

ÆGIS



Addressing threats that affect your bottom line

Volume 8 Number 4, April 2005

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 Announcement**

1. **Asset Location and Due Diligence — D&O lawsuits as a tool**
2. **OPSEC, Economic Espionage, and Competitive Intelligence — OPSEC and embarrassment**
3. **Executive Protection — Planning for tiger attacks**
4. **Technical Issues — More anti-spyware**
5. **Real Stories from the Field — Online dating scams**
6. **Book and Product Reviews — Buying artwork for the office:
George Pissarro and Catherine Nicodemo**
7. **Subscription/Unsubscription/Copyright Information**

L. Burke Files will be speaking at the Offshore Summit
21-22 April in Miami, Florida
www.samuelgroup.com

Richard Isaacs will be speaking at CPM 2005 West
24-26 May 2005, Las Vegas, Nevada, USA
<http://www.contingencyplanningexpo.com/information/invitation.asp>

1. Asset Location and Due Diligence — D&O lawsuits as a tool

Recently the entire board of directors of a professional organization resigned en masse, along with the executive director. This came as the culmination of years of efforts of a single member who wished to change the direction of this popular organization. This member had, in fact, eventually been elected to the board, but was forced to resign by popular vote of the general membership at an annual conference.

The de-frocked director subsequently ran for office again, and was again re-elected, giving them, no doubt, the mandate of the people. The director then began a series of costly lawsuits against the organization.

Eventually, the organization's insurance company said they would not cover any further costs for lawsuits from this individual. The board members, being no fools, recognized that they served in order to help the organization be more professionally fruitful, rather than for money or for anything else central to their lives. Therefore, the risk of personal impoverishment through legal fees was simply not worth it, and they resigned.

We are not concerned here in whether the member was right or wrong, or whether what they did was good or bad, or whether fundamental changes were or were not needed or desirable, or whether the organization will survive. We are only concerned with how the board failed to deal with this novel technique for using the system as a tool of attack.

As always, when looking at any policy measures, what should be done must be judged by the five basic criteria:

1. What problem is the policy or measure trying to solve?
2. How can it fail in practice?
3. Given the failure modes, how well does it solve the problem?
4. What are the costs, both financial and social, associated with it, and flowing from its unintended consequences?
5. Given the effectiveness and costs, is the policy or measure worth it?

In this case, the organization simply did not recognize that it faced a long term, well-organized, ongoing threat. Because the measures they took didn't address the problem (as so often happens, nobody ever asked the first question), they were simply inadequate to deal with the threat.

Because there was not a recognition that a threat was faced, the board did not dignify the attacks with a meaningful public response. Since, in the minds of many, silence is taken as guilt, this put them at a perceptual disadvantage.

Additionally, and again because the attack was not taken seriously (largely, on a guess, because the board members knew they were not doing anything wrong, nor acting for their own gain), the board did not take measures to either throw the member out, or put in a prophylactic bylaw change to prevent members who were expelled from the organization or forced to resign from the board from future participation.

When faced with legal action, the board apparently (we have had no contact with board members, and can only make assumptions based on our experience and what we observed) responded, but did not counterattack. In fact, our experience tells us that in cases such as these, if there is no countersuit there is no reason for the attack to stop.

This last issue points out a final problem: While not all attorneys are bad (one attorney pointed out that their firm was very good, but that they were so overworked that they never had time to do an adequate job), if you actually become involved in litigation it is important to have a good lawyer. Good lawyers sometimes cost more per hour than bad lawyers, but keep in mind the truism that the only thing more expensive than a good lawyer is a bad lawyer. Lawyers, however, don't exist *in vacuo*.

By this, we mean two things. The first is that all lawyers don't know all the same stuff. The body of law is so enormous that lawyers specialize and the more specialized your problem the more specialized the lawyer you should seek out. Thus, a lawyer, who is a great collections attorney, may not be a good attorney for a libel action.

