



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 7 Number 7, July 2004

From the case files of

The LUBRINCO Group

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

and

Financial Examinations and Evaluations, Inc.

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

Due diligence outside North America and Western Europe? Call us!

This month's features:

- 1. Due Diligence — Background checks of the unseen**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Information protection as a tool for social status**
- 3. Executive Protection — Ready when you are, C.B....**
- 4. Technical Issues — Explosives as a tool of cyber-disruption**
- 5. Real Stories from the Field — False alarms as a tool of the bad-guy**
- 6. Book and Product Reviews — Travel Sentry[™] Certified Locks
Zone Alarm 5 **warning****
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Background checks of the unseen

No matter what your political or philosophical or emotional view of the war in Iraq, in the zero-sum game of government financing, \$200 billion spent in Iraq is \$200 billion not available to be spent on the search for Bin Laden, Al Quaida, and other terrorist threats not related to Iraq.

How does this apply to our day-to-day life? Well, let's forget international actions and look simply at the United States. Some time ago we saw an hour-long news show on the smuggling of people into the U.S. by Mexican coyotes (the smuggler coyotes, not the animals). According to those coyotes interviewed, they had largely stopped smuggling Mexicans, and, instead, were smuggling Middle Eastern men, who paid better. The estimate was that they were smuggling roughly 500 men a month.

Astonishingly, the show also interviewed some of those who were being smuggled. Our recollection is that they largely said that their task was to get invisible jobs, and remain out of sight until contacted and given instructions.

So, figure that about 5000 men from the Mideast come across the border a year, and have been doing so for the past few years. This means a lot of potential troublemakers invisibly spread throughout the country. Since many Americans have significant sympathy for the plight of the Mideast (keep in mind the poll taken after 9/11 that said one out of every 20 Americans thought the attacks were completely justified), this creates a potential national security issue of significance.

What can you do? Well, for a start, be aware that under the best of circumstances it is prudent to do a background check on anyone you hire. As it happens, companies tend to be very bad about checking the background of senior-level people. And they are not too good about checking the background of middle-level people. And they are even worse at checking the background of low-level people. All of this is a bad combination.

This means that you can do a great deal to stop crime and violence by taking the time and effort to do at least minimal background checks on anyone with whom you deal. By finding people who have criminal backgrounds, or whose backgrounds simply don't hold up to even minor scrutiny, you will not only reduce your negligent-action liability, but you will also go a long way toward contributing to a safer workplace, as well as to a safer country, and, in the end, to a safer world.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Information protection as a tool for social status

Although American businesses lose an estimated \$300 billion every year through failure to identify and protect critical information, virtually nobody outside the government pays any attention to OPSEC, which is the identification and protection of critical information. Even within the government many people do not understand the importance of protecting critical information. As OPSEC professional Layne Marino says in his popular talk on *Marino's 10 Laws of OPSEC*, "You are the only one who cares about OPSEC, and you are delusional." We are therefore always delighted when someone expresses an interest in protecting information, but sometimes amused by the reasons for the interest.

As an example, someone recently went to the person at their (very large) corporation who was responsible for assigning offices, and *demanding* a larger office. Putting aside issues of how best to get favors, they were told that their office was of an appropriate size for their position in the corporate food chain, and asked why they should have something larger. The answer was that they were in the M&A group, and that they, even more than most, has sensitive information that needed to be protected, which meant that they needed more space.

Now, in fact, it is true that people involved in mergers and acquisitions do have a lot of information that is sensitive, and perhaps even critical. This information would certainly qualify as insider information if used by its caretakers for their own profit, and which, if widely known, could influence the market price of both the company doing the acquiring and the company being acquired.

The argument would, however have been more convincing had the facilities manager not recently been in an elevator where the m&a type got on and, for 20 floors, discussed the acquisition of company Y by client X, the current price of each, and the estimated purchase price.

Now, as it happens, acting on information you hear while listening to people foolishly talk in an elevator, or in a bar, or in a restaurant, or at a party, or on the train, or at a conference, or anywhere else where there is no expectation or privacy, is neither insider trading nor economic espionage. And it is not an unreasonable guess that twenty people were privy to this confidential information, and that some of them discussed this information with others. And that one or more of the widening circle of the informed acted on the information for their own profit.

We frankly don't know whether a larger office was obtained, but we are fairly sure the talkers were neither disciplined nor fired. This would have set a good example for others in this probably leaky corporation, but in a corporation with a corporate culture of disinterest in protecting critical information, the real defense against information loss is to be large enough not to mind the losses, rather than to stop the leaks.

