



ÆGIS journal

Addressing threats that affect your bottom line

Volume 10 Number 6, June 2007

From the case files of

LUBRINCO

<http://www.lubrinco.com/>
1-212-695-1759

and



<http://www.feeinc.com/>
1-480-838-1728

Asset location in fraud, theft, and divorce? Call us!

This month's features:

- **Special Announcement**

1. **Asset Location and Due Diligence — Fostering corruption. Or not.**
2. **OPSEC, Economic Espionage, and Competitive Intelligence — Surprise!**
3. **Executive Protection — Putting yourself in God's hands**
4. **Technical Issues — Translation services**
5. **Real Stories from the Field — A new ACH scheme**
6. **Book and Product Reviews — Surefire U2 Ultra**
7. **Subscription/Unsubscription/Copyright Information**



AEGIS journal, in conjunction with
The Center for the Study of Law, Science, and Technology,
Sandra Day O'Connor College of Law at Arizona State University
and
The OPSEC Professionals Society
will be hosting its two-day **Critical Information and IP Conference:**
Identification, Valuation, and Protection of Critical Information and Intellectual Property
For Directors, Finance Officers, and Counsel
At Arizona State University in Tempe, Arizona, **2-3 October 2007**
For information, contact us at conference@aegisjournal.com

L. Burke Files will be presenting at the AFP Tampa Conference on June 8th, and the 18th Annual ACFE Fraud Conference July 15-20, 2007

1. Asset Location and Due Diligence — Fostering corruption. Or not.

People tend to make use of opportunities presented to them, often with little regard for ethics. In some cases this is done within the constraints of the law (which does not concern us here), and in some cases this is done outside the law (which does concern us here). Since we know that people will take advantage of opportunity, those developing projects have a fiduciary obligation to make sure that the possibilities of fraud and corruption are minimized without damaging the opportunity. This is generally done through the internal audit function.

Auditing can be intrusive and disruptive, particularly when the auditors are demanding records from the past. While forensic auditing is important after the fact, we are largely interested in preventing problems with an internal audit, rather than in picking up the pieces after an incident. Because of this, we believe that it is better to figure out the areas of risk and audit the present

activities in these areas. If, when we show up, the risk is less than we had expected, we are happy to admit we misjudged, and move on. By taking this approach, common to most forms of risk management, we are able to minimize cost, maximize effectiveness, and minimize the opportunity for fraud and corruption on projects,

The problem, however, is often not the approach to auditing, but the sheer failure to provide sufficient on-site concurrent internal auditing and oversight when it is clear that it is needed. As an example, in the March 2005 issue of AEGIS we discussed the fact that both the UN Food for Oil program and the US Iraq Development Fund failed to provide adequate on-site audits, when it was clear that this would lead to corruption and fraud, as this kind of failure always does. The UN auditors with whom we have spoken believe that they could have predicted, based on the lack of supervision, how much would be lost to corruption, and that their GAO counterparts could have done the same for the losses in the Iraq Development Fund.

The bottom line is that risk management allows you to manage risk. If you *choose* not to implement risk management, you are, by default and abrogation of your responsibilities, *choosing* to allow risk to manage you. Internal audit of high-risk areas of exposure is a key tool. Use it, and use it wisely.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Surprise!

We were trying to explain the concept of OPSEC to someone foreign to most of the professional worlds in which we live. We finally came up with a comprehensible analogy in the surprise birthday party.

- The management objective we need to protect is the party itself, which you can think of as the civilian equivalent of bombing a fortification or releasing a new product.
- The adversary is the person for whom the party is being held: The child, spouse, parent, friend, or other.
- The threat is the natural curiosity or observance of the celebrant.
- The vulnerability is that the birthday celebrant will either put together what is happening from what they see and here (why are all those caterers calling?), or that some blabby friend will tell them.

Since we know the adversary and their capabilities, we can now work on the vulnerabilities, getting friends to promise not to talk about the party when they might be overheard, putting the cake in someone else's house, avoiding

e-mail from a shared account, and doing all the other things that we need to do in order to successfully pull off a surprise birthday party.

Three things to be aware of are:

1. You are doing the same things you would need to do if you were protecting critical information in a commercial or military (rather than home) environment.
2. There is no huge cost required to protect the secrecy of the party, which is also generally the case in a commercial or military (rather than home) environment.
3. In spite of your best efforts, your cunning adversary may still figure out what is going on.

