



**ÆGIS** e-journal

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

Volume 2 Number 8, August 1999

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 — Some good / bad examples**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Disinformation**
- 3. Executive Protection — Piracy**
- 4. Technical Issues — Who can read your data?**
- 5. Real Stories from the Field — Skip tracing**
- 6. Book and Product Reviews — Who Knows What?**
- 7. Free-Subscription/Unsubscription/Copyright Information**

## **1. Due Diligence — Some good / bad examples?**

*“With Due Diligence you can determine who is the predator and who is the prey. The answer often comes as a great surprise to both parties.”*

A July 4th tragedy occurred when a fireworks event went terribly wrong during set up. A worker, adjusting a mortar, somehow ignited the mortar. That sent a hot round into a truck that transported fireworks, and ignited the unloaded fireworks. Some of these ignited fireworks launched themselves into a van where specialty (larger motor size) fireworks were being kept. A large fireball of fireworks and explosions occurred, severely burning two, one of whom who later died.

The show was contracted by the city where the explosion occurred. The fireworks display company hired had been cited by neighboring city fire departments in previous years for violations, and, as a consequence, this company was *not* invited to bid on the neighboring cities fireworks displays.

The disaster could have been avoided with a simple round of calls to the previous clients of the independent contractor, requiring maybe two hours of work on the telephone.

The moral is that if there is risk involved in a business deal — and there *always* is — you should exercise due diligence in seeing that all is as it should be. While risk can never be avoided entirely, it can generally be reduced significantly at little cost.

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — Disinformation**

*The process of disinformation is the creation of a plausible set of circumstances and events to misinform a competitor as to the actual events surrounding one’s activities.*

When this editor was in graduate school, a friend left a deck of computer punch cards in the computer room one evening. Assuming this was an oversight, I mentioned this to him. He explained that he was involved in a very competitive school project, and that if he “accidentally” left the deck overnight, one of the other teams would find it, run it, be misinformed about his group’s project, and change their project accordingly.

It works about the same in real life.

Phoenix, Arizona, is a very active area for the semiconductor industry. What California has in design and build capabilities Arizona can match in sheer

volume of chip production. It was because of this that a major semiconductor manufacturer decided to locate in the Phoenix metro area.

A plant site was selected and permits were obtained for a variety of manufacturing processes and building locations on the plant site.

Several, though not all, of the buildings were constructed on the plant site, and the manufacturing equipment was beginning to be delivered when the hazardous material storage area began construction. To construct such an area the soil must be pre-tested before construction. Once tested the area must be lined with an impermeable layer and then paved with concrete. Once paved with concrete the storage tanks and their holding pens can be constructed on the site. Shortly after the permits for storage of hazardous chemicals were obtained, a series of angry protests erupted over the location of the plant, over the types of chemicals used in the manufacture of semiconductor chips, and over the proximity of the plant to residential areas. These protests reached city hall and appeared on the local news.

Sometime after the hazardous materials site was paved, the real nature of the plant was discovered. It was not involved in the manufacture of computer chips. Rather it was to manufacture of new equipment used to manufacture compact disks.

This elaborate ruse, one among many, was used so the manufacturer did not alert competition that a plant to manufacture this specialized equipment was being built. It allowed the manufacturer to gain a 14 month lead on the competition. This lead — and the competitive advantage the new equipment gave to the manufacturer — allowed the manufacturer to come from no presence in the market to a market share of over 85% within six months of the time the plant opened.

When asked what became of all of the other planned buildings, hazmat permits, and the storage tank field, the answer was succinct: *Permits* to build buildings and store hazardous materials are cheap, while advance warning to competitors is not.

The paved area for the “hazardous storage facility” has been striped, and now serves as part of the employee parking lot.

### **3. Executive Protection — Piracy**

Piracy is alive and very dangerous. I have been persuaded to write this article after a friend nearly was - [robbed, hijacked, killed] during a pleasure sail in the Caribbean. Several shots from a old 50 caliber BAR fired at the

pirates' heads, and then at the waterline of their approaching vessel, dissuaded the pirates from approaching any closer. How did they know it was a pirate ship approaching them? There were 6 men with rifles at the edge of the boat posed to jump to the pleasure vessel when and if it came within range. It wasn't a catering boat.

How big is piracy on the high seas? it's big — really big — and a real problem. A recent conference was convened in Japan because their commercial shipping has been being hit hard by pirates. Total attacks by pirates are on the rise, 1995 <=> 140, 1996 <=> 175, 1997 <=> 229, and in 1997 over 400 persons were held as hostages and 50 were killed! Most of these reports are on commercial shipping, only. The pleasure craft industry is hit with losses due to theft and piracy to the tune of \$100 million per year world wide.

### ***How do modern day pirate operate?***

Pirates are in the business of piracy for profit. Large commercial ships with valuable cargo and ships that have been “flagged by countries of convenience” are primary targets. Highly automated, these ship are run with few crew members, and there are no extra bodies to stand watch. Pirates use small high speed boats to select and attack their prey. The pirates approach from the sides and/or the rear and board the ships. The ships crew are often robbed, the ships safe is robbed, and the crew members held hostage while the pirate take what they can. During this period of time, while the pirates are searching the ship and the ships crew is held hostage, no one is steering the ship!

Some shipping companies now keep the ships safe empty. When that occurs the murder rate increases. No money, no live hostages.

The areas that have been hit the hardest have been Indonesia, China, Hong Kong, Macao, and Brazil.

