



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 7 Number 8, August 2004

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:

• **Special Announcement**

- 1. Due Diligence — Trading identity theft for fraud**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Protecting indicators with offshore companies**
- 3. Executive Protection — Tracking mobile devices**
- 4. Technical Issues — Reading competitors' e-mail. Legally!**
- 5. Real Stories from the Field — Due diligence in unfamiliar fields**
- 6. Book and Product Reviews — Xcaper® Civilian Smoke Mask Dictionary of Strategy**
- 7. Free-Subscription/Unsubscription/Copyright Information**

L Burke Files will be speaking at OffshoreAlert's 3rd annual International Conference on Due Diligence and Asset Recovery. <http://www.offshorebusiness.com/DDARS/agenda.asp>

Hugo Guerrero, CPP, Vice President of The LUBRINCO Group, will be speaking at the American Chamber of Commerce (Medellin) Security conference, 21-22 October, Hotel Intercontinental, Medellin, Colombia.

1. Due Diligence — Trading identity theft for fraud

HR 2971, the *Social Security Privacy and Identity Theft Prevention Act of 2004*, just passed the ways and means committee. Identity theft is a serious problem, and nobody could object to legislation that cuts back on identity theft any more than they could object to the *Protection of Soft and Cuddly Bunnies Act*.

Unfortunately, when looking at any policy or measure five questions need to be asked.

1. What problem is the policy or measure trying to solve?
2. How can it fail in practice?
3. Given the failure modes, how well does it solve the problem?
4. What are the costs, both financial and social, associated with it, and flowing from its unintended consequences?
5. Given the effectiveness and costs, is the policy or measure worth it?

In the case of HR 2971, our concern is with the cost of unintended consequences. Imagine that you are not the victim of identity theft, but an abandoned wife who needs to collect child support from a deadbeat dad. Or that your life savings have been stolen by a fraudster. Or that your wealthy spouse wants a divorce, and insists that they are broke and have no property to split with you.

If you fall into any of these categories, HR 2971 virtually guarantees that you will never see the money owed you. The reason for this is that neither the police nor the state nor the federal government will drop what they are doing to locate the assets that have been concealed from you. Instead, your attorney will hire a private investigator.

Private investigators, not the government do the lions share of locating concealed assets in civil cases. LUBRINCO, for example, is involved in the search for roughly \$600 million dollars a year (mostly in high-value frauds, which tend to involve over \$100 million in any give case). But one of the tools we use is the social security number. Of 2000 John Q. Publics, which one has the same social security number as Mrs. Public's ex? What is the

social security number of the fraudster, and what accounts and properties can we find associated with someone who has that social security number? Without access to the information in credit header and other locator information, which will be denied to licensed private investigators under sections 107 and 108 of HR 2971, investigations will become either impossible or cost-prohibitive.

For the very rich, the law will have little effect. They will either have the clout to get law enforcement to take action, or will be able to afford to spend large amounts to get the information they need.

For those of us in the middle class or below, or for those stripped of resources by a fraudster, concealed assets that might have been located will now never be seen, because their location will become un-affordable for us. For some, the penalties will far outweigh the risks of identity theft, and HR 2971 might best be renamed the *Deadbeat-Dad and Fraudster Protection Act of 2004*....

2. OPSEC, Economic Espionage, and Competitive Intelligence — Protecting indicators with offshore companies

Most of what is known about offshore financial centers comes from novels describing a clandestine event in the Cayman Islands in the middle of the night behind the fourth palm tree from the left.... And, in truth, many offshore locations specialize in privacy. And privacy can be a very good tool for the corporation trying to protect its business plans, its research, and its products in development.

Let's take the jurisdiction of Nevis, which has created a class of companies that can conduct business anywhere in the world. Well, anywhere in the world except Nevis. This class of company is *relatively* free from disclosure of ownership, operations, and financial condition.

How can this class of company be used to protect indicators that point to what you are doing?