3. Executive Protection — Putting yourself in God's hands

During hurricane Katrina, a police car was dispatched in New Orleans to pick up a minister and take him to safety. The minister said thank you, but that he put himself in God's hands, and would stay.

When the levee breaks, a boat is dispatched to pick up the minister and take him to safety. The minister said thank you, but that he put himself in God's hands, and would stay.

Soon the water rises, and the minister is forced to the roof. A helicopter is dispatched to pick up the minister and take him to safety. The minister says thank you, but that he put himself in God's hands, and would stay.

Eventually the water rises and the minister drowns. When he gets to Heaven he asks, "God, I put myself in Your hands and You let me drown. Why?" And God says, "I sent a car. I sent a boat. I sent a helicopter. What more could I do?"

We were reminded of this story recently when taking a taxi into Gotham from JFK, and someone mentioned that they thought New York City taxis were expensive. This is, of course, a matter of perspective. For comparison, you might look at the cost of a ride from the Baghdad airport to the Green Zone: \$5,000.00 USD. While this may seem high compared to getting into Manhattan, it is, in fact, not unreasonable when you consider that it will most likely get you where you want to go, alive and un-kidnapped.

One group that finds the cost of Iraqi taxis to be too high is missionaries, who often simply drive across the border from a neighboring country. When

they do this, they don't bother with high-priced security escorts, since they are doing God's work, have put themselves in God's hands, and therefore do not need to take security measures.

While we certainly admire their faith, it is important, when facing danger, to try to reduce the likelihood of getting killed. This is why even the most faithful should wear seat belts, not smoke, and practice safe sex. Similarly, when thinking about high-threat security for transferable targets (if you can't get one foreigner, any other will do), it is important to realize that our goal is to make those we wish to protect sufficiently costly to go after that it makes more sense for the bad guys to go after someone else. We are not trying to remove the threat: We just want it directed at someone else. Missionaries (and, for that matter, journalists and NGOs) do not adopt this philosophy, which makes them that someone else.

The result of this is fairly clear. The US Embassy Hostage Working Group (HWG) in Baghdad maintained an extensive database over a two-year period tracking every reported foreign kidnapping. From April 2004 to April 2006, 448 individuals were reported taken hostage. Metrics included the incident date, location and what the victims were doing in Iraq at the time of their abduction. Interestingly (yet not surprisingly), 82% of all kidnapping incidents occurred during vehicle movement between secure compounds or during daily commutes from residence to work. This follows the pattern normally seen in kidnappings throughout the world.

The analysis below depicts the percentage breakdown of what occupation was most targeted by criminal gangs and insurgent groups for kidnap and ransom (K&R) or kidnap and kill (K&K).

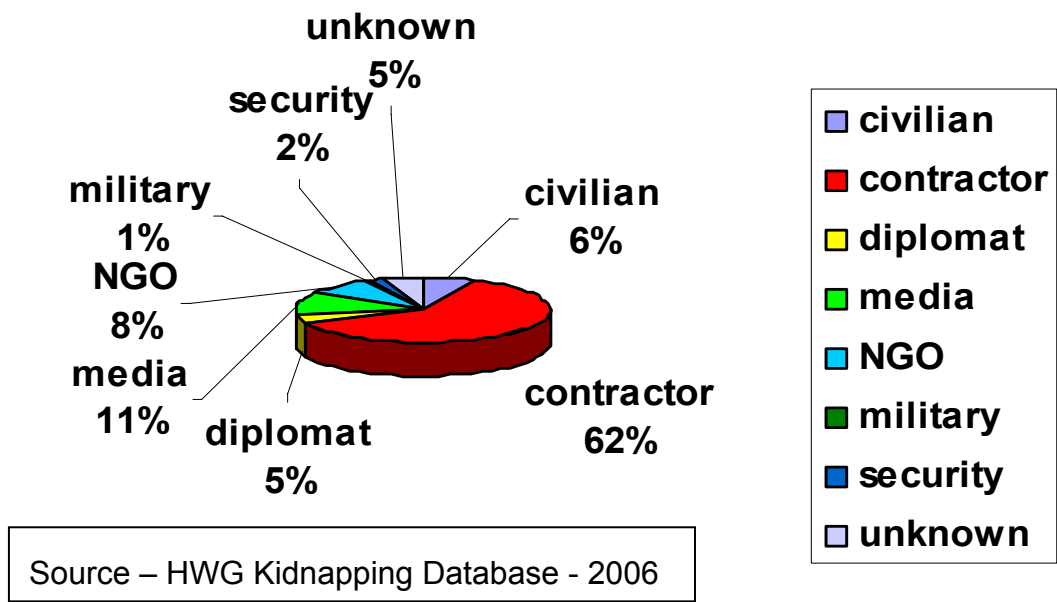
Of particular note, however, is who *wasn't* taken. Military (denoted more than 150,000 soldiers, sailors, airmen, and Marines from the Multi-National Coalition Forces) and Security (represented more than 25,000 private military company staff who served as bodyguards or with convoy security details) were the least taken, which may seem surprising considering that they presented the most numerous and desired target by the insurgency. In two years of a full-blown insurgency, with daily attacks on Coalition soldiers and convoys, only one American soldier and ten private security "guns for hire" were reported taken hostage. The obvious question is why not more? And the answer even more simple: They were hard targets. These individuals understood that Iraq represented "Indian country" and conducted daily trips into the "Red Zone" driving armored vehicles, wearing body