Pleasure craft have been hit hardest in Indonesia, Thailand, and the Caribbean coasts off Nicaragua and Columbia.

What do these places have in common? Indonesia, China, Malaysia, Vietnam, Thailand and Malaysia all border on the South China Sea. The South China Sea is a tremendous cross road for shipping, and is the entrance to the strategic Straits of Malaga, with Singapore at the eastern entrance. Nicaragua and Columbia are on either side of Panama Canal.

Both locations have a great deal of traffic, and all of these countries are experiencing a tremendous amount of political and economic upheaval.

A great deal of information for this article came from <http://maritimesecurity.com/>, and the Maritime Bureau of the International Chamber of Commerce.

#### **4. Technical Issues — Who can read your data?**

We have all heard about PGP and how it will block all eyes from our e-mail and how important it is to encrypt our disk drives, yadda, yadda yadda....

In fact, this is true, sort of. Rumor has it that while the government can crack a PGP encrypted file, it can take several weeks. We assume that while it is possible for a competitor to do so also, most competitors don't have the resources and expertise of, san the NSA.

But what about our privacy and what about protecting our proprietary information from business competitors who would like to spy on us? We need to be ever vigilant. If you wish to have a system that is ,more or less, tamper or invasion resistant (nothing is ever 100% secure) do the following.

If you only send out important messages and data encrypted, and someone is monitoring your lines, this raises a red flag for them. Encrypt *all* transmissions, no matter how trivial: Volume and expansiveness is a barrier to effective information gathering in and of itself.

The same goes with stored data: Encrypt all of the work product you can, no matter how trivial: Volume and expansiveness is a barrier to effective information gathering in and of itself.

While encryption can be effective, it is *not* effective on things that you have not bothered to encrypt.

Information on PGP can be obtained online at <http://web.mit.edu/network/pgp.html>

#### **5. Real Stories from the Field — Skip tracing**

How do you find someone who doesn't want to be found? Once you have separated the credit challenged from the credit criminal how do you find the credit criminals? It is easy: Follow their tracks.

Following and finding credit criminals is a lot like a woodsman tracking an animal by following its scat and broken twigs. Credit criminals leave behind their messes and broken agreements just like scat and broken twigs. The

simple fact is that most people don't disappear, and most people use or need credit to live. People also have to live somewhere, use water, gas, electricity, and telephones. Most people (outside of Manhattan) also have automobiles. With these basic needs, and the required fulfillment of these, needs a person can usually be tracked.

### **Utilities**

Absent a direct line to a utility pole, most credit criminals have stiffed one or more utility companies. Check the public records in small claims court for past utility bills that have been left unpaid. Many of the utility suits will contain full information about the person and their previous whereabouts.

### **Mail**

Send a letter addressed to the credit criminal at all of the known addresses and place in the upper left hand corner of the envelope a legend reading *Please do not forward. Address correction requested. Please return to sender. Return postage guaranteed.* The forwarding addresses received may lead to another bad address, or you may find a new address. If you are a process server, a private investigator, or an attorney you can use the *Request for Change of Address or Boxholder Information Needed for Service of Legal Process* form from the Post Office. The rules governing this form are printed on page 21607, 2-19-87 of the Postal Bulletin.

### **Vehicles**

While we may have a driver's license for from 5 to (in some states) 30 years our vehicles must be continually registered. Look for driver's license information and vehicle ownership information. (This, in many states will require a PI or a law enforcement officer to access the records). On the driver's license look for recent tickets, and the license plate of the vehicle in which the ticket was received. The credit criminal will either own the vehicle, or the person who owns the vehicle will know where the credit criminal is located. Most of the driving (80%) we do is within 3 miles of one's home, so a good guess can be made as to where the credit criminal will be living.

### **Credit Reports**

If you have access to credit reports, use it. You need an established credit relationship, request for relationship, or a judgment to access a credit files (General rules, but various from state to state. Check out your state's rules).

Look for recent or current accounts, and call the “Skip Trace Department”. They may try to put you off and say “Privacy Laws forbid us sharing that information.” That is incorrect. They can share *locate* information with you if they so chose: They merely can’t share *credit* information. And you don’t care about their credit: You just want to find them.

Note that skip tracing is as much a art as it is a science. You need to use all of your life skills to gather information and locate the credit criminal, their job, and their bank accounts for your clients — and before anyone else does.

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

*Who Knows What?*

Daniel Starer

Henry Holt

Go purchase this book. This is as great a source on business associations as I have seen. You need to know about the Yarn Industry? 17 listings of companies, industry associations, periodical’s and other information sources! While not all industries are small enough to be covered as thoroughly as the yarn industry, the 1200 page book is an excellent reference source for most industries.

So now you have an industry you are researching. Look to the Library Association for the source of those obscure publishers of Masters and Doctoral thesis’s on the subject or industry you are investigating. Look for periodicals that cover the industry you are researching. Interview the reporters for that periodical. These people will have an excellent feel for the industry, usually without a bias, and for who the leaders of the industry are today, and where it is going tomorrow. (Refer to the April 1999 issue of the *ÆGIS* e-journal article on working with reporters at <http://www.lubrinco.com/ejournal/lgej9904.pdf>). Call the Federal Trade Commission or the Department of Commerce for more information on the topic. Many time you can also find libraries dedicated to an industry.

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

•• *ÆGIS* e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 1999 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 August 1999 ÆGIS e-journal (© 1999 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.