



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 5 Number 8, August 2002

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 notice**

1. **Due Diligence — Why we sometimes recommend against insurance**
2. **OPSEC, Economic Espionage, and Competitive Intelligence — Who is that masked invoice?**
3. **Executive Protection — and whom do you know?**
4. **Technical Issues — Keeping the *Deus* out of the *Machina***
5. **Real Stories from the Field — Tipsy hotel guests, forceful security**
6. **Book and Product Reviews — Sprint PCS Wireless Web Modem**
7. **Free-Subscription/Unsubscription/Copyright Information**

L. Burke Files, President of FE&E and Vice President of The LUBRINCO Group, will be speaking at the 12th Annual Anti-Money Laundering Audit & Compliance Forum, to be held in New York City September 18-20, 2002.

1. Due Diligence — Why we sometimes recommend against insurance

One of the services we perform is the occasional transport of people with things that are compact and valuable. By valuable we mean anywhere from fifty million dollars through three hundred million dollars. When moving items of this value – and usually the principals accompanying the items – we often recommend against getting insurance. Now, at first blush it seems that not insuring something of this value is an obvious failure to exercise due diligence. As it turns out, this is not necessarily the case.

In moving items of this value several things are critical. First, it is ideally done with great security: We need to be able to withstand any attack that might be made. Second, it is even more ideally done with great *secrecy*: We don't want the bad guys to know about it, thus preventing them from being able to even consider attacking us in the first place.

If we insure these items, the insurance can be very expensive. This is largely because they are such tempting targets that the risk is, by definition, very high. The cost, however, is not a factor, as it pales in comparison to the value of the items. More to the point, the insurance companies tend to be very picky about the transport, and, like journalists, not unreasonably tend to want a good deal of information about the who, what, where, when, why, and how. Unfortunately, the information they need is exactly the information the bad guys need to rob us. Now, imagine you work for an insurance company, and someone offers you several years' pay for a little information. Might you be the teeniest bit tempted? After all, it is a lot of money, and it is insured....

Does this mean we think that insurance companies willingly give this kind of information away? Or that we think employees of insurance companies are particularly bribable? Not in the least. It merely means that there are many places where someone will take a life for five dollars, and that for a hundred million dollars some people will put a lot of time, effort, and money (including bribing and threatening to get information) into trying to take away your property. And probably your life in the process.

Because of this it is often a greater guarantor of security to take the money that would have been spent on insurance and use it to buy greater secrecy and security, thus increasing the likelihood of success.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Who is that masked invoice?

The work that we do is generally very confidential. Indeed, we are so concerned with confidentiality that none of our offices have listed phone numbers or listings in the building directories (a policy which I must confess we are currently re-considering), and our phones are answered simply with a cheery “hello!” Sometimes this confidentiality extends to invoices.

Traditionally, invoices spell out what was done, and, in many cases, it spells this out in great detail. As it turns out, however, there are certain cases in which this is not a prudent approach. This is because the invoice is not processed by the people for whom we do the work, and, in many cases, the people processing the invoices really shouldn't know, for example, the name of the company or individual on whom we did an investigation. While the good folks in accounts payable have to pay the bill, if they knew even the gross details of what was done, they would have information they didn't need to know, and which, if it were discussed, might have unfortunate consequences.

Another example is one in which we move valuable commodities from one place to another. If we move, say something worth \$100,000,000 from one place to another, a *lot* of money is likely to go into pre-paid expenses, so we need a bunch of money up front. If the people processing the invoices have too much information, the operation – dangerous under the best of circumstances – becomes even more dangerous. As with insurance, as discussed above, we really don't want a paper trail that can be bought and sold, or elicited.

Now, you may think that it is unlikely that anyone would be looking for this kind of information, or that anyone in your accounting office would either sell information or discuss it. And that may be true, but if \$100,000,000, the lives of a dozen people, and a very fancy plane are at stake, or if a deal worth hundreds of millions might be jeopardized, it is not worth the risk. And, unfortunately, if dealing with a person trained in elicitation, the likelihood of anyone not volunteering the information lies in the slim-to-none category, particularly if the sensitivity of the information has not been identified.

3. Executive Protection — and whom do you know?

Since a good portion of our work is high-risk protective services, we work with a lot of protective specialists. These people often guard assets worth tens of millions of dollars, and business, political and, entertainment people subject to real (albeit not generally life-threatening) and multiple threats.

So, how do you know you have the wrong executive protection person when you interview them? An example came to mind when we were recently part of a group that was interviewing executive protection professionals that were to be hired in a private company to protect an entertainment attorney who often threw lavish parties with many luminaries attending.

The first thing the executive protection person did was tell me about the most recent detail where he got to rub shoulders and talk and meet with Jennifer Lopez, Burt Reynolds, Clint Eastwood and Brittany Spears. He went on at length about what a wonderful time he had had with all of them. After the interview the two other people said, “He seemed like a very convivial and interesting security protection specialist.”

I said, “Well, you know what, I would put him at the bottom of my list and will never hire him!”

They asked why?