3. Executive Protection — Ready when you are, C.B....

There are a lot of people who have cars pick them up and carry them from place to place. Some of these people are folks who, either because of their wealth or their job, are at risk.

While it is nice to have the safety and convenience of a car and driver, it is not nice when these expose you to unnecessary risk. The basic risks are, of course, the risks you face in any car, which can easily be summed up as don't drive if you or your driver are drunk or on drugs, and wear your seatbelt. Lest you think that these basic safety tips don't apply to you, keep in mind that if they applied to Princess Di, they probably apply to you...

Another issue which we have discussed in the past is letting common sense be overcome by pride, and insisting on having parking spaces which say either "Kidnap Me," "Kill Me," or, roughly equivalent, have your name or your position.

But an issue that we have not discussed is the fact that the mere presence of your car can be, in OPSEC terms, an indicator of your presence. If your car is recognizable – and you can rest assured that it will be if someone is interested in you – you don't want it being used to give adversaries a long lead time to come for you.

The car should be at hand, but not waiting at the curb so that anyone who knows it will know you will soon be there. This way, when you are ready for the car it can arrive at roughly the same time you do, thus eliminating this particular indicator. And if you are delayed you can send it away again.

In the past this kind of co-ordination was more difficult. But now, between cell phones and small encrypted radios, you can safely communicate between car and passenger, and eliminate, at the very least, the risk that you might otherwise face by the mere presence of your vehicle.

4. Technical Issues — Explosives as a tool of cyber-disruption

There is a lot of concern these days over protection of our cyber-infrastructure. You can't read anything these days – including this journal – without getting advice about firewalls, anti-virus tools, dealing with hackers, and backup storage of data.

All of this advice is both valid and important, and should be taken to heart. Nonetheless, if you keep in mind the adage that simple is best, you can see that your cyber world also has a physical component which should not be overlooked so quickly.

This means that you may have the best hardware and the best software, and full-time monitoring of your network, and feel pretty good about how safe your system has become. However, if we can get into your facility – and we can assure you that we *can* get into your facility – there is little stopping us from blowing up your computer. And when we blow up your computer not all the software and monitoring in the world will be of help, and you'd best hope you had good backup and recovery plans.

You can deal with this issue in two ways. First and foremost, you really do need to listen to the contingency planning folk, and be prepared for the loss of everything you have. The good news is that you don't, in this case, have to worry about the cause of the loss. In fact you really don't care: Fire, flood, tornado, hurricane, act of God, war, crime, accident, or mere fluke, it doesn't matter. If you are prepared for a loss from natural disaster, you will be prepared for a loss from unnatural disaster.

The second is by having physical security appropriate to the possible threat and impact. Your security people are, in fact, likely to either know something about physical security, or where to find specialists that can help you analyze the threats you face, the vulnerabilities you have, and the impact if your vulnerabilities are exploited.

Obviously, there is no such thing as perfect security (which is why you have insurance), but you can at least deal with a significant number of the issues you face. But when doing your planning try to keep an open mind, and to think of the extraordinary threats, not just the ordinary ones. We have recently listened to a lot of people describing sophisticated solutions to sophisticated problems, and clearly overlooking the simple problems. Like someone blowing up your data center.

5. Real Stories from the Field —False alarms as a tool of the bad-guy

There are lots of reasons why physical security measures work, and are of great value. And we have often been assured by people that their premises are secure. While this may in general be true, it usually means that it is secure from normal attacks, not from well-planned attacks so unlikely that nobody has planned to counter them. It also usually means that premises are secure from specific individual threats. But what happens when there are multiple threats? At what point does your facility become vulnerable.

We have heard of several cases where multiple threats occurred – generally a series of false alarms, coupled with real physical events, were enough to displace people enough for bad guys to get in and do damage.

As an example, let's talk about data centers. When there is a fire in your premises, who stays in the fire area to guard your data center? And if there is a bomb threat, who stays in the threatened area to guard your data center. And if a package arrives at the data center, and, when it is opened, white powder spills out, who stays in the threatened area to guard your data center? And if there is a category 3 hurricane heading your way, who stays in the building to guard your data center? If a car alarm goes off in your parking lot will a guard leave a post uncovered to investigate?

Now let us assume that someone really wants to get into your data center, but not enough to actually kill people to do so (which is a different scenario). How many critical events need to be triggered to compromise the facility? If there is a fire and a bomb threat simultaneously, will that be enough to cause the area to be abandoned?

