



**ÆGIS** journal

***Addressing threats that affect your bottom line***

Volume 9 Number 11, November 2006

From the case files of

**LUBRINCO**

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

and

**FE&E** CLARITY FROM COMPLEXITY  
Financial Examinations & Evaluations, Inc.

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

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

**This month's features:**

- **Special Announcement Critical Information and IP Conference**
- 1. **Asset Location and Due Diligence — Other ways of getting information**
- 2. **OPSEC, Economic Espionage, and Competitive Intelligence — Competitors and adversaries**
- 3. **Executive Protection — Walking sticks in lieu of impact weapons?**
- 4. **Technical Issues — Self defense issues**
- 5. **Real Stories from the Field — Houston Networking Group**
- 6. **Book and Product Reviews — The Bat! Private Disk**
- 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](mailto:conference@aegisjournal.com)

## 1. Asset Location and Due Diligence — Other ways of getting information

In the exercise of due diligence the most obvious route is not always the most possible route. As an example, we know of a recent case in which a larger retail company was interested in acquiring a smaller retail company that was not interested in being acquired. Because there was no immediate interest in being acquired, the smaller company did not provide information on their sales, though they did provide a figure that they considered would tempt them to sell.

Since the smaller company was privately held, sales figures were not publicly available. While an annoyance, this lack of sales information was at best a minor hindrance for the acquiring company, because while the figures might not be publicly available, they were nonetheless still available.

How did the larger company get the information? While sales may have been kept confidential, the sales locations were clearly not confidential, and their locations, present and planned, was readily available. As it happens, retail rentals agreements frequently involve a percentage of sales as part of the rent. Thus, the malls where the smaller company had stores knew the

sales figures for the private company's stores. And since boilerplate lease agreements do not specify that information relating to the lessees be kept confidential, the larger company was therefore able to use its economic clout (sometimes referred to as threats and bribery) to get the landlords to provide them detailed sales information.

When it became clear that the smaller company was not willing to sell at the price the larger company wished to pay, the larger company chose to take proactive steps to hinder the growth of their competitor. By observing the actions of the smaller competitor – looking for indicators of what they were doing – they were able to figure out where new stores were to be built. With this knowledge in hand, they offered to pay higher rental rates to the malls where the smaller competitor wanted to put stores, displacing them. This tactic was very successful in closing off good retail expansion possibilities for their smaller competitor.

When exercising due diligence, it is therefore important to recognize that there may be multiple sources for any given piece of information, that certain critical information may reveal what is being done, and reveal it as precisely as if the detailed information itself were made available from the target (source).

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — Competitors and adversaries**

One of the things that distinguish OPSEC from other forms of risk management is the emphasis on specific threats. That is to say that normally a risk management team looks at what is valuable and figures out how to protect it from likely threats. This means that we are largely aiming at crimes of opportunity.

In some cases this means that we try to make the potential target unattractive, so that bad-guys will go elsewhere. Thus, when dealing with protective services, our hope is that our principal will be protected to such a degree that a potential kidnapper will choose some other, less-well protected potential victim.

In other areas it means that we look at potential solutions to general problems. Thus, if we are prepared for flood and fire, we are equally prepared to deal with earthquakes and either random or specific violence. This approach generally works well, especially with common threats so we know that if we build to code, have sprinklers and fire alarms, do regular fire

drills, and have fire extinguishers at hand, we are largely safe from fire. But we still aren't safe from arson.

OPSEC – the identification, valuation, and protection of critical information – information which would give your competitors and adversaries an advantage – steps in where there are specific threats. But in order for OPSEC to work, you have to be able to identify these threats. And herein lies the somewhat artificial distinction between competitors and adversaries.

Competitors are fairly easily identified: They are the people and companies that do what you do, and are competing with you for business. Most domestic competitors within the United States will cheerfully gather competitive intelligence to use against you for their own benefit. Rarely will a U.S. corporation do anything illegal to gain information. Foreign corporations may not be so scrupulous, particularly on their own turf. But since over ninety percent of the information gathered even through questionable means is open-source intelligence, the threat from competitors – from competitive intelligence – can generally be dealt with in a cost effective manner once the company commits to dealing with the problem.

