



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 7 Number 10, October 2004

From the case files of

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

and

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

Concealed assets in fraud, theft, and divorce? Call us!

This month's features:

- **Special Announcement**
- 1. **Due Diligence — The Social Security Privacy and Identity Theft Prevention Act of 2004**
- 2. **OPSEC, Economic Espionage, and Competitive Intelligence — Sarbanes-Oxley and OPSEC**
- 3. **Executive Protection — A novel scam against corporations**
- 4. **Technical Issues — SMS delivery**
- 5. **Real Stories from the Field — Shooting the messenger**
- 6. **Book and Product Reviews — The X-TAG™ System**
- 7. **Free-Subscription/Unsubscription/Copyright Information**

**L Burke Files will be speaking at OffshoreAlert's 3rd annual
Due Diligence and Asset Recovery Symposium.
13-15 October 2004, Coral Gables, Florida, USA
<http://www.offshorebusiness.com/DDARS/agenda.asp>**

The LUBRINCO Group was quoted in the October issue of *Worth*

1. Due Diligence — The Social Security Privacy and Identity Theft Prevention Act of 2004

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?

Failing to look at the unintended consequences often leads to increased problems in unanticipated areas, which may far-outweigh any benefits brought by the legislation.

HR 2971 (introduced in the Senate as S 2801), the *Social Security Privacy and Identity Theft Prevention Act of 2004*, which recently passed the Ways and Means committee, is a good case in point. 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*.

On the other hand, imagine you are an abandoned wife who needs to collect child support from a deadbeat dad. Or that your life savings have been stolen in a clever fraud. Or that your wealthy husband has just run off with another woman, and insists that he is broke and has no property to split with you.

If you fall into any of these categories, HR 2971 goes a very long way to guarantee 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 for you. Instead, your attorney will hire a private investigator.

Private investigators do a good job of hidden assets: The LUBRINCO Group, for example, is involved in the search for roughly \$600 million dollars a year, largely in large frauds and high-profile divorces. 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 of that name 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, 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 have us get the information they need.

For those in the middle class or below, concealed assets that might readily have been located will now never be seen, as their location will become unaffordable for the normal person.

For most American citizens, the penalties will far outweigh the risks of identity theft. We encourage you to call or write your senators and congressmen to suggest that sections 107 and 108 be changed to better protect the public. Otherwise, the *Social Security Privacy and Identity Theft Prevention Act of 2004* should be renamed the *Deadbeat-Dad and Fraudster Protection act of 2004*....

2. OPSEC, Economic Espionage, and Competitive Intelligence — Sarbanes-Oxley and OPSEC

As regular readers of this journal are aware, loss of critical information from economic espionage and competitive intelligence are estimated to cost American companies about \$300 billion a year.

In the past, companies that discovered their victimization – many never discovered that they had been ripped-off, attributing losses and even bankruptcies to other causes – tried to hide these incidents. (We ourselves are contractually forbidden to even mention our clients' names). And, in fact, the traditional approach used to be to simply write off these losses as undifferentiated operating expenses, thus making them neatly disappear. This saved a great deal of embarrassment.

And then came Sarbanes-Oxley....

Under Sarbanes-Oxley (SOX) material changes must be reported and discussed, including those resulting from competitive intelligence and economic espionage. This means that those responsible for company

governance – senior managers and their boards of directors – now have the same negligent-action liability that they have had in other areas. And with \$300 billion in losses, and an average cost of \$50 million in manufacturing environments and half a million dollars in non-manufacturing environments, we are talking between 6,000 and 600,000 incidents a year, indicating a high probability of hitherto-unreported victimization.

Most companies don't think of anti-espionage as a business activity. This should not come as a big surprise: Their MBAs are not taught about the problem. Their consulting firms have no expertise in it.

It follows that they also don't think about losses from competitive intelligence and economic espionage as being covered by Sarbanes-Oxley. But, according to the letter of clarification we recently received from the SEC, they are covered by Sarbanes-Oxley!

The second part of the story is, of course, since there is an obligation to report and discuss these losses, there is, therefore, a reasonable expectation that, because of the high dollar volume and the large number of incidents, a firm's governors knew – or should have known – that there was a very real, very addressable, problem. And that shareholders are likely to feel, through counsel, that this problem should have been addressed before the fact, rather than after. Thus, companies now have a set of obligations and liabilities that should lead them to want to prevent these incidents.