- You have a large research project for which there is no statutory reporting requirement, and you are trying to keep your activities secret as long as possible. You can run the research and the contracts through a Nevis based international entity, so your competitors will have a much more difficult time following the trail.
- Your project requires that you hire a large number of people for a short period of time, either in your home country or a third party country. You

could hire them through an offshore company, so that even the employees don't know who the beneficiary of their labors may be.

- Your new product requires that you make significant purchases of a rare item. If the shipment of the rare item is linked to you by a competitor, that tell them about your future commercial activity. Purchases can be made from different shell companies in offshore jurisdictions. These shell companies can have the product shipped to a location not tied to you. The product can then, several times removed from its origin, be transshipped to you.
- You have a significant project you wish to explore in a dangerous area, where a representative of a large corporation is a prime target for kidnapping, but where the representative of a small company has a lower risk of being snatched. It may be prudent to form a number of small offshore companies in one or more offshore financial centers. The team arrives in the target country as unrelated employees of many different companies from different countries, with different cover stories. As an example, a geologist masqueraded as the buyer of mineral specimens for a Dominican manufacturing concern. The appearance of being with a small company reduces the likelihood of an individual being seen as an attractive target.
- You can avoid any obvious connection to your company by using offshore centers for the payment of travel and goods and services.

How do you handle the mechanics of setting up and running these offshore companies? You do it in conjunction with a trust company in the offshore jurisdiction of your choice. The trust company will act as a firewall between you and the rest of the world, and will have affiliated service providers in other jurisdictions to provide a more scattered profile if needed.

If you are just getting your feet wet in the world of offshore finance, a good place to start exploring is through the lexicon of offshore terms at the website of Tarsus Trust (<http://www.tarsustrust.com/publications.htm>), of which one of our editors is a principal.

If you are looking to delve a little more deeply into the world of legitimate offshore finance, one of the best primers on the industry is *The Offshore Money Book*, written by our friend and associate Arnold Cornez, JD.

3. Executive Protection — Tracking mobile devices

A new service, ChildLocate (<http://www.childlocate.co.uk/>) is available to allow parents in the UK to track children through their mobile phones. The children – or at least the handset– can be located within 30 meters, and tracked via the internet, or via text messages to another mobile handset. The accuracy will be better in the U.S, if ChildLocate makes it here, because of upgrades to the mobile system to enhance accuracy for 911 calls.

Obviously, if we can locate a child’s handset, we can do the same for an adult, giving the service a wider potential appeal.

However, there are two issues that need to be considered.

1. Does knowing where a person’s handset is located mean you know they are safe?
2. If you can find out where they are, can someone else find out to?

This second issue has been of some concern within the U.K (<http://www.spy.org.uk/cgi-bin/childlocate.pl>), and is worth considering when thinking about the protection of high-risk adults, especially since location technology used by law enforcement is making its way to the private sector.

We take society’s obligation to protect children very seriously (see our discussion of the *National Center for Missing and Exploited Children* in the April 2004 issue of *ÆGIS*). The question is whether this measure is worth the minor cost? To answer this question we come back to the five questions we need to ask of any policy of measure:

1. What problem is the policy or measure trying to solve?
2. How can it fail in practice?
3. Given the failure modes, how well does it solve the problem?
4. What are the costs, both financial and social, associated with it, and flowing from its unintended consequences?
5. Given the effectiveness and costs, is the policy or measure worth it?

Although over 300,000 children go missing each year, virtually all of these are either taken in a custody battle, or run away because they have been physically, emotionally, or sexually abused. We are not sure that this system will help when a child, knowing they have the tracking device, willingly goes with the other parent, or with a grandparent. And we are not sure the custodial abductor will not know about the system. We are also not sure that

we want a sexually abused child to be returned to their abusers, rather than, say, social services. And certainly children too young to have a mobile phone will not be helped, nor will it help those children where the abductor throws away the handset.

