



ÆGIS journal

Addressing threats that affect your bottom line

Volume 12 Number 4, April 2009

From the case files of

LUBRINCO

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

and

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

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

Intellectual property being stolen or at risk? Call us!

This month's features:

- **Special Announcement**

1. **Asset Location and Due Diligence — Financial Plus**
2. **OPSEC, Economic Espionage, and Competitive Intelligence — Cyber-security or general protection of IPCI**
3. **Executive Protection — Tritium and laser sights**
4. **Technical Issues — Over-regulation of American companies**
5. **Real Stories from the Field — Policy based on bad statistics**
6. **Book and Product Reviews — Kaspersky Internet Security 2009**
7. **Subscription/Unsubscription/Copyright Information**

Special Announcements:

L. Burke Files will be speaking at 15th Annual East West Security Conference, 21 - 22 April in Dublin, Ireland <http://www.oceexhibitions.com/>

L. Burke Files will be speaking at the Offshore Alert Conference, 26 - 28 April in Miami, FL <http://www.offshorealertconference.com/OAC2009/home.asp>

1. Asset Location and Due Diligence — Financial Plus

While the recent Financial Plus Ponzi scheme in Los Angeles has all the elements typical of most similar frauds (e.g. no due diligence, unrealistic returns, religious element), it was unusual in that it went after non-wealthy Hispanics whom one might not think of as being potential dupes investors for an ambitious scammer.

Although this somewhat limited the scope of the fraud in terms of overall dollars – these fraudsters were more modest in their ambitions than was Madoff – it also limited the capacity of the victims to exercise due diligence: In most cases they had neither the financial background nor the resources to consider exercising any semblance of true due diligence.

As one victim noted, the ads were done by a Latino *star*, and a man of God – we are not sure which god, but Mammon seems a fair guess – started every meeting with a prayer. What more could one want?

What more could one want? This is an interesting question. On the one hand, it is unreasonable to expect the individuals in the Financial Plus fraud who lost their life savings, and in some cases their homes, to exercise the same level of due diligence we might have expected (but didn't see) from the Madoff participants. On the other hand, we were at that time going through a government rebellion against enforcement of onerous regulation, with the SEC faced with budget cuts if it chose to investigate violations, or even reported indications of fraud as in the larger Madoff case.

As a rule of thumb, most financial fraud is avoidable, just as many financial disasters are avoidable: We had advised clients against investing with well-regarded fraudsters like Madoff and Stanford, and one editor of this journal advised his wife, third quarter last year, to move her 401K to CDs since it was so apparent that the U.S was heading for a financial meltdown. But this rule of thumb holds only for people interested in and capable of protecting themselves.

If individuals are not capable of protecting themselves, and if the government is not willing to provide them legitimate protection, then the individuals are simply out of luck.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Cyber-security or general protection of IPCI

Some time ago a friend in the U.K. sent us a paper on cyber losses of intellectual property and critical information (IPCI). As best as we could discern, losses because of computer issues amounted to a not-insignificant seventeen percent of the total IPCI losses. This seventeen percent was enough to demand well over ninety percent of the funds spent overall to protect IPCI.

The more mathematically astute may feel that the response is somewhat disproportionate. And that more than ten percent of the resources should have been devoted to the other eighty-three percent of non-computer related losses.

While this might seem to be the case – actually, it is the case – in truth there are a number of psychological reasons for the disparity. For a start, security is generally aimed at protecting things on the inside from people on the outside. Firewalls, anti-malware software, and other such defenses fall into this mold and are therefore comprehensible and reasonable to those making such decisions. And while these prophylactic measures are mainly aimed at stopping the destruction caused by malware and cyber-attackers, they also prevent some loss of IPCI as a sort of unintended side benefit.

For the rest, corporate security is also generally aimed and protecting what is inside from what is outside, with all the rest – which is where the action is – generally ignored.

However, while it may be being ignored in the real world, it is not being ignored in the movies. When we recently saw the Tony Gilroy movie *Duplicity*, which is about corporate spies, we practically fell out of our seats when one of the characters mentioned that the OPSEC team was coming in to investigate. While we have seen many companies with competitive intelligence groups, we have never encountered a company with an OPSEC, or counter-intelligence group.