The second is that you have to explain your problem to a prospective lawyer, make sure that they understand your problem, and that they can help you solve your problem. You then have to work with your lawyer to make sure that they are doing what is needed to be done, and that what they are doing makes sense. If it doesn't make sense, you need to have them explain to you why what they are doing makes sense. If it still doesn't make sense, you need to change lawyers.

2. OPSEC, Economic Espionage, and Competitive Intelligence — OPSEC and embarrassment

OPSEC can protect against a wide variety of problems. In general we think of economic losses or of people being placed in physical danger because information has been discovered. But it can also save from embarrassment. This was brought to mind recently when we read an announcement from Nokia that they had dropped plans to develop mobile phones with fuel cells.

For those in the business, this was no surprise. Nokia, which once was a great technological innovator – the 6150, 6160, and 6190, followed by the 6360 and 6310i were among the best terminals ever made, and their user interface, left over from that era, is unparalleled – has fallen so far behind on the technology curve that in a quad-band world they have been unable to produce anything more than a tri-band handset – hardly a “worldphone.” Indeed, if you look at the last 25 GSM terminals released by Nokia, you discover that 9 of them (36%) are current-technology domestic dual-band devices, one of them (4%) is an outdated single-band device), and fifteen of them (60%) are outdated tri-band devices. None of them (a whopping 0%!) are current technology worldphones!

It is certainly not uncommon, as technology advances, to see companies fall behind. Sometimes, when this happens, they simply go out of business or are acquired. Or, if they have a lot of cash, as Nokia does, they may acquire a smaller company that has kept up with technology. But, in general, no matter what your status, you really don't want publicity telling others that you are falling behind. And you certainly don't want to be putting it out yourself!

If Nokia had an inclusive OPSEC program, the PR and advertising people would be in the loop, along with a manager able to distinguish information that is of benefit to the company from information that would embarrass the firm. While jokes about Nokia realizing there is a gap in the buggy-whip industry are amusing, they are probably less so internally, especially since they can easily be avoided with an OPSEC program.

3. Executive Protection — Planning for tiger attacks

Tigers can be a real threat. They have killed substantial numbers of people over the years. Beautiful as they are, the experience of even trained folk such as Sigfreid and Roy should still give one pause. While those who own cats may occasionally get scratched or bitten, the stakes are really upped when the cat weighs hundreds of pounds, and is not, by the wildest stretch of the imagination, domesticated.

It has been estimated that as many as 3 out of every thousand tigers might eventually attack a human. While some simple measures, such as wearing a mask on the back of the head (tigers almost always attack an unsuspecting human from behind) work for a while, tigers are not stupid, and learn to distinguish between a person walking backward and a man wearing a mask.

There are, of course, other threats that are even greater. As an example, for every person killed by a tiger, a hundred die from snakebites! And as dangerous as tigers and snakes might be, lions can be worse. In one case, a pride of lions killed more than a thousand people over a fifteen-year period. And in Alaska, the barren ground grizzly killed ten people in 2000. This may not sound like many, but it is when you consider the low human population density in the area. And the fact is that the barren ground grizzly does not think of humans a prey, but, rather, simply doesn't like us.

We are proud to say that we have never suffered a tiger attack at any LUBRINCO office, nor have we ever lost a client to a tiger attack. Nor, thankfully, to anything else, either!

What, you might ask, is the secret of our success in dealing with the tiger threat? In spite of the title, it is not our not-inconsiderable planning skills and experience, but, rather, the fact that, outside of a zoological garden, neither we nor our clients have ever been anywhere near a tiger. Indeed, the closest we have ever come to a wild animal here in Gotham was when we left our Manhattan apartment one morning and discovered, in the children's park next to where we lived, roughly twenty New York City police, guns drawn, facing down a baby deer. If a fawn can appear in Manhattan and terrorize a neighborhood (save for the kids, who thought it was adorable), why not a tiger?