armor, carried with fully loaded weapons, and rehearsed worst-case scenarios in the event of an attack.

On the opposite spectrum were many of the journalists and NGO (Non Government Organizations) aid workers who frequently drove around Baghdad and Iraq with no acknowledgement of the dangerous environment beyond, of course, their abiding faith in their missionary zeal or the noble cause about which they were writing. Ironically, most kidnapped journalists and NGO victims believed that supporting the cause of the insurgency against the “evils” of the American occupation would protect them from the scourge of kidnapping that affected every walk of life in Iraq. At best, most of them placed their lives in the hands of an Iraqi translator and driver they paid a paltry \$20 a day to drive them around in a local car. In many cases, it was later discovered that the “trusted” driver delivered the oblivious victim to the doorstep of one the numerous kidnapping elements operating in Iraq. Subsequent investigations would reveal that in many instances, the driver would receive a delivery fee greatly exceeding any monthly salary offered by his Western employer. Journalists and aid workers, whose numbers never rose above 1,000 in total, constituted nearly 20% of all kidnap victims.

In between these two extremes was the number one *practical* target: The contractors rebuilding Iraq, and principally truck-drivers, delivering supplies to military bases spread all over the country. There are a lot of them, so the number kidnapped is not disproportionate to their presence.

Iraqi Kidnap Victims by Profession



There is an old Arab saying; “It is foolish to hunt a tiger when there are plenty of sheep to be had.” This philosophy was exploited to the fullest by the kidnapping gangs operating in Iraq. The days of the Old Testament in Babylon (in modern day Iraq), when Daniel survived a night in the lion’s den on prayer alone, are over. People who do not take the steps to mitigate the threat will pay the consequences of their action. Thus, while putting yourself in God’s hands may be good for your immortal soul, when thinking of your mortal body it is a good idea to remember that God put high-threat protective specialists here to protect your corporeal being in areas of danger.

Special thanks to Dan O’Shea (<http://www.danielrisk.com/>), former Coordinator of the Hostage Working Group (HWG) in Iraq, for providing the hard data for this article. We strongly urge everyone interested in this area to look at his Web site.

4. Technical Issues — Translation

Recently, one of our clients asked us to translate a legal document from Spanish to English. The document was the articles of incorporation of a Mexican company. The client was performing their due diligence on the company and their authority to operate in Mexico. The document was the key foundation document for this company, and laid forth who was able to bind the company and who was not.

Translation of any sort is difficult, and, independent of what is being translated, it is prudent to keep in mind Rossetti’s dictum regarding translation of poetry that “The life-blood of rhythmical translation is this commandment that a good poem shall not be turned into a bad one. The only true motive for putting poetry into fresh language must be to endow a fresh nation as far as possible with one more possession of beauty. Poetry not being an exact science, literalness of rendering is altogether secondary to this chief law. I say literalness, not fidelity, which is not the same thing.” Several translators started, but failed early into the project, because legal translation was not their strong point. We finally found a service – L2 Language Services (<http://www.L2Languages.com/>) – that was equipped to do the job.