Prevention will save the company from direct financial loss, and the company's governors both the embarrassment of public disclosure as well as the potential for resulting shareholder lawsuits. The proven way to reduce exposure is through the implementation of an OPSEC program. Who should take responsibility for this? Because of explicit governance liability under Sarbanes-Oxley, OPSEC needs to be authorized and overseen by a senior executive with detailed knowledge of the company's business functions. It is generally handled through a finance/operations team reporting to the CFO or COO, or to the Corporate Counsel.

Since LUBRINCO is the leading private sector provider of consulting in OPSEC, the identification and protection of critical information, we suggest that if your company does not yet have an OPSEC program, now is the time to call us.

3. Executive Protection — A novel scam against corporations

From time to time we hear of new scams, and like to pass them on. This one came from the FBI.

“Recently an individual contacted a Fortune 500 company via email from South America and notified them of a plot to kidnap the CEO’s family members. The individual provided vague information relating to the CEO and his/her family; however there was enough personal information within the email to cause a great deal of concern. The author of the email stated that several individuals tried to recruit him to participate in the kidnapping. The author stated he fled his home to avoid being involved in the plot and wanted to share the information in hopes of warning the intended victims. The author stated he had documentation, photographs, and videotapes that would validate his story of the kidnapping plot. The author wanted to send these items to the victims or his/her company but was having financial difficulties and could not afford to do so.

At this point, the victim company wired the author of the email a small dollar amount to cover the cost of shipping the evidence of the plot. After the money was transferred the author did not contact the victim or the company again and none of the items of evidence were ever received. The author was never fully identified; however the emails were verified as being sent from South America. It is feared that this individual may be contacting other companies or high profile individuals with similar information of a threat.

It is strongly recommended that any company that experiences similar circumstances contact your local FBI Field Office to report any such criminal activity.”

We concur. When you are at risk, failure to exercise due diligence in your protection, or in the protection of someone under your care – particularly in a potentially criminal matter – is imprudent at best.

4. Technical Issues — Text message delivery

Communications can sometimes be a little iffy, as much in the electronic era as it was in the past. When we send a page or a text message, we may think it has been delivered, and yet we may be wrong. Because of this uncertainty regarding delivery, religious courts have ruled that Muslim men cannot divorce their wives via text message: They must show up and do it in person.

For many people, text messaging from one mobile device to another has become a way of life. This editor, for example, sends many, many, many messages. How do you know that a text message has actually been delivered? Well, in many cases you get a message back telling you that it has been delivered. And therein lies the rub!

In truth, the message does tell you that it has been delivered, and it has been delivered. But delivered where? As an example, if I send a text message from my American T-Mobile handset to another T-Mobile handset, or to a Eurotel Praha handset, it means that the message was actually received at the other handset, and I am in essence getting a confirmation from that handset. But if you send a message to a Sprint handset they will be accepted by Sprint, but not delivered unless they pay for the service.

On the other hand, if I send a message from an AT&T Wireless handset, the delivery message seems to indicate that the message has been received by the SMS system, but not that it has actually been delivered. As best as we can deduce, AT&T Wireless simply didn't bother to implement this particular feature. And if you send to other service providers,

The bottom line is that we tend to make assumptions as to what things mean, and that sometimes these assumptions are wrong. If you depend on communications, keep in mind that, as a good rule of thumb, the only time you can be sure someone got your message is if they send you one back in response. Or if you speak with them, and they tell you that it has arrived.

5. Real Stories from the Field — Shooting the messenger

Bad things happen to the best of us, and often for reasons beyond either control or reason. While we don't like talking about our fortunately-rare failures, the result of a recent divorce case is instructive.

We were told by the client through her attorney of her belief that her husband had substantial overseas interests. The husband claimed that he had received a few million from the sale of his overseas interests, and that his only other tangible assets were his 43 classic cars.

We determined that his financial interests had been located in Slovenia. Our associates in Eastern Europe went to work, and, lo and behold, we discovered that it had apparently slipped the husband's mind that he still owned a business outside of Tomlin. Since he had recently sold a third of the business for \$7 million, we were able to demonstrate that his remaining two-thirds share of the business was worth in the neighborhood of \$14 million. We were pleased with the job we had done. It was done right. It was done in a timely manner. It was done for less than we had estimated.