In terms of the small number of other abductions – the frightening and tragic abductions that make the papers and terrify parents – where there is a high probability of the child ending up dead, the odds of this happening are so miniscule that almost anything else done with the money would be a better investment. As an example, 36,000 people die in this country every year from the flu. Having your family vaccinated each year will do more to assure the survival of your child than a tracking system.

For those where a child – or an adult – is at high risk, however, there may be justification for considering technological approaches, one of which we hope to discuss in the next *ÆGIS*.

4. Technical Issues — Reading competitors' e-mail. Legally!

The United States District Court for the District of Massachusetts (*UNITED STATES OF AMERICA v. BRADFORD S. COUNCILMAN*), in noting the decision of United States Court of Appeals for the Ninth Circuit (*ROBERT C. KONOP v. HAWAIIAN AIRLINES, INC., CV-96-04898-SJL*), has made it clear that a provider of e-mail services can read e-mail sent by customers, and that they can use this information for their own benefit. This opens up a lot of possibilities.

One, of course, is the acquisition of information that can be used to the advantage of whomever reads the e-mail.

Another is that it now becomes attractive to form a service provider with the specific intention of gathering information from client e-mail. Or getting someone hired as an employee of a service provider handling clients in whom you have an interest. Or suborning an employee of such a company.

This decision also tells us that if you are concerned about other people reading your e-mail, it is now even more imperative that you send it in an encrypted form. One widely used set of encryption tools is PGP, which is available in freeware (<http://web.mit.edu/network/pgp.html>) and enterprise (<http://www.pgp.com/>) solutions. The software can be made to integrate with most commonly used e-mail clients, including Outlook, Outlook Express, Notes, Groupwise, ICQ, Entourage Apple Mail.app, and even The Bat!, which this editor uses.

Why would one not use encryption for sensitive e-mail? We are hard pressed to come up with a valid reason. While use of encryption does require remembering your secret passphrase, the difference between sending or receiving an encrypted e-mail versus an unencrypted e-mail, or of sending and receiving an encrypted attachment versus an unencrypted attachment, is literally a matter of mere seconds, so there is no valid reason not to encrypt sensitive e-mail.

Get encryption software. Use encryption software.

5. Real Stories from the Field — Due diligence in unfamiliar fields

How transferable are skills? Nobody is quite sure, which can make for some interesting problems when trying to hire a professional. On the one hand you would like to hire someone who has done that specific job before. On the other hand, the job may be sufficiently generic that some of the details do not really matter. As an example, if you hire a chauffeur, does it really matter that he has primarily driven black cars, while yours is blue? We rather think not.

This issue was recently brought home to us when a person whom one might have thought of as a very sophisticated international investigator did a background check, and found that the subject of the background check had lied about their credentials.

The victim of this background check claimed to have been in the securities industry, dealing in commodities. However, this alleged experience – at least from the perspective of having been licensed – was 15 years in the past. On the not-unreasonable (albeit incorrect) assumption that commodities are part of the securities industry, the investigator called the SEC looking for information on the subject's licenses. None were to be found.

Eventually realizing the mistake, the investigator finally called the commodity exchanges and found that the subject was not, in fact a commodities broker, but merely an *affiliated person*, which certainly sounds like some sort unlicensed peripheral position, and a *commodities trading advisor*, which sounds a step beneath salesman. The conclusion was that the subject never had a securities license as claimed, and had never been a commodities broker. Since the subject had never claimed to have been a commodities broker, we can only deduce that the investigator had confused a trading advisor with a broker.

The commodities and securities industries, while logically related, are, in fact, licensed and regulated by different bodies. The Securities and

Exchange Commission (SEC), a governmental body, regulates the securities industry. The National Association of Securities Dealers (NASD), a membership organization overseen by its member firms, licenses securities dealers and salesmen. The Commodity Futures Trading Commission (CFTC), a governmental body, regulates the commodities industry, and the member exchanges grant affiliate status to members once they have passed an exam and a background check.