One way to reduce this problem is to actively think about how you would penetrate your own facility. What series of things would you need to do to get in and out. What if you were not afraid to cause some physical damage, like knocking down doors. And how about if you were willing to actually kill people? As you think of scenarios, see if your protective measures would deal with them, or whether you would be vulnerable.

Oh, by the bye, this approach can also be used for good, not just for evil. We recall the case of the French terrorist holed up in an apartment in Paris. The police had cleared the apartments above, below, and on the rest of the floor. All they needed was to get the terrorist to come out. They finally glued a cat to the wall in the hall. When the terrorist eventually came out to see why the cat was making such a racket, he was captured without incident.

The hero cat was carefully shaved off the wall, none the worse for wear.

6. Book and Product Reviews

Travel Sentry™ certified locks

<http://www.travelsentry.org/>

One of the annoyances of modern air travel in the United States is that you must leave your luggage unlocked. The two easy ways to get around this have been to take only carry-on luggage, or simply not fly. Neither of these has been entirely satisfactory.

Now there is another alternative. Some clever guys have teamed with the TSA and manufacturers to come up with locks that can be opened by you and by the TSA. At the moment Master Lock is making these locks, and locks can be purchased at Target and Brookstone. In addition, a number of manufacturers of luggage are developing lines that will use *Travel Sentry™ Certified lock*.

Now, if the TSA has the tools or combinations to open these, aren't they likely to be obtained by criminals, too? Well, if the FBI and the CIA have problems from time to time, it is safe to assume that TSA will be no better. Nonetheless, we like to think that problems will be sporadic, and that locked luggage will still put you way ahead of the game in terms of the safety of your luggage.

The bottom line is that if your current luggage will allow use of a padlock, you might wish to get a *Travel Sentry™ certified lock* and travel with somewhat greater peace of mind.

Zone Alarm, Version 5 **warning**

Zone Labs, Inc.

<http://www.zonelabs.com/> 1-415-633-4500

We have on several occasions recommended that readers use a firewall on their home computers, and have noted that we ourselves use Zone Alarm. Those of you who have followed our lead in using Zone Alarm, and have automatically updated the software as new versions came available, will have suffered some problems after installing Version 5.

We first noticed two problems: Chkdsk would not run on our C drive when we re-booted our computer after the upgrade, and Norton Anti-Virus stopped scanning incoming and outgoing e-mail. Others we know had other problems, including not only programs that did not function properly, but also the dreaded Blue Screen of Death!

We started by sending a message to the technical support folks at Executive Software, who make Diskeeper, the leading software for de-fragmenting hard drives. We knew their software wasn't responsible for the problem, but guessed that they had heard every question possible regarding this kind of problem. They responded immediately with an explanation of what was happening, and a few possible causes, including the new version of ZoneAlarm.

Our next step was to look on the ZoneAlarm support forum (<http://forums.zonelabs.com/zone/zone/>), where we discovered a whole host of problems associated with version 5.0.590.015 and 50.590.043.

According to the online information, Zone Labs is aware of the issues, and we have every confidence that they will deal with them in a timely manner. Nonetheless, since they have chosen not to pull the upgrade pending resolution of the problems (see our article *What companies can learn from Abu Ghraib* in the June 2004 issue of *ÆGIS*), if you have just upgraded to version 5.0.590.015 or 50.590.043 and are having mysterious problems, we recommend that you uninstall version 5 and re-install version 4.5.594.000. For users of the free version, this can be found at <http://download.zonelabs.com/bin/free/information/znalm/zaReleaseHistory.html>.

For those who have ZoneAlarm Pro, you can download 4.5.594.000 at <http://download.zonelabs.com/bin/free/information/zap/releaseHistory.html>.

7. Free-Subscription/Unsubscription/Copyright Information

•• *ÆGIS* e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2004 by The LUBRINCO Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com) and L. Burke Files (LBFiles@lubrinco.com).

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

- **Protection of trade secrets and intellectual assets.**
 - Anti-economic espionage.
 - OPSEC: The identification and protection of information that would give your competitors and adversaries an advantage.
- **International financial investigations and due diligence consulting.**
 - Location and recovery of missing and hidden assets.

- Establishing business relationships and strategic partnerships in Central and Eastern Europe, the offshore financial centers, Beijing and Shanghai, Central Asia, and Latin America and the Caribbean.
- Anti-money laundering and financial fraud requirements under the *International Money Laundering Abatement and Anti-Terrorist Financing Act of 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 July 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.