The movies, however, often condition society as to what is appropriate and inappropriate behavior. *Duplicity* may be a precursor to American businesses taking the \$300 billion avoidable annual loss of IPCI more seriously. Or not...

3. Executive Protection — Tritium and laser sights

Based on the feedback from non-professional readers of our review of the *XS Sight Systems Big Dot Tritium Express Set* in the August 2008 issue of *ÆGIS*, it is clear that many non-professionals do not understand the function of tritium sights and laser sights on handguns, somehow thinking that they will be of help during the few seconds duration of a gun fight. In fact, tritium sights and laser sights on handguns should be thought of more as offensive devices, not defensive devices.

If you are moving around in the dark trying to locate your enemy and get a bead on him, these will certainly help you, particularly for the first shot. Some, however, note that while you are circling around in the dark trying to draw a bead on your opponent, he is doing exactly the same, and if he gets behind you and sees the telltale glow of the tritium sight, you are toast. If you are in a secure position, and your opponent is exposed, laser sights will be of great help. Plus, it really attracts your attention if you happen to look down and notice several of them dancing around over your heart!

However, if something happens and you have to draw your gun and start firing, you will never see the tritium sight – you likely won't see the front sight at all – and never have time to use the laser.

While there are a wide variety of valid reasons to have tritium sights and laser sights on a handgun, none of these come into play when you are drawing your gun and firing back.

4. Technical Issues — Over-regulation of American companies

We vaguely recall having read an article that said the Hudson River was so clean that one could now eat up to four ounces of fish caught from it, per month, assuming one were over eighteen years of age and not pregnant. This factoid, which may or may not be true, encapsulates for us the conundrum of balancing regulation with necessity. On the one hand, we do not wish to make American corporations non-competitive with their foreign counterparts. On the other hand, we also do not want corporations doing bad things simply because they are “not illegal.”

A recent example of the latter comes from the Salmonella Typhimurium-laden peanut butter scandal of last year. In this case, the company apparently sent a sample of the peanut butter to a lab, as required by law. It came back as contaminated, which should have caused the batch to be destroyed and the source of contamination found and cleaned up.

Instead, the company sent out another few batches, until they finally got a lab result they liked, at which point they released the contaminated peanut butter. It is our understanding that the law had no clear statement that if the first batch came back as contaminated there was no do-over. Nor that the lab report the finding to the FDA.

The problem is that constraining regulations tend to be put into place because companies, acting on the principle that “if it is not illegal, then it must be legal,” have severely abused the public trust. Should all companies be saddled with onerous over-regulation because of the sins of a few?

An easy way to answer this is to get six jars (this gives you the same odds as Russian roulette) of peanut butter, one of which was on the recall list (which can be found on

<http://www.fda.gov/oc/opacom/hottopics/salmonellatyph.html>), and make a peanut butter and jelly sandwich using a mixture of all six jars. If you are a diehard opponent of all regulation, you will eat it.

We do not know what needs to be done to make it more profitable for American corporations to be doing their work in America (though lowering of the corporate tax rate to make the climate more hospitable – or even structuring it so that the U.S. became the world’s most favored tax haven – with a requirement that any individual remuneration over forty times the remuneration of the average employee be matched with an equivalent contribution to employee benefits, to discourage corporate executive pay abuse). We do, however, know that the American manager and worker are the best in the world, and that they represent a significant resource that should be better utilized. And that we should be able to order a peanut butter product with some assurance that it won’t kill us.

One suggestion has been that we follow the Chinese model, and give the government the ability to have business offenders put to death: If the CEO of a large corporation were summarily executed it would probably cause others to re-think doing bad, yet not illegal, things. However charming an idea this might be, it fortunately doesn’t fall under the rule of law.

A better idea might be to look at the *effectiveness* of regulation, rather than its volume, and to work on the development, of effective regulation that is free from politics and special interests, if such is possible,. And that after-the-fact regulation look at what would have been effective in preventing the problem, rather than acting merely as an administrative tax.

5. Real Stories from the Field — Policy based on bad statistics

We are always fascinated when we see policy being made based on bad statistics, particularly when the bad statistics are being used to push a political, religious, or philosophical agenda.

One recent example is the use of guns from the U.S. by drug dealers in Mexico. The claim has been made that 90% of guns confiscated from the drug lords originate in the U.S.

