



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 7 Number 1, January 2004

From the case files of

The LUBRINCO Group

<http://www.lubrinco.com/>

and

Financial Examinations and Evaluations, Inc.

<http://www.feeinc.com/>

Business in Bogotá or other high-threat areas? Call us!

This month's features:

• **Special Announcement**

- 1. Due Diligence — Fraudsters, and your ideal best friend**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Why fraud feasers do not need to use OPSEC to protect themselves from individual victims**
- 3. Executive Protection — How fire drills can save your life, and why you can't do them**
- 4. Technical Issues — Why you soon may be able to get an encrypted cell phone for under \$2,500**
- 5. Real Stories from the Field — Is your anonymous proxy server anonymous?**
- 6. Book and Product Reviews — InfraGard**
- 7. Free-Subscription/Unsubscription/Copyright Information**

**Read *A Field Day for Spies While a Deal Advances* by Richard Isaacs
in the January 2004 issue of *Mergers & Acquisitions, The Dealmaker's Journal***

The LUBRINCO Group was quoted in the January *Robb Report*

Richard Isaacs will be speaking at the 21 January *New York City InfraGard Chapter* meeting

**L. Burke Files will be speaking at the *American Export Business Intelligence Conference*
12 February 2004, Long Beach, California**

<http://www.americanexportbusinessintelligence.com/>

1. Due Diligence — Fraudsters and your ideal best friend

Imagine that you could invent your own best friend. What qualities would you like in them? No doubt they would be bright, interesting, loyal, friendly, helpful to others, a contributor to the welfare of society, and have a host of other virtues to make them desirable as friends.

Now imagine that you were a fraudster. What qualities would you like to project to your potential victims? You would doubtless want to appear to be bright, interesting, loyal, friendly, helpful to others, a contributor to society, and have a host of other virtues to make you desirable as a friend.

It is obvious that bad guys – particularly in the movies – will be obvious bad guys, but it is our considerable experience that a successful fraudster will rarely seem like a bad guy.

Think of it this way. Imagine that you are walking down the street one evening, having had a few beers with your friends, and see someone playing three-card Monte. You decide to amuse your friends by betting five bucks. When you lose, are you surprised? We hope not.

Now imagine that you have to make a decision about investing your life savings, or a substantial amount of money for a charity, or a large sum of money for your company. Are you likely to do it with someone who gives the impression of being a three-card Monte dealer? Not a second time, and probably not even a first time!

Most of us are comfortable in different situations with different kinds of people. And in general, most of us prefer to deal with people we like, independent of the situation. And in fact, most of us make a big effort to try to deal with people we like. Now, obviously, this is going to mean that we deal with people we like during honest dealings, and people we like in dealings where we are being victimized. Only we won't realize we are being victimized until after the fact, and we will rarely admit it when we have been victimized, even to ourselves!

Does this mean that we should stop using liability as a criterion for doing business? No it merely means that the appropriate exercise of due diligence is important even when doing business with people we like.

The key to due diligence is to do due diligence.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Why fraud feasons do not need to use OPSEC to protect themselves from individual victims

Fraud is big business. We don't mean small fraud; we mean **BIG** fraud, where hundreds of millions of dollars disappear.

In most cases it takes a large amount of effort to find out where the money went, because fraudsters go to a lot of effort to hide the money. It is not impossible to find the stolen money, but it takes special experience and skills in some very strange courts and places to effect a recovery in a major international fraud. There is only a small handful of attorneys equipped to deal with big international fraud, and only small handful of international investigative firms, such as LUBRINCO, equipped to locate the hidden assets.

But while criminals take a lot of care to hide their loot, they expend little effort covering up the actual fraud. You might also expect fraudsters to be skilled practitioners of OPSEC, shielding critical information that might reveal that they are crooks. But they really don't. Why not? Because it simply isn't necessary!

