites) can be recorded and indexed to the recipient's e-mail address. In short, the sender's anonymity will have been severely compromised by the recipient's e-mail software, without the recipient's knowledge or permission.

These sorts of attacks can take many forms. In one possible scenario, the sender could generate a unique URL for each outgoing e-mail message, joining random names (trixi, bubbles, etc, ...) with random letters or numbers (a, b, or 1,2,3). As each piece of e-mail is sent, the sender saves the outgoing e-mail address in a database, keyed by the unique portion (trixi - 1) of the URL. When the image request is received, a hidden CGI script can record the request in the database, send the recipient an identifying cookie. You must remember, any image request could be tagged.

Finally, if the recipient is foolish enough to click on an unknown URL, the sender doesn't need parameters or even "hidden" code. The same logic applies: Because the sender knows whom he told about trixi - 1, the sender knows who is asking to see the Web page. It is apparent that convenient "features," made possible by aggregating pieces of software (in this case, e-mail and Web clients), can lead to unexpected security holes.

Microsoft is the most obvious perpetrator here, but Netscape and others have contributed to the situation. This is not about blame; it is about fact, and in truth most of us value convenience over security. In an environment where random miscreants can send e-mail to unsuspecting victims, keeping a few barriers in place seems only prudent. The spate of e-mailed “macro viruses” provides a clear example of the reasons. Putting macros — interpretable code — into word processors and other programs is clearly a powerful and useful idea. Having e-mail software start up a copy of the word processor, so you can read formatted mail, is convenient. The combination means that bad people can run macros on a recipient’s machine merely by sending e-mail.

We are aware of no global solutions. However, many feel you shouldn’t use web browsers or highly integrated systems, such as Microsoft Outlook, as e-mail clients: They’re far too accommodating to bad people sending e-mail. If you must use e-mail software with known security holes, try to use it in a conservative manner. Turn off any automated features, such as automated program invocation, that might allow others to take over your machine. Until the vendors add some real security, the user must weigh the risks versus any possible convenience.

Trojan horses can come in many guises, and one should not trust a stranger’s offerings, even if they contain no visible threats.

## **5. Real Stories from the Field — Echelon**

Echelon is a network of surveillance stations stitched together in the 1970’s by the United States’ National Security Agency in conjunction with Australia, Great Britain, Canada, and New Zealand. These are intended to intercept select satellite communications, according to recently declassified information in Washington.

Echelon had been set up as a military system, dating originally from 1948, to eavesdrop on the Soviet Union and its allies in the cold war. Today, according to some, it appears that the network has been diverted to the purposes of economic espionage and for keeping a watch on competitors.”

The computers watch and listen for key words in telephone, fax, and Internet communications, and route intercepted messages on a topic requested by a participating country.

Echelon came into the public view with the publication today of an 18-page report, which was written by a freelance journalist, Duncan Campbell, and based in large part on other newspaper accounts, and said Echelon had been

used by the United States to gain the advantage in at least two deals that involved major European companies.

Mr. Campbell described Echelon as a vast coordinated system that includes a system of satellites and at least 10 listening posts worldwide that can intercept telephone calls, e-mails, and faxes. The report drew skepticism from conservative parliamentarians, some of whom said it had failed to provide sufficient proof.

Press reports from 1995, according to Mr. Duncan, said information learned through Echelon had been given to Boeing and McDonnell Douglas when they were trying to win a \$6 billion contract from Saudi Arabia. His report said the spy network had intercepted calls between Airbus, the European consortium, and the Saudi airline and government officials.

Mr. Campbell also said spy information had helped an American company, Raytheon, win a bid for a \$1.3 billion surveillance system for the Amazon forest away from Thomson-CSF, a French company.

In recent years, Echelon has been criticized in the United States as an excessive intrusion into the private communications of Americans and their allies. Some critics said the system emerged from the cold war as a Big Brother without a cause.

On the Internet, Echelon has achieved a mythical status as a spying arm of the American government. A "Jam Echelon Day" was declared in October, and people around the world sent a huge volume of communications over the Internet and on the telephone using words like "terrorism" that they presumed were key words and would overload the system.

R. James Woolsey Jr., who headed the CIA from 1993 to 1995, said in Washington that "basically the United States does not conduct industrial espionage." But he noted that the government might look into some economic areas, like questions of bribery.

"You collect intelligence on bribery by some of our friends abroad and then you tell the U.S. government so they can try to get the other government not to award the contract," Mr. Woolsey said at the Council on Foreign Relations. "But you don't go to the American corporation and say 'Hey, you're about to lose...'"

While the world at large is just hearing of this technology and however-present the technology has become, many of those trying to do business in France, South Korea, Japan and China have known for quite some time that a prospective bidder cannot send their documents to a local office (in France,

Japan, China or South Korea) without losing a presumed privacy. ALL OF THESE TYPES OF TRANSMISSION ARE INTERCEPTED, READ, AND PASSED ON TO DOMESTIC INDUSTRY FOR ACTION. This has been going on for years, and the naiveté about how the information is intercepted and used is ridiculous.