By our calculation, the actual number is closer to 15% (though we have seen some other calculations, which we cannot replicate, as high as 17%, so one might wonder where the 90% figure comes from. Well, of the roughly 35,000 weapons confiscated, only those that *might* have come from the U.S. are sent here for tracing. Of the roughly 11,000 weapons sent to the U.S. for tracing, roughly 6,000 were actually traceable, and of these 6,000 only 5,114 were found to have originated in the U.S. This is slightly over 85%, which has apparently been rounded up to 90% for mathematical simplicity.

Now, some of these weapons are likely supplied by the U.S. government as part of our support of Mexico's army and police. Certainly actual assault weapons – by which we mean fully-automatic weapons, not merely weapons that look ~~ugly~~ military – are simply not available for purchase by civilians in the U.S. They are, however, available from our government, from other countries in Latin America, from China and South Korea, and from a host of other countries that we are sure would be accessible to a drug cartel with \$40 billion in annual revenue. Certainly more easily available in the international arms market than buying them a few at a time in Texas!

There is no question but that American consumption of drugs has caused a serious drug war problem in Mexico. This drug war may possibly be a national security issue. Or it may not: An NPR interview, which can be heard at <http://www.npr.org/templates/story/story.php?storyId=102390087>, presented border mayors who claim that the drug war problem is overblown.

But, national security issue or not, it is not an issue fueled primarily, or even largely, by guns from America. Because of this, any American gun policy based on the bad 90% statistic would be bad policy indeed.

More to the point, any policy based on bad statistics will result in bad policy.

6. Book and Product Reviews

Kaspersky Internet Security 2009

Kaspersky Lab \$59.00

<http://www.kaspersky.com/> 1-800-406-4966

As anyone with a computer knows, we are drowning in a sea of spam and malware. The problem is exacerbated by the significant percentage of people with computers who have either no anti-malware software, or who don't bother to keep it current.

While we find this puzzling, we don't fall into that group, and, at the moment, use *Kaspersky Internet Security 2009* as our PC anti-malware program of choice. We have chosen this software for several reasons. It is an integrated program, containing a virus scanner (used by a number of other similar products), firewall, popup blocker, email scanner, the ability to protect your computer registry, and more. This is good, because you don't have to buy, install, and maintain multiple programs. It is easy to install: Just accepting the defaults will give the unsophisticated user good protection.

The program updates its databases regularly – it seems to do an update every hour or so – and uses less memory and system resources than other anti-malware programs we have used, which is a relief even on a powerful machine with a lot of memory.

Kaspersky Internet Security 2009 has a number of features, like parental control, which we didn't look at. A feature we only recently discovered – it is new in the current version – is a security analyzer, which looks at all your programs and tells you which ones are compromised, and where to get updates. We updated Java, as well as a few other programs, and got rid of the vulnerabilities.

It also scans for *rootkits*, which often modify parts of the operating system or install themselves as drivers or kernel modules. While some rootkits are malware designed as malware, others are by folks like SONY, whom one would have thought knew better, with its dangerous DRM rootkit (http://www.schneier.com/blog/archives/2005/11/sonys_drm_rootk.html).

While Kaspersky has business solutions, we only looked at tools appropriate for the home and small-office user. This program has our recommendation.

7. Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2009 by The **LUBRINCO** Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com), L. Burke Files (LBFiles@feeinc.com), and Terry Phillips (TPhillips@aegisjournal.com).

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

- **International asset location and due diligence.**
 - Anti-money laundering, financial fraud, and anti-corruption program development and training.
 - Statutorily mandated AML independent examinations for financial institutions and gatekeepers;
 - Investigation and location of missing or concealed assets, related to fraud, theft, and divorce.
 - Due Diligence to prevent fraud and loss, as well as validate potential business partners or potential business acquisition or merger.
LUBRINCO has significant expertise in performing Due Diligence in China, Central and Eastern Europe, Central Asia, the offshore financial centers, Latin America, and the Caribbean.
- **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.

- **Protection of executive 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, please send your request 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**, please send it as an attachment to an e-mail to editor@aegisjournal.com.

Submission of an article for publishing consideration 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 2009 **ÆGIS** (© 2009 **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.