Adversaries are a more active threat. They can vary from people or organizations who wish you harm, to governments or corporations willing to move from competitive intelligence to economic espionage. People or organizations may wish to do you physical harm for a wide variety of reasons. These span the spectrum of motives: Those who wish to kidnap or harm you for money; those who wish to harm you for religious reasons; those who wish to harm you for political reason; those who wish to harm you for ideological reasons; those who wish to harm you for economic reasons, and those who wish to harm you because they are just plain crazy.

While it is easy to identify competitors, identifying adversaries requires more sophisticated intelligence gathering and will involve co-operation with others, both on a governmental and non-governmental basis.

### **3. Executive Protection — Walking sticks in lieu of impact weapons?**

In the last issue we discussed collapsible impact weapons. One might wonder if walking sticks and umbrellas might serve as a reasonable alternative to impact weapons for those providing protective services, yet not involved in law enforcement. To find out, we carried a walking stick for a month, and practiced a lot of stick techniques from various sources.

There are plusses and minuses to carrying a walking stick.

**Plus:** Canes are legal in places where impact weapons, guns, and knives are not.

**Minus:** If you are not old enough to look like you might actually need a cane you might have to do some explaining as to why you have it (with the easiest explanations being either that you have hurt your knee, leg, or foot; or that you like walking sticks and it is simply an affectation).

**Plus:** You can always have it with you.

**Minus:** If you don't need a cane, and are not used to carrying one, you are likely to leave it in a restaurant or car.

**Plus:** It is already deployed and in your hand.

**Minus:** You always have at least one of your hands full when you carry it.

Assuming that you can carry a walking stick without looking like a total fool, you next need to address the question of how to use it. One approach is to use it as you would any other impact weapon for which you have received certification. This approach has the advantage of allowing you to use your existing physical skill set backed up with certification in a set of techniques, even if the tool with which you are using them is different. It has the disadvantage of removing many techniques associated with use of sticks.

A second approach is to take non-impact weapon stick fighting training. Note that some stick fighting training comes from martial arts, rather than being developed specifically for canes and umbrellas, and may not be appropriate for most of us. This is not because the techniques are flawed, but because martial arts are *arts*, and require continual practice to be able to use successfully. For defensive tactics, long experience by generations of law enforcement trainers tells us that it is more appropriate to adopt a small set of techniques that can be learned quickly and retained for a long time without practice.

A third approach is to find instructions for non martial arts cane fighting in books or on the Internet and self-train using that. One option would be the January/February 1901 article on can fighting from Pearson's Magazine written by E.W. Barton-Wright, and reproduced in the December 2000 (vol. 3) issue of the *Journal of Non-lethal Combatives* ([http://ejmas.com/jnc/jncvol3\\_1200.htm](http://ejmas.com/jnc/jncvol3_1200.htm)). These articles can be found at [http://ejmas.com/jnc/jncart\\_barton-wright\\_0200.htm](http://ejmas.com/jnc/jncart_barton-wright_0200.htm) and [http://ejmas.com/jnc/jncart\\_barton-wright\\_0400.htm](http://ejmas.com/jnc/jncart_barton-wright_0400.htm). While quite instructive and useful, these articles (which seem to us to cry out for heavy canes such as blackthorns), are doubtless merely a précis of what was offered in training.

Two things are striking (if you will forgive the pun) about the Barton-Wright article. First is the assumption that your adversary will also be carrying a

walking stick. While this was likely true in 1901, it is not the case now. Second is the fact that while the article's Conclusion notes that the more dangerous techniques are not described, in the less dangerous techniques shown there is a willingness to whack people over the head, or break their arms or knees.