## **6. Book and Product Reviews**

### *Financial Investigations and Forensic Accounting*

George A. Manning, CFE, E.A.

CRC Press ISBN: 0-8493-0435-0 488 pages \$79.95

<http://www.crcpress.com/> 1-800-272-7737

I really enjoyed this book. It is NOT an accounting book, but rather a book that thoroughly describes financial crime investigation and documentation. It goes from the beginning of crime recognition and covers such diverse topics as Offshore Money Laundering, Trial Preparation, RICO Net Worth Solutions, Wagering and Gambling, and all sorts of related topics. The topics are each treated in a separate chapter, so you can skip what doesn't interest you, and very easily focus on what you want to read. It does cover some accounting principals on calculating net worth determinations and cash from un-disclosed sources.

This book is a very good tool for training law enforcement professionals engaged in expert testimony, lawyers, judges handling such cases, and any one else who is interested in the topic. A good addition to the library.

## **7. Free-Subscription/Unsubscription/Copyright Information**

•• AEGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2000 by The LUBRINCO Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com) and L. Burke Files (LBFiles@lubrinco.com).

**The LUBRINCO Group** provides services in three high-threat areas, too specialized to be dealt-with in-house, that can adversely affect domestic and international bottom lines.

- **Protection of trade secrets and intellectual assets.**
  - Anti-economic espionage.
  - OPSEC: The identification and protection of information that would give your competitors and adversaries an advantage.

- **International financial investigations and due diligence consulting.**
  - Location and recovery of missing and hidden assets.
  - Establishing business relationships and strategic partnerships in Central and Eastern Europe, the offshore financial centers, Beijing and Shanghai, Central Asia, and Latin America and the Caribbean.
  - Anti-money laundering and financial fraud requirements under the *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001* and the *EU Revised Money Laundering Directive of 2001*.
- **Protection of management, staff, and families.**
  - In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.
  - When traveling and living overseas.
  - When transporting items of substantial value.

LUBRINCO identifies and quantifies threats and vulnerabilities, and their associated risk, then manages the vulnerabilities so you can transfer or live with the residual risk. We prevent disastrous financial loss to your company, and physical harm to you, your family, and your staff.

For information on **The LUBRINCO Group** and its services, or for the archive of all past issues of *ÆGIS* e-journal in PDF format, please go to <http://www.lubrinco.com/>.

To sign up for a **complimentary subscription** to *ÆGIS* e-journal or the *ÆGIS* e-journal PDF notification list, go to <http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com).

To subscribe to our AvantGo channel, go to [http://avantgo.com/channels/\\_add\\_channel.pl?cha\\_id=1773](http://avantgo.com/channels/_add_channel.pl?cha_id=1773)

To be removed from the subscription list, follow the instructions on the mailing you received, or send an e-mail to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com).

If you know of anyone else who should be receiving *ÆGIS* e-journal, please send their e-mail address to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com).

If there is a topic that you would like to know more about, send it to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com) and the editors will consider it as the topic for an article in an upcoming issue.

If you would like to submit an article for publication in ÆGIS e-journal, send it as an attachment to an e-mail to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com). Submission of an article certifies that (a) all information in the article is in the public record, or (b) that you are authorized to release any personal or corporate proprietary information contained in the article, and (c) that none of the article has previously been copyrighted. The submission of materials for publication in ÆGIS e-journal constitutes a license to The LUBRINCO Group Ltd, Inc., and/or Financial Examinations and Evaluations, Inc, their assigns, associates, or affiliates, to abridge and/or edit said submission, and to copyright and publish/republish any submitted materials in whatever written and/or electronic form they may choose.

If you would like to go beyond normal fair-use in reproducing articles from this issue of ÆGIS e-journal, you may do so freely as long as appropriate source, copyright, accreditation, and link to the LUBRINCO website is included. This should be in the form

*Article Title*, from the April 2000 ÆGIS e-journal (© 2000 LUBRINCO & FEE), to be found at <http://www.lubrinco.com/>.

ÆGIS e-journal is a forum for the exchange of information, ideas, operating styles, theories, and related topics for corporate managers who make decisions about threats typically outside the expertise available in-house, yet which have the potential to affect their company's domestic and international bottom lines. Nothing appearing in ÆGIS e-journal should be construed as legal advice. The information provided is "general information," not "specific advice."

The solution to any problem is highly dependent upon the precise facts involved. Thus, before making any reliance upon anything said here, you should consult with an appropriately skilled professional. Opinions expressed by contributors are not necessarily endorsed by the publisher, and may be presented to encourage a dialogue among subscribers. The publisher and any re-publisher cannot be held responsible for any loss incurred as a result of the application of any information published in ÆGIS e-journal.

Please be safe, and be smart.