The point of this is that when protective measures are taken, they should have some strong relationship to threats faced. Notwithstanding the level of danger involved in a tiger attack, not a penny should be spent by any protective team in Manhattan – and most of the rest of the world – in protecting from tigers. Or other *specific* threats of equally low probability.

4. Technical Issues — More anti-spyware

Recently a colleague received a message from his Norton Anti-Virus software that he had a specific piece of spyware (SAHAgent) on his computer. He was running several anti-spyware programs, so this was disturbing. Even more disturbing, he could neither find the infection via a

manual search, nor could he get information from Symantec on how to eliminate it.

About then, he fortuitously got an e-mail from the folks at Firetrust, makers of the wonderful can't-live-without-them MailWasher and Benign (<http://www.firetrust.com/>) recommending an anti-spyware package made by someone else, called Spyware Doctor (<http://www.pctools.com/spyware-doctor/>). Our colleague downloaded and installed the software, ran the update, and then did the scan. It found, and eliminated, the offending piece of software that had been plaguing him!

Filled with enthusiasm, he called us, and we shelled out our money and bought a copy. When installed, it blocked the tracking cookies associated with using AOL Instant messenger, alerting us every time AIM tried to install the cookie, as well as cookies from Microsoft's BCentral.

When we did run a scan, it didn't find anything wrong, which was fine with us, but it did reveal a teeny issue. When we ran the scan, our firewall, Outpost (<http://www.agnitum.com/products/outpost/>) detected that the scan had modified the memory of several running processes, and cut off their access to the Internet. A typical message said, "Network access for navpw32.exe was blocked because its memory was modified by another process." Since navpw32 is needed for us to get e-mail, a re-boot was necessary.

Now, we don't know why the scan modifies the memory of other processes, and, in fact, the people at Spyware Doctor don't know either. We are certain that it is unintentional and benign. And we know that three other programs we run (Oxygen Phone Manager II, and BigFix, and Acrobat writer) do the same thing. If we weren't running Outpost we would never have known, and if you aren't using Outpost you will never know. We are delighted that Outpost does this, as it could be important if this were a malevolent attack.

Does this mean that we won't use Spyware Doctor? Not at all. What we did was make sure we installed all the updates, then ran an original complete scan, then reboot. We then scheduled regular automatic updates in the middle of the night. And when we plan to do our daily reboot we do a quick scan, then we do our reboot. When we do our weekly cleanup we run another complete scan before the reboot.

We like to think that between the folks at Outpost and the folks at Spyware Doctor someone will figure out what is going on and how to make it stop. In the meanwhile we are perfectly delighted to have the protection offered by each of these programs, and are perfectly willing to deal with the minor

inconvenience of running the scan just before we plan to reboot. We recommend Spyware Doctor to those concerned about spyware.

5. Real Stories from the Field — Online dating scams

Recently we were asked to get involved in correspondence with a girl on a cyber dating service. The girl, whose picture was certainly more than appealing, turned out to be located in Ghana, which raised enough concerns that we were asked to participate in the exchange.

Now, it is certainly true that this could be a desperate and attractive young woman for whom *anyone* in the States would be an attractive alternative, independent of their age or looks. We have certainly seen many beautiful Russian women desperate to escape to here. And we see nothing particularly wrong with this as long as both parties know what they are getting into.

However, it seemed more likely that this would culminate in a request for money, (we estimated that the likelihood that this was a desperate girl would be around two percent, and the likelihood that we were sending messages to other middle-aged men behind the picture to be approaching 100 percent.

It was suggested that we might like to come to Ghana to meet her, which was rejected because we were too busy. It seemed impolite, if not inappropriate, to mention in the conversation that men who went to meet women in Africa – and sometimes even to meet them in Europe – often didn't fare so well.