The exercise was worthwhile in that it confirmed to our client what had been represented to date, which is comforting when performing due diligence. Comforting to the Mexican counterpart was the knowledge and the questions asked by our client about the Mexican process of incorporation and the language used in the corporation document. This impressed the Mexican counterpart a great deal. According to the Mexican businessman, few have gone to the bother to make an accurate translation of documents, let alone make further inquiries in the vagaries of Mexican civil code.

5. Real Stories from the Field — A new ACH scheme

We have frequently used a variety of languages (ancient Hebrew, Arabic, German, French, Latin, Spanish, and Urdu, to pick a few off we recall), with some confidence that our readers will understand. But when it comes to understanding the arcania of electronic payments we want to be really sure you understand, so we have included a glossary in front of the article. Electronic payments are replacing check and drafts. As wise and informed people, we need to know the language of this electronic payment frontier. Willy Sutton used to rob banks “because that’s where the money is.” Fraudsters are going to work on the ACH system because that where the money now is.

Glossary for Article

The Automated Clearing House (**ACH**) Network is a highly reliable and efficient nationwide batch-oriented electronic funds transfer system governed by the **NACHA**.

NACHA is a not-for-profit association that represents more than 11,000 financial institutions through direct memberships and a network of regional payments associations, and 650 organizations through its industry councils. **NACHA** develops operating rules and business practices for the Automated Clearing House (**ACH**) Network and for electronic payments in the areas of Internet commerce, electronic bill and invoice presentment and payment (**EBPP**, **EIPP**), e-checks, financial electronic data interchange (**EDI**), international payments, and electronic benefits services (**EBS**).

Prearranged Payments or Deposits (**PPD**), used in an **ACH** header record to indicate the **ACH** format being used and to identify...

Once authorization is acquired, the Originator then creates an **ACH** entry to be given to an Originating Depository Financial Institution (**ODFI**), which can be any financial institution that does **ACH** origination. This **ACH** entry is then sent to an **ACH** Operator (usually the Fed) and is passed on to the Receiving Depository Financial Institution (**RDFI**), where the Receiver's account is issued either a credit or debit, depending on the **ACH** transaction.

R7 and **R10** transactions are where the customer goes to their bank and disputes or revokes debit to their account. These have always been heavily scrutinized and subject to a 2.5% threshold. A higher percentage typically results in suspension of their **ACH** processing rights.

Written Statement Under Penalty of Perjury (**WSUPP**) to the **ODFI** is what is used to dispute **ACH** transaction usually under **R7** or **R10**.

And now, the article...

Last year we saw another **ACH** scam, where the **NACHA** rules worked against a financial institution.

An individual opened a mutual fund account and signed the **ACH** authorization form. He then phoned to make a \$65,000 purchase into the fund, paid with a **PPD** debit originated to his bank account. A couple days later he phoned and made a \$70,000 purchase, again funded by a **PPD** debit. Then about a month later he phoned to redeem the money, which he did with a **PPD** credit. All phone calls were recorded and available, as is mandatory in these financial institutions.

About 55 days after the first debit, he went to his bank (the **RDFI**, in this case) and claimed the two debits were unauthorized. The **RDFI**, of course, credited him with \$135,000 (again!) and sent an **R10** to the mutual fund.

The day after receiving the **R10** the fund knew it was a fraud, but there is nothing the firm could do to protect themselves under the **NACHA** Rules (the money was, of course, already gone from the bank.). A **WSUPP** was requested, and a copy appeared two days before the required delivery deadline - and it was as accurate as most **WSUPPs** we have seen.

A little research would have shown he had received the \$135,000 already into his account, but under the Rules the **RDFI** has no reason – more to the point no incentive – to question the consumer. But since the **RDFI** can push all liability onto the **ACH** Originator, why should they make the effort?

This exposure of all **ACH** Originators to the “60 day right of refusal” has been around for as long as the **ACH**, and has been a hurdle for some fund and brokerage firms to use **ACH**. **NACHA** steadfastly has refused to even try to find equity or balance in the legal exposure of **ACH** Originators.

Interestingly, the definition for an **R10** in the **NACHA** Rules (and in Reg. E) says: “An unauthorized debit entry does not include a debit entry initiated with fraudulent intent by the Receiver.” Even though that was clearly the case in our instance, where do you go with that?

Obviously there is legal recourse against the individual involved, but it is a long and very hard road to pursue.