Even assuming the basics of a reasonable claim of self-defense (opportunity, ability, jeopardy, and preclusion), you may have a hard time explaining away why you were carrying a cane when there is no medical reason for you to have one, and the amount of force used (breaking a knee is grave bodily harm). This is an acceptable risk if your life is, in fact, at risk (which happens to the average American once every 83 years, with the risk being higher in the trade). You will face liability if the situation was not as you envisioned it to be, so you must think of a cane as the equivalent of a firearm.

A more modern option is the 1923 book *The "Walking Stick" Method of Self-Defence by "an officer of the Indian Police."* This book addresses directly the potential for injury of walking sticks, noting that "Certain of these exercises will occur to many as being somewhat brutal. This may be the case; but we must not overlook the fact that no sane person will employ them in any but the last resort. At the same time we should bear in mind that the individual who attacks us without provocation is unlikely to observe the "Don't hit below the belt" rule, and when up against such a one we owe it to ourselves and those dependent on us not to allow ourselves, in an affair not of our seeking, to be overcome by an opponent out to employ any means best suited to attain his own ends, "Your money or your life!" The techniques still require you to think of the cane as being at the same level of force as a firearm. This book, available through Paladin Press (<http://www.paladin-press.com/detail.aspx?ID=1086>) favors the light stick, with the techniques being less obviously lethal, yet, one might hope, equally effective.

There is also a contemporary program offered by *Canemasters*, which will be covered in the December issue.

Independent of the approach taken, walking sticks and umbrellas can be an effective emergency safety tool, and may well be a good alternative to impact weapons for some of our professional readers.

#### **4. Technical Issues — Self-defense issues**

We recently were set up to go to a meeting, with people flying in for this event. Unfortunately, the person with whom we were to meet was in the hospital, so all the travel and preparation was for naught.

The hospitalization came about because the day before the man went to pick up his daughters at his ex-wife's home to take them into Gotham for the day. For reasons not relevant to this article, the ex-wife apparently decided she didn't want the daughters to go, and called a neighbor. The neighbor – formerly the neighbor of the husband – came over, dragged the father from the car, and beat him up in front of the daughters, sufficiently badly to require hospitalization (and missing our meeting).

Now, you can defend yourself, and those under your direct care, if you reasonably feel that you are in danger. This generally means that you can verbalized why you felt your attacker had the *opportunity* to do you harm (he was close enough); Why your attacker had the *ability* to do you (he was bigger, was armed, etc); Why you reasonably felt you were *jeopardy* (he was threatening or attacking you, had a reputation for violence, etc); The actions you took in the way of *preclusion* (you tried to run away, talk him out of it, etc.).

The rules change a bit if you are not defending yourself or those under your direct care. To protect yourself you need to show that you had a *reasonable* belief that you faced death or grave bodily harm, with “reasonable” meaning that a reasonable person would agree with your assessment of opportunity, ability, jeopardy, and preclusion. If you are randomly intervening, however, your assessment has to be both reasonable and *correct*.

While there may be a certain charm when watching a good guy beat up or kill a bad guy on television or in the movies, violence in real life is never as gratifying or clean. In the movies someone gets beaten or shot and is fully functional by the end of the episode. In real life you may punch someone in the face and have them fall down, striking their head and dying. Or they may require a lifetime of physical (and emotional) therapy.

We don't know how the attack that cancelled our meeting will affect the victim, the attacker, or the young girls who saw their father being beaten. But we would wager that the event will turn out to be a costly one for all involved in this needless event.

## **5. Real Stories from the Field — Houston Networking Group**

When dealing with adversaries, it can be greatly beneficial if those with a common interest band together to share information. While it requires forethought, dedication, and initiative to share information, it can be done. An example of this recently began in Houston, where a group of professionals from energy, law enforcement (active & retired), and aerospace have formed an Executive Protection/Security Driver networking

group. The group met for the first time this past April at ConocoPhillips. Regular readers will recall articles by Bob Reyes of ConocoPhillips in the June 2003 and October 2005 issues of this journal.

Nine people attended the first meeting, which was an ice-breaker of sorts, with introductions being made over a catered dinner.