We eventually reached the point of her suggesting that money be wired to her via Western Union. We suggested that we would spare her the necessity of soiling her hands with cash, and would instead send money to our counsel in Accra, the capital of Ghana.

The other side said that this was too much effort on our part.

We pointed out that it was little effort for us, plus the attorney could help make sure all her paperwork was in order, which would help speed the process in getting her here. Plus, it would give her relatives some feeling of confidence in knowing that their little girl was in good hands. The correspondence eventually tapered off. They ended up doubtless moving on to someone more willing to send money, and we ended up with this story.

However, not everyone gets off so easily. Someone else we know met a woman online and ended up deeply involved – at least on the phone. They chatted on the phone for hours every day, and the woman even called his

father and introduced herself as his son's girlfriend. She sent him pictures, and we must say that the girl in the pictures was drop-dead gorgeous.

Because the son was lending the woman money, the father hired a private detective who said the girlfriend bore no visual resemblance to the woman in the picture. While she insists the detective was wrong and that the money will be repaid, we are not holding our breath.

Why is it that in the first case nobody got burned and in the second someone did? It was, in fact, the mirror test, rather than cunning or paranoia: The first person looked in the mirror and asked whether, considering his past dating experience, a woman who looked like that would be going out with him. Since the only positive answer involved an alternative universe, he called us. The second person did not do the mirror test.

Does this mean that on-line dating is dangerous? Not more than off-line dating. Many people have met other people this way, and in most cases it has worked out reasonably well for all involved.

Nonetheless, in online dating, or anything else where something seems too good to be true (as the father of one of our editors found out when he got a letter – with no fine print – from Time Magazine saying he had won a lot of money from them), it is good to remember that, if it sounds too good to be true, it probably is....

6. Book and Product Reviews — Buying artwork for the office

We were recently asked to recommend places to buy artwork for an office (we know a lot of artists). You can, in fact, with relatively little effort buy really fine works of art that will give you endless pleasure, and cost relatively little. The process itself, visiting with the artists and looking at their work, is itself generally a pleasure, and the small amount of time it takes will almost always give you a more pleasant working environment than merely calling facilities management and asking them to fill up the wall.

In addition, by buying works of artists who are not so famous that the price has escalated beyond all reason, you get to spend your art budget on works that you really like, rather on works largely bought for the signature, or because they fill the space and more or less blend with the furniture.

Plus, the economics of going directly to the artist and not through a wholesaler or a dealer or a decorator are significant. Artwork is usually marked up from 30% to 100% as it passes from the artist to the wholesaler to the dealer to the public. A \$12,000.00 retail sculpture may be purchased

from the artist for approximately \$4,000 and the buyer has no worries about provenance, and the notorious art dealers trading in forgeries – you purchased an original from the source – the artist!

Two artists of our acquaintance whose work is of collector-quality are the sculptor George Pissarro and the pastelist Catherine Nicodemo, both of whom are friends, and both of whom reside in New York City.

George Pissarro is one of the best carvers of stone today. His works are both technically excellent and extremely sensual. George Pissarro can be reached at 1-212-541-5829.



Catherine Nicodemo is unusual for a pastelist, in that her technique is so unique that some initially think that the medium is something other than pastel. In addition, the works are often *much* larger than one would expect from a pastel. The works are imaginative



and subtle, generally conjuring up a story in the mind of the viewer, and the images frequently burst out of the confines of the traditional space indicated by the paper. Her work may be seen at <http://www.catherinenicodemo.com/>, and she may be reached at nafissa@att.biz.

7. Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2005 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.**
 - American businesses lose \$300 billion in revenues annually to competitive intelligence, economic espionage, inappropriate disclosure, and information theft.
 - LUBRINCO provides private sector consulting access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information.
 - Implementing an OPSEC program is likely to increase revenues for an at-risk operating group by \$75 million.
- **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, 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, 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 April 2005 **ÆGIS** (© 2005 **LUBRINCO** and FE&E), 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.