This is one more case that points to the importance of **KYC** (Know Your Customer). If you're going to allow customers to originate these types of transactions, as more and more brokers seem to be doing, you need to make sure you protect yourself by underwriting the customer, since you've actually created a potential creditor relationship. If you're unwilling to extend this type of credit, then you shouldn't be allowing him to originate the transactions involved. Or, at least should be providing some form of reserve and/or credit protection for yourself.

6. Book and Product Reviews

Surefire U2 Ultra

Surefire \$279.00

http://www.surefire.com/maxexp/main/co_disp/displ/prrfnbr/24187/sesent/001-714-545-9444

In terms of frequency of use, we find that a good flashlight is among the most useful tools to have at hand. As with all such tools, we are always seeking to find the most appropriate choice of tool. And, as always happens we need to make tradeoffs among size, power, and duration.

The balance of these three factors depends on many factors, which vary depending on the ultimate use. In this particular case, we were looking for a flashlight to carry in our pocket. We have sometimes carried the Surefire E2E, which at 4.5 inches with a bezel width of one inch is a good size, and puts out 60 lumens for 75 minutes. At other times we have carried the Surefire 9P, which at 6.5 inches with a bezel width of 1.25 inches still fits in a pocket, and, depending on bulb choice, puts out either 105 lumens for 60 minutes (with a high-output bulb it puts out 200 lumens for 20 minutes, which makes it something of a specialty choice). Both of these flashlights use incandescent lamps, and require the prudent user to carry a spare bulb.



We have currently opted for an excellent compromise unit, choosing the Surefire U2 Ultra. This device uses a 5 watt LED, and, at 6.13 inches and a bezel width of 1.47 inches is about halfway between the other two in length, albeit wider. It is adjustable to six output levels, ranging from 2 lumens for 40 hours to 100 lumens which we estimate will last for over an hour.

We had originally feared that the 2 lumen setting – two of anything doesn't sound like enough – would be too low for practical use. We were wrong: It is a fine setting for most work done indoors in a normal size room in the dark, or for looking in cabinets. 100 lumens, as we already knew from the 9P, is a lot of light, and enough for most uses outside, including dazzling an attacker. Because it uses an LED, it is sturdier than an incandescent bulb, and no extra bulb is either necessary or available.

We feel confident that we have made a good choice, and do not hesitate to recommend this for your consideration.

7. Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2007 by The **LUBRINCO** Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com), L. Burke Files (LBFiles@feeinc.com), and Terry Phillips (TPhillips@aegisjournal.com).

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

- **Identification, valuation, and protection of intellectual assets and critical information.**
 1. American businesses lose \$300 billion annually to competitive intelligence, economic espionage, and information theft.
 2. Sarbanes-Oxley requires internal controls tracking the costs, and impact on valuation, of competitive intelligence, economic espionage, theft, and deliberate disclosure.
 - LUBRINCO is the leading private sector provider of access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information from competitive intelligence, economic espionage, theft, and deliberate disclosure.
- **International asset location and due diligence.**
 - Location of concealed assets in fraud, theft, and divorce.
 - Due diligence to prevent fraud and loss in China, Central and Eastern Europe, Central Asia, the offshore financial centers, Latin America, and the Caribbean.

- Financial fraud, anti-money laundering, and anti-corruption program development and training.
- **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 **LUBRINCO** and its services, or for the archive of all past issues of **ÆGIS** in PDF format, please go to <http://www.aegisjournal.com/>.

Subscription to **ÆGIS** is available for \$15 per year in North America and \$20 per year outside of North America.

To sign up for a **complimentary subscription** to **ÆGIS** or the **ÆGIS** PDF notification list, go to <http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to subscribe@aegisjournal.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 unsubscribe@aegisjournal.com.

If you know of anyone else who should be receiving **ÆGIS**, please send their e-mail address to subscribe@aegisjournal.com.

If there is a topic that you would like to know more about, send it to editor@aegisjournal.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**, send it as an attachment to an e-mail to editor@aegisjournal.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** constitutes a license to **LUBRINCO**, 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**, you may do so freely as long as appropriate source, copyright, accreditation, and link to the **ÆGIS** Web site is included. This should be in the form

Article Title, from the June 2007 **ÆGIS** (© 2007 **LUBRINCO** & FEEINC), to be found at <http://www.aegisjournal.com/>.

ÆGIS 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** 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**.

Please be safe, and be smart.