The commodities business is a field that has a great deal of specific nomenclature, and an associated person is, in fact, an Associated Person, which is a licensed position. A Commodities Trading Advisor is also a licensed position. Although the subject never claimed to be a Commodities Broker (yet another specific licensed title), the fact of being an Associated Person and a Commodities Trading Advisor would mean that the subject had, in fact, been licensed and in good standing for some period of time.

Undoing the harm took the better part of a week, but required looking in the right places, which included speaking with the subject's previous supervisors for third-party confirmation.

How did what should have been a straightforward investigation go astray?

- 1) The investigator lacked industry specific knowledge, including detailed knowledge of the financial products and service industry.
- 2) The investigator did not call the subject and ask why they could not find any of the information that should have been (and was) there.

Background checks in some industries require specific knowledge of the industry. Doctors, lawyers, programmers, securities professionals, etc, belong to very technical fields, and the investigator needs to be aware of the industry nomenclature, terms of art, licensing requirements, and industry practices. Without specific knowledge, common-sense deductions may turn out to be wrong: To an American, a person claiming to be a British surgeon being called Mr. Smythe by all who know him, rather than Dr. Smythe, is suspicious. If you are aware of this custom – more of an affectation – you will know that is not actually a clue.

Calling on an industry expert makes sense if you don't know the field. And remember that, most of the time, background checks are not surreptitious. If something seems odd you can ask the subject about it, and verify what they tell you. This can prevent professional embarrassment, and reduce harm to the innocent.

6. Book and Product Reviews

Xcaper® Civilian Smoke Mask

Xcaper Industries, LLC

\$44.95

[http://www.whiffs.net/Merchant2/merchant.mv?Screen=](http://www.whiffs.net/Merchant2/merchant.mv?Screen=CTGY&Store_Code=W&Category_Code=Civilian)

[CTGY&Store_Code=W&Category_Code=Civilian](http://www.whiffs.net/Merchant2/merchant.mv?Screen=CTGY&Store_Code=W&Category_Code=Civilian)

1-949-852-2021



There are a lot of things that keep us up worrying about our clients at night. One of them is a concern about smoke, which is why we have reviewed smoke masks in the June 2001 and October 2001 issues of *ÆGIS*. The Xcaper Civilian Smoke Mask – the civilian variant of the mask made for emergency service workers – is a good addition to our lineup, and well worth considering.

The mask itself feels like a beanbag placed over the mouth. It comes vacuum packed, and is very compact. When you open the bag, you need to massage the mask for four or five seconds before removing it from the package. This re-distributes the aloe vera gel that helps the carbon monoxide, cyanide, acrolein, nitrogen monoxide, nitrogen dioxide, and other byproducts of a fire to be adsorbed. There is also a set of goggles available. By having separate goggles you avoid the problem of a hood misting up from your breath.

The vacuum packed mask is very small, and a good choice to throw into your briefcase, bag, or emergency kit.

Dictionary of Strategy: Strategic Management A-Z

Louis Kelly and Chris Booth,

Sage Publications ISBN: 0761930736 200 pages \$29.95

<http://www.sagepublications.com/> 1-800-818-7243 or 1-805-499-9774

We came to appreciate its contents after a week of reading through it bit by bit. We enjoyed reading the brief definitions for terms used in management strategy, and realized how many people really need something like this. It helps the reader translate managerial idioms, phrases, and terminology into the underlying concepts.

The importance of these “translations” became clear when a friend opened the book and began looking for terms in a management memo with which he was unfamiliar. The book allowed him to make of the memo. This is a good reference book for the student of management.

7. Free-Subscription/Unsubscription/Copyright Information

•• ÆGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2004 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.

To subscribe to our AvantGo channel, go to 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.

If you know of anyone else who should be receiving ÆGIS e-journal, please send their e-mail address to ejournal@lubrinco.com.

If there is a topic that you would like to know more about, send it to 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. 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 2004 ÆGIS e-journal (© 2004 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.