We presented our findings, complete with all the appropriate documentation, and were promptly fired by the angry wife. The attorney later told us that his client was so enraged at finding out that her husband really *was* lying to her that she fell back on the time-honored approach of shooting the messenger.

6. Book and Product Reviews

The X-TAG™ System

Worldtrac, LLC

<http://www.usatrac.com/> 1-888-443-2443



The X-Tag system is designed to track objects – people or things. It consists of a small transmitter, which can be imbedded or secreted in almost anything – it can even be swallowed – and two flavors of tracking receiver. The short-range tracking receiver is good for up to 350 feet, and the long-range tracking receiver is good for up to 25 miles – 40 if you are airborne.

The ability to hide a small transmitter reduces the chances of it being found, particularly if it is not being looked for, as might be the case with goods or objects that you fear might be hijacked or stolen.

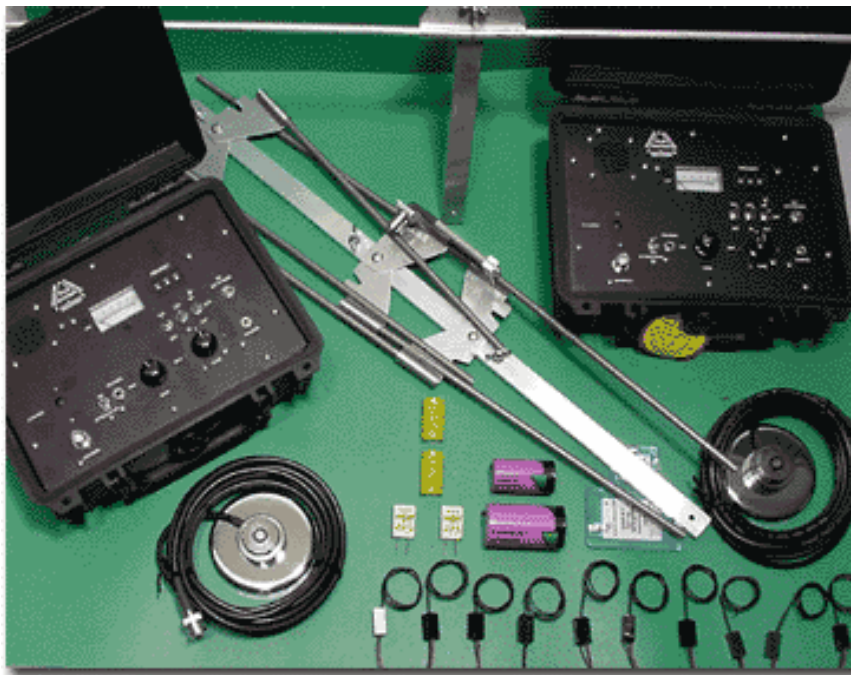
In the case of people being kidnapped, there might well be an expectation of a monitoring device. In this case, it is not unheard of for a victim to be stripped of all clothing and possessions, re-dressed in different clothing, and hustled off into the mists. In this case, no matter how cunningly hidden, the device, once discarded, is no longer helpful. Even if its removal triggers an alarm, if you are unable to close off the area in a very short period of time the best you will be able to do is to recover the discarded device.

In this situation – stripped of clothing and possessions – a transmitter that has been swallowed will prove to be of value. There are, of course, some obvious problems. For a start, the device will stay in your alimentary system a relatively short time, and will have to either be recovered and cleaned, or simply flushed and replaced. And the range will be somewhat less.

What does this mean in real life? Well, imagine that you had someone who was going to be in a risky place – Colombia, Mexico, or Iraq, for example, where there is a real risk of being kidnapped – but they will only be there for a few days. In this case, since the transmitters are under \$300 each, the cost is not prohibitive, especially when compared to the cost of a recovery.

Twenty-five miles may not seem like a lot, but the assumption is that when the short-range receiver indicates that the person or object has moved beyond the 350 foot radius, you will immediately begin tracking and following using the long-range receiver.

This system has enough advantages to be worth considering.



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.

- **OPSEC: The identification and protection of information that would give your competitors and adversaries an advantage.**
 - Sarbanes-Oxley compliance.
 - Protection of trade secrets and intellectual assets.
 - ◆ Anti-competitive intelligence.
 - ◆ Anti-economic espionage.
- **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 October 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.