We know a man who decided, with the advent of computer dating, there was a need for quick and inexpensive background checks on prospective dates. He soon discovered that while there was a need, there was very little demand. His wife explained that people wanted to meet Prince (or Princess) Charming, and that a background check would spoil the illusion and kill the romance.

The same thing holds true with major fraud, where the process is not all that different from dating. When Martin R. Frankel stole \$350 million dollars (ÆGIS July 1999) from a variety of sophisticated investors, including the Church (Fraudsters, including high yield investment promoters commonly prey upon religious people. They do not seek out people of a specific religion or denomination, just people of faith.), it was not his clever use of OPSEC that prevented investors from seeing obviously disqualifying red flags. It was, rather, the fact that the investors were looking for Prince Charming, even in a high yield investment program.

A simple way to avoid getting burned by high yield investment programs and other participatory frauds is to ask specific questions and look for *specific* answers, not answers that change the question, or answers that slip quickly into vague generalizations. Any time the investment professional tells you that how the yields are generated is a secret, or that the yields are somewhere near astounding, you have been given a clue, even a warning. But if investors, like prospective dating partners, are looking for a particular outcome (in this case inordinately high returns), red flags are invisible, or rationalized away.

While a quick call to us to exercise some appropriate level of due diligence can prevent the embarrassing loss of millions of dollars – sometimes by very sophisticated investors – it will also spoil the illusion and kill the romance. Which is why there is generally no need for fraudsters to make the effort made to hide their fatal flaw.

While a fraudster may not need to practice OPSEC, you do. If you think like your adversary – which requires you to recognize that you might have an adversary – you greatly reduce your likelihood of being victimized.

3. Executive Protection — How fire drills can save your life, and why you can't do them

One of the mistakes frequently made in all areas of selection is to be too specific in the selection criteria. Thus, we often hear computer programmers complaining that someone is looking for a programmer who has already done a specific application, rather than a skilled programmer who can perform a wide array of tasks. Someone once said that they were sure that at some point someone had refused to hire a limo driver because they had only driven blue limos, while the limo that needed to be driven was black!

It is quite common to see people make the same mistake when looking at protective measures. That is to say we will get a call on how to deal with some particular threat *du jour*, i.e. “How do we get someone out of the building in case of a bomb?” when they should really be asking more basic questions, such as “How do we get everyone safely out of the building?”

The fact is, if you are protected from fire and natural disasters, you will be protected from most everything else, too. Fire is a good place to start, because if you can survive a fire, you can survive almost everything. If your building burns down and you can start up elsewhere, you can survive most other disasters, both natural and unnatural. In terms of people, if you can evacuate your building when there is a fire, you can evacuate it in a host of

other situations, too. If your people regularly do full fire drills, they are well on their way to safety. That's the good news.

Now the bad news: Unless you own your own building, you probably can't do a fire drill. For a start, to do the fire drill, you will probably have to go into common areas like stairwells, which are not leased by you. This means that the building owner faces liability for anything that happens to your people, and it is unlikely that they or their insurance company will be willing to run that risk.

And if you make it to the street you are now congregating on city property, which transfers the liability to the local government, which they don't want, and which you probably can't do without a license – a license which, in all probability, the municipality's insurance company won't want issued.

How do you deal with the conflict between bureaucracy and safety, between the liability faced if you practice, and the liability you will face after the fact if you could have been prepared, but weren't?

- Recognize that potential disasters, whether natural disasters or man-made, have common elements which need to be dealt with in order to prevent the potential disaster from becoming an actual disaster. If you are prepared to safely evacuate your office in case of an electrical fire, you are prepared to evacuate in case of an earthquake or an explosion or a criminal act.
- Recognize that solutions to problems, particularly solutions to problems that happen rarely, don't plan themselves. Make sure someone has given thought to a variety of bad things that might happen, and put together plans for dealing with them.
- Recognize that plans won't cover factors that you have not considered, many of which will show up only in testing – or real life – and that it is better to refine a plan through testing than to have it fail needlessly.
- Even the best plan will fail if people haven't practiced implementing the plan. Whatever plans you have developed must be practiced and evaluated on a regular basis, both to take into account any changes in your situation, and to keep skills at an adequate level.
- Support your staff in their efforts to overcome the inertia and bureaucracy that will be unique to your particular building owner, municipality, involved insurance providers, and perhaps even to you.