The hope is to begin with quarterly meetings, where they will discuss issues that affect all participants as they perform their respective corporate security duties. The initial focus will be on executive protection/security driver duties. All those present that evening felt good about organizing and continuing the program, with everyone agreeing that a group such as this should have been organized long ago. The second meeting, through the kindness of Mike Bechaud, Marathon Oil corporate security representative, was at Marathon Oil headquarters in July.

The profession of executive protection is a very involved field, and has become more and more dangerous as threat level of the principals increases. Without networking among peers, professionals are robbing themselves of this valuable resource. The first meeting was immediately positive, as the participants now know others in Houston who are performing the same types of duties. They can now call upon each other for assistance, and discuss common issues such as training, equipment, and methods. Subsequent meetings have been equally fruitful.

After the first meeting there were inquiries from other corporations who are interested in joining the networking group. In addition, the group will be a resource for fellow professionals who may find themselves in Houston and may need assistance.

We would urge those executive protection professionals interested in forming similar groups to contact:

Bob Reyes (ConocoPhillips Executive Protection Officer)  
+1-281-293-1275 (work)  
basilio-bob-jr.reyes@conocophillips.com

or

Mike Bechaud (Marathon Oil Domestic Security Representative)  
+1-713-295-3836 (work)  
jbechaud@marathonoil.com

## 6. Book and Product Reviews

### *The Bat! Private Disk*

RITLabs, \$29, or \$19.43 if you use The Bat! E-mail client  
<http://www.ritlabs.com/en/products/pd/>

In the July 2006 **ÆGIS** we wrote about *The Bat! Voyager*, the portable version of our e-mail client of choice that we installed on a USB flash drive (it would go on any portable drive). We mentioned that while Voyager encrypts all the data for your safety, we also carry other data suitably protected. A number of people asked what we recommend for that protection. Our choice is *The Bat! Private disk* from the folks who make The Bat! (discussed in the January 2005 **ÆGIS**) as well as Voyager.

Private Disk installs easily, either onto a hard drive so that you can know that all of your confidential information *is* confidential, even if the computer or drive is stolen. You can also install it onto the flash drive. It allows you to create an AES encrypted virtual disk that Windows sees as just another drive. In our case it is seen when opened as a 3.5 gig Z drive. When you create the password it gives you an analysis of how strong the password is. We recommend you use an entire sentence. This should be something easy to remember, but too long for anyone to randomly guess. The file which contains the encrypted data can be backed up as needed.

To open the virtual drive you run the Private Disk program, which asks you which file you want to use. When you select the file and click OK, the drive mysteriously shows up in Windows Explorer, and behaves just like any other drive. Obviously, you can also create an encrypted virtual drive on your hard drive for sensitive information.

The disadvantage of Private Disk is that, unlike (apparently) Voyager (see the July 2006 issue of **ÆGIS**) or Password Safe (see the February 2001 issue of **ÆGIS**), it requires that its drivers have been run at least once by someone with administrative privileges. This means that if you use the computer in an airport or hotel or internet café, you may get a message saying you do not have sufficient rights to run it, and you may not be able to get someone with administrative privileges to run it.

In this case you need a plan B, which would be encrypted on-line backup such as iBackup (see the August 2006 issue of **ÆGIS**). If you don't have access to the Internet from that machine, and can't find an administrator willing to let you run unknown drivers requiring administrative privileges, you are out of luck.

There is a 30 day free trial, so you can give it a try with no obligation. We recommend that you do so.

## **7. Subscription/Unsubscription/Copyright Information**

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2006 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 Philips (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](mailto:subscribe@aegisjournal.com).

To subscribe to our AvantGo channel, go to [http://avantgo.com/channels/\\_add\\_channel.pl?cha\\_id=1773](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](mailto:unsubscribe@aegisjournal.com).

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

If there is a topic that you would like to know more about, send it to [editor@aegisjournal.com](mailto: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](mailto: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 November 2006 **ÆGIS** (© 2006 **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.