“What is an executive protection specialist doing socializing with the people he is there to protect? This person was more awestruck and star struck than most any EP person I have ever met.”

The point of executive protection is not to interact with the guests and the hosts. The point of executive protection is to separate the guests and the hosts from any threat real or imagined, from anything that may be a nuisance to the host or the guests, and from anything that might cause real harm to the host or the guests.

4. Technical Issues — Keeping the *Deus* out of the *Machina*

There is a tendency in today’s world to substitute technology for common sense, and assume that technology with which we are not familiar is better – or more reliable – than technology with which we are familiar. This can lead to potential difficulty.

A case in point: A man had been jailed for rape. While he was still incarcerated, there was a second rape in the same neighborhood, and the DNA of the semen on the second victim matched the semen of the jailed rapist. When I say matched, I don’t mean it was a *close* match: It was a *perfect* match! As you might imagine, this threw everyone into a tizzy until one of the brighter bulbs in the investigative chandelier realized that it was easier to smuggle out a semen sample and fake a rape than to find two sets of perfectly matching DNA.

In a second case, reported by both *Cryptogram* and *Informed Sources*, Tsutomu Matsumoto, a Japanese cryptographer, used gelatin to make a finger. He was able to lift a fingerprint using one of the superglues, copied it using a video camera, cleaned the image up with Photoshop, and made a transparency, from which he etched a copper plate, which he used to put the fingerprint on the fake finger. He was reportedly able to fool eleven commercially available fingerprint readers about 80% of the time.

We have spoken with people who wanted to go from magnetic stripe devices to smart card devices, primarily because they had stripe readers and writers, and knew their limitations, but didn't have smart card writers (and didn't really understand the technology), and so assumed they were "better." In fact, smart cards can store a lot of data, and can do many things very well, but no device is perfect.

On a silly note, some of our readers apparently use home e-mail addresses shared with their children, and have services which screen email to make sure that anything which arrives is fit for young eyes. We understand and sympathize with this parental concern. To our amusement, however, the well-intentioned content screener at *yycweb.com* bounced an issue of the *e-Journal* because it had an article dealing with airline security, and included the word "cockpit!"

When looking at better technology, it is very important that before becoming too enthusiastic you determine what you mean by better, and, also, that you determine how this better security measure can be circumvented or fail.

5. Real Stories from the Field — Tipsy hotel guests, forceful security

A female advertising executive by the name of Anna and her boyfriend, Aaron, were entertaining a client and Anna's sister Beth at a Dallas resort. They had been drinking from 3:00 to 7:00, at which point they decided to go from the bar area to the restaurant. As they visibly stumbled out of the bar, the client saw a large, wooden banister and thought it would be wonderful to slide down the banister. He sat on the banister, and down the banister he went, thoroughly enjoying his great two-story slide down the banister.

Anna, too, thought this was absolutely marvelous, so, in her very, very short linen and silk skirt, she sat on the banister and started down the banister at a great rate of speed. About halfway down she flew off the banister. Unfortunately, she went off the banister not towards the steps, but into abyss on the other side. She fell 10 or 15 feet and landed in a decorative area populated by some clay pots. Aaron, Beth, and the client quickly ran down

and pulled her out. She was terribly embarrassed, and fortunately, other than a deep gash in the leg and a very fat lip, she seemed to be OK.

They quickly left the crime scene and went to Aaron and Anna's room. Aaron went to fetch some ice cubes, arriving back just as the phone rang: It was security, and they wanted to know what had happened, why there was damage, and how it had been caused. Aaron told them to mind their own business. He hung up the phone and prepared an ice pack for Anna's face, opining that he thought there were probably going to be some problems, at about which time the security guards came pounding on the door demanding to see Anna. Anna excused herself and said it would be some time before she could come to the door because she was in the bathroom. The security guard said, "Well that's fine: We just wanted to make sure she was OK." She assured them that she was indeed OK. As Anna recalled, there was a quiet discussion among the security guards out in the hallway, and then the security guards said, "Well, we still want to come in and talk to you." At this point in time Anna and Aaron realized that there was a real problem.

The problem was that they wanted no report to be filed, and no mention of this event to occur, either to Anna's employer or to her husband. You see, Aaron was the boyfriend, not her husband, and any report could get back to her husband. At this point in time Anna and Aaron made the decision to escape.

Aaron opened the door and walked out, closing the door behind him. He told the security guards "Gentlemen, if you will please excuse me, I must go look for her earring."

He wandered out to the parking lot, gave the valet \$50.00 and said, "Get me my car, quick!" Meanwhile, back in their room, Anna had packed everything up into their overnight bags, thrown them out the second story window of the hotel, had slipped out onto the balcony, and had begun shimmying down the downspout. Just as she was almost down – literally within two feet of the ground – the downspout tore loose, taking a spectacular 30 foot section of downspout, along with a piece of gutter, crashing down into a common area. Thinking quickly, Anna decided it would be a good time to grab her bags and scoot to see if she could find Aaron. Just then Aaron drove around the corner, picked up Anna up and the two fugitives were off."