4. Technical Issues — Why you soon may be able to get an encrypted cell phone for under \$2,500

Encryption of telephone calls is a funny area, because there is a very high need (your unencrypted conversations can do things like compromise attorney client privilege, give your competitor critical information about your company, and expose you as being a dope. The first two will be decided in a court – the third comes as a consequence of the first two), combined with a very low demand.

By this I mean that if you have a sensitive executive – or even non-executive – position in a company of any significant size, there is a good chance that your conversations are from time to time overheard, and that this is costing your company real money. If so, you have a real need to be making calls over an encrypted line.

On the other hand, the likelihood is that, real need or not, you are not using encryption. In fact, even if you work for a major institution, the likelihood is that there is not a single voice encryption device anywhere in the firm.

This is not because encryptors are unavailable, or that they are horribly expensive, or that they are difficult to use. The Privatel™ 960V Personal Telephone Security from L3 Communications (<http://www.apcominc.com/cs-east/programs/infosec/privatel.htm>), which we reviewed in the April 2001 issue of *ÆGIS*, is small, portable, easy to use, effective, and inexpensive. And yet, few people use it or any other encryption device.

The situation with mobile devices is even worse. While the need is as high as, or higher than it is for landline communications, the options are fewer, and the price is higher. In the U.S., there is the General Dynamics Sectéra system (<http://www.gd-decisionssystem.com/sectera/>), but that sells for about \$2,500, and only comes in a 900/1800/1900 MHz GSM version. While this was fine a few years ago, GSM 850 has now been implemented in Antigua & Barbuda, Argentina, Cayman Islands, Colombia, Dominica, Ecuador, Grenada, Montserrat, Panama, Paraguay, St Kitts & Nevis, St Lucia, St Vincent & The Grenadines, and the United States. Since the Sectéra was implemented using the now-discontinued Motorola TimePort, you shouldn't expect to see a quad-band version. Rohde & Schwarz (Munich) modified the Siemens S35i for encryption, but that is a European 900/1800 MHz handset and sells for around \$3,000.

However, for that small group prudently interested in encrypted mobile devices, there is hope on the horizon in the form of voice encryption software being developed for Pocket PC-based terminals. Some will come with the software already installed (€1800), and some will have just the software (\$250), with you supplying the handset. Unfortunately, there is at the moment neither a quad-band version of a Pocket PC device, nor is there an 850/1900 MHz device. However, Siemens, which makes the 900/1800 MHz SX45 and the 1900 MHz SX56, is likely to be bringing out an 850/1900 MHz device in the next year.

This means you could now put the software in 900/1800 MHz device (for everywhere but North America), as well as in a 1900 MHz device (for North America), and when the 850/1900 MHz device becomes available use that instead of the 1900 MHz device.

Before getting too excited, keep in mind that good cryptography is not easy, and there is nothing yet to indicate whether these products will be even commercially useful. By this I mean that in a commercial environment we may not really care if the cryptography is more than marginal, or if the NSA can easily crack it. All we really care about is that can't be easily overheard by those without a court order. Will this be better than the base encryption now available in GSM? Well, for those of us not concerned about being overheard by law enforcement, the bad encryption that comes with GSM may be enough for our needs. Nonetheless, while we have not yet had a chance to see any of these software-driven devices, the concept is interesting, and we look forward to trying them out.

5. Real Stories from the Field — Is your anonymous proxy server anonymous?

We have in the past (ÆGIS November 2002, December 2002, July 2003) discussed use of anonymous proxy servers. Anonymous proxy servers allow you to surf the web under the guise of the proxy server's IP address, rather than your own. Why would you want to do this? One reason might be that you are participating in public forums that display the IP address with which you signed in, and you don't want to give hackers a leg up on finding you. Another is that you may be visiting web sites where you want to obscure your visit. As an example, we often visit websites that are believed to be run by terrorist organizations in order to get a better feel for certain threats, and would prefer, for obvious reasons, to make our presence as little known as possible to all participants. So we use an anonymous proxy server, so that it is the server's IP address that is left, not ours.