Anna called back to the hotel and asked for Beth's room. As Beth picked up the phone and said hello, a voice cut in and said, "This is security, is this Anna?" She hung up. The next day at work, nursing two stitches in her leg and quite a fat lip, she received a call from a police officer with the Grapevine police (this being the jurisdiction where the resort was located).

The police had taken a formal report from the hotel for criminal damage that was done to the hotel. What she feared could happen had happened. Thinking more quickly, being quite sober, Anna very said, "I think you need to speak to my attorney."

Anna and Aaron themselves then spoke to an attorney, who called the police officer and said, "If you wish to take a report, that is just fine. In the meantime we'll use any damages that they claim as part of an offset against the suit against the hotel." The hotel had knowingly served Anna and Aaron and Beth and the client way too much alcohol. It was estimated that Anna herself had consumed six large glasses of scotch on the rocks, in addition to a beer slightly earlier than that. No food was served. The case was very clearly negligence on the part of the hotel for serving too much liquor. To this he added the attractive nuisance of a banister, plus failure to take safety precautions in case someone were to slide off the banister, plus the breach of privacy for cutting into the phone call between Anna and her sister, Beth.

Sum total, the damages the hotel and the hotel insurance carrier had to pay were in the neighborhood of \$395,000, settled out of court. This included a \$3,000.00 offset for damages done to the hotel, of which \$2,400.00 of the damages had to do with the reattaching the downspout that had been spread across the common area.

We asked Anna and Aaron why they sued the hotel after they left the hotel. They said that it was pretty simple: They had no choice.

While Anna and Aaron were aware that the hotel might have some theoretical liability for the incidents surrounding the banister and the drywall, all they wanted was to preserve their privacy. They said that all of this could have been handled quite easily: The hotel should have sent a concierge or assistant manager to inquire if there was anything he could do to help, and to inquire about what to do regarding the damage caused to the plants in the little area where Anna fell. Anna said that they would have more than happily paid right on the spot out of their pocket.

Instead, the strong-arm security tactics of a group of big, muscle-bound, shaved-head security guys literally pounding on the door and shaking the wall forced them (admittedly using logic springing from drink) into a defensive posture, and from the defensive posture into flight. Hence, by the time what they tried to avoid had occurred, they had obtained counsel and gone on the offensive.

Was the hotel entirely in the wrong? Clearly not. Should they have handled the incident differently? Clearly yes.

6. Book and Product Reviews

Sprint PCS Wireless Web Modem (Aircard 510) (Type II PCMCIA Card)

Sprint PCS

http://www1.sprintpcs.com/explore/PhonesAccessories/PhoneDetails.jsp?selectSkuId=510pcs&PhoneName=showcaseB&Link=Link1&FOLDER%3C%3Efolder_id=2421&CURRENT_USER%3C%3EATR_SCID=ECOMM&CURRENT_USER%3C%3EATR_PCode=None&CURRENT_USER%3C%3EATR_cartState=group&bmUID=1026591880700
\$249.99

Service costs: You can either share minutes with your Sprint PCS minutes, or get a standard plan for use with the card alone.

Sprint is a leading provider of CDMA service in the US. Although Sprint will be coming out with a third generation product this summer, we thought it would provide a good basis of comparison if we reviewed their soon-to-be-old offering first. The card itself is a standard PCMCIA card, with a nice touch being that the antenna retracts into the card, which means the laptop can be packed without removing the card (or tucked in when kids are playing with the computer).

Installation is easy if you are running Windows 98. You put in the CD and follow the directions. We were running Windows 2000, and the installation worked, but wasn't quite right, so we downloaded more-current software from the Internet, which worked just fine.

Because this card uses Sprint's voice system, it connected at their base rate of 14.4 Kbps, which is fine for email and for Instant Messaging. They also use the BlueKite compression software, which nominally makes your browser simulate functioning at 56K. When we first loaded the software and started using the device, the BlueKite server was being upgraded, and we noticed a definite increase in speed once it was fully functional again. We were not, however, able to quantify this, nor would we like to do a lot of web surfing at such a low speed. In two weeks of use, we were dropped twice, both times in a building in which there was virtually no signal.

Using the card for sending email required, with our ISP, changing from SMTP to ASMTTP with authentication. This merely meant we went into the email program and changed the name of the ISP's SMTP server to that of their ASMTTP server, and checked the authentication box. Since this works equally well when connected via landline, you don't need to re-set it as you change from modem to modem. We were able to download and use large

files (such as the Norton AntiVirus virus definition updates) with no corruption problems. We were also able to email out fairly large Acrobat files with no problem.

Bottom line, if you need to use your laptop for reading email while away from a landline connection, this device provides a reasonable, cost-effective solution in areas where Sprint has coverage. If you need to be doing a lot of web browsing while en route, you may be better off waiting to look at their 3G offering when it is unveiled.

7. Free-Subscription/Unsubscription/Copyright Information

•• AEGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2002 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 2002* and the *EU Revised Money Laundering Directive of 2002*.
- **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 2002 ÆGIS e-journal (© 2002 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.