Recently, the manufacturer of the software we use for this (*Anonymity 4 Proxy* <http://www.inetprivacy.com/a4proxy/index.htm?a4>) released a beta version, which we installed. Now, we don't wish to appear to be mistrustful, but a beta is, by definition, less reliable than production code, so after re-calculating the anonymity of possible servers, we used *Reveal Your IP* (http://www.computercops.biz/modules.php?name=Reveal_IP) to verify that our IP address showed up as that of the proxy server.

To our surprise, *Reveal Your IP* showed that in the beta software (not the production software) a number of the proxies listed both our proxy IP address and our real IP address. We notified the software manufacturer of the bug – this is the purpose of beta testing – and removed the non-anonymous servers from our list of desired choices.

If you use anonymous proxy servers, and want to re-assure yourself of your anonymity, we suggest that you take the few minutes to verify whether your IP address is really invisible, just to be sure.

6. Book and Product Reviews

InfraGard

<http://www.infragard.net/>

Ever wonder how your company can be working closer with the government to deal with some of the issues that deal with national security? One way is to have your people work with InfraGard. As stated on its website:

InfraGard is an information sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a cooperative undertaking between the U.S. Government (led by the FBI) and an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to increasing the security of United States critical infrastructures.

All InfraGard participants are committed to the proposition that a robust exchange of information about threats to and actual attacks on these critical infrastructures is an important element for successful infrastructure protection efforts.

The goal of InfraGard is to enable the flow of information so that the owners and operators of infrastructure assets can better protect themselves and so that the United States government can better discharge its law enforcement and national security responsibilities.

InfraGard is a tremendous potential resource with chapters in Albany, Albuquerque, Anchorage, Atlanta, Austin, Baltimore, Baton Rouge, Birmingham, Boston, Buffalo, Charlotte, Chattahoochee Valley, Chicago, Cincinnati, Cleveland, Columbia, Columbus, Connecticut, Dallas, Dayton, Delaware, Denver, Des Moines, Detroit, Eastern Carolina, El Paso, Fort Wayne, Harrisburg, Honolulu, Houston, Indianapolis, Jackson, Jacksonville, Jefferson City, Kansas City, Knoxville, Lafayette, Las Vegas, Little Rock, Los Angeles, Louisville, Madison, Memphis, Miami, Milwaukee, Minneapolis, Mobile, Nashville, New Jersey, New Orleans, New York, Norfolk, Northern Nevada, Oklahoma, Omaha, Orlando, Pensacola, Philadelphia, Phoenix, Pittsburgh, Portland, Richmond, Rochester, Sacramento, Salt Lake City, San Antonio, San Diego, San Francisco, San Juan, Savannah, Seattle, Springfield, St. Louis, Tampa, Toledo, Tucson, Vermont, Washington Field Office, West Virginia, and Wilmington.

InfraGard is also a resource that is oddly unknown in many business circles. Besides having good resources online, the presentations at the local chapter meetings are authoritative, informative, and helpful in areas where sharing is often helpful.

At a recent meeting of the New York chapter, there were a number of useful presentations, including presentations on Gramm-Leach-Bliley, Sarbanes-Oxley, a information security presentations by the World Bank, and by Price Waterhouse Coopers, and presentations by the US Attorney's office, and the Secret Service.

It is quite likely that your people are unaware of InfraGard. You can dazzle them by bringing it to their attention. You will also be doing your own organization a favor by encouraging your staff's participation in InfraGard.

7. Free-Subscription/Unsubscription/Copyright Information

•• AEGIS 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 2004* and the *EU Revised Money Laundering Directive of 2004*.
- **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 January 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.