



ÆGIS journal

Addressing threats that affect your bottom line

Volume 13 Number 3, March 2010

From the case files of

LUBRINCO

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

1-212-695-1759

and



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

1-480-838-1728

Have a BSA regulatory finding, or fear you might? Call us!

This month's features:

- 1. Asset Location and Due Diligence — OFAC compliance issues**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Steal me now**
- 3. Executive Protection — You need how many knives???**
- 4. Technical Issues — Useful computer stuff**
- 5. Real Stories from the Field — But I can get it cheaper...**
- 6. Book and Product Reviews — Vigny Walking Stick**
- 7. Subscription/Unsubscription/Copyright Information**

1. Asset Location and Due Diligence — OFAC compliance issues

Contributed by Eric A Sohn, CAMS, Senior Engagement Manager, Accuity (<http://accuitysolutions.com/> eric.sohn@accuitysolutions.com). Contributed articles do not necessarily reflect the viewpoint of AEGIS.

Did Credit Suisse's \$536 million fine by the Treasury Department's Office of Foreign Assets Control (OFAC) get your attention? Other than by not doing what they are alleged to have done, what should you be doing to comply with OFAC's regulatory sanctions programs?

First, it is critical to understand what OFAC wants and what is required. This can be accomplished by reading the details of each sanctions program posted on their website (<http://www.ustreas.gov/offices/enforcement/ofac/programs/>). You'll notice that it's not as simple as merely looking for the names on the OFAC Specially-Designated Nationals (SDN) list published on their site. If you're going to choose a commercial data vendor to properly cover the things you do need to screen your data for, make sure they understand too, by asking them specifically whether they enhance the SDN list, and if so how such enhancements are done.

Next, accept the reality that the overwhelming majority of the items that look like matches will, in fact, not be true matches. BNP Paribas did an internal study that showed that, when matching listed names exactly (as opposed to using 'fuzzy logic' or phonetic matching), they received 1,000 of these "false positive" matches for every legitimate match. This could be due to a number of factors, including the fact that many of the terrorists and drug traffickers on the SDN list (two of the largest categories of listed individuals) have common names. Also, since nothing requires a person to supply their full or legal name when conducting business (look at your credit cards and driver's license to see what I mean), OFAC screening entails matching incomplete data to incomplete customer data, a fact that will naturally pump up match rates and corresponding false hits.

Now, it's time to design your program and process. What information are you screening? And, why and how are you screening the data selected? You could screen your customer database, your employees, your contractors, your vendors...and/or every business transaction you're involved in. Is that necessary? It depends on your business. If you only deal with known counterparties, such as existing customers and vendors, you may potentially be able to skip some or all transaction screening. When will you screen? Best practice is to screen when you establish a relationship and when you conduct transactions, as well as re-screening your static data when the OFAC SDN list changes. However, if the nature of your business makes

it less likely to run into entities on the list, you may be able to perform periodic screenings on certain data, rather than screening on a more timely basis such as in screening transactions.

Who will review matches (resulting from the screening process) and who will be empowered to make decisions about vetting such matches? That's not such a cut-and-dried question. For example, you might allow front-line staff to perform triage, weeding out obvious false positives, but require them to escalate anything requiring greater scrutiny to compliance or legal staff (or a call to OFAC to get insight as to how to proceed) If front-line staff will perform triage, you should review their work on a periodic basis; you just figure out how often, by whom and how you will accomplish it.

Additionally, you'll have to decide upon how you will document every decision made by staff, as well as how and when upper management should get involved. And please, please, please - document all this, since it will help you greatly if there is ever an investigation into violations your firm was involved in.

Lastly, let's go back to our second point about costs. There are ways to reduce the size of your "data haystack" in your daily search for the needles. When selecting a screening solution vendor, you should inquire into the nature of false positive reduction tools and how they are used. Using them, of course, raises a host of other internal process questions, including: How are new system changes to reduce matches tested, and by whom? How are changes to rules or to processes used proposed, and approved - and by whom? And, since not all false positive reduction changes are without risk, what sorts of risks are acceptable in order to reduce our match rate (and your costs)?

2. OPSEC, Economic Espionage, and Competitive Intelligence — Steal me now

One might imagine that, in these difficult times, economic espionage would be on the rise. And, in fact, that is true. The cost of investing in theft is much lower than the cost of investing in research, and cutbacks in protecting IPCI have made it even easier to steal than it has been in the past.

This, then, is the perfect time for theft of intellectual property and critical information, and both companies and governments are taking advantage of this in all sectors.

Does this mean that your company is being robbed? Unquestionably! Is there anything that can be done about it? In theory, yes. In practice, your

company probably doesn't even have an inventory of its IPCI, or a program in place to protect these assets, so the answer actually turns out in most cases to be "no."

3. Executive Protection — You need how many knives?

People are often astonished by the amount of stuff we carry about us: Guns, knives, clubs, flashlights, *et cetera*. The other day someone asked us how many knives we habitually carried. The answer was three. Knives are a very personal choice in the business of personal protection services, and we can only give you *our* personal choices.

Our most-useful knife is a small knife used for opening packages, cutting strings, and other mundane tasks. While some like Swiss Army knives, we are uncomfortable with blades that do not lock open, and our preference is for the Spyderco LadyBug. The LadyBug has a blade of a bit over an inch, holds a good edge, and, in a color like yellow – or anything other than black – is definitely non-threatening. You can keep it in your pocket, or put it on a keychain.



The second knife is a rescue knife, whose main purpose is to break windshields and cut seatbelts after an accident. While rarely used, when you need it you really need it. Our preference is for the Smith & Wesson SW911, which we discussed in the February 2003 issue of *ÆGIS*. There is a new version of this knife available, the SW911N, which we will discuss soon in another issue.



The third knife is a utility knife. While less-used than our little knife, it is invaluable for larger jobs, and great for cutting steaks if the knife at the restaurant isn't sharp. While we carry a Mission Knives MPF1-TI, discussed in the July 2006 issue of *ÆGIS*, this category of knife is REALLY where personal preference comes in. We know many who carry the excellent Smith & Wesson SWHRT, or any of a variety of excellent knives from Spyderco, plus a host of other fine manufacturers.



So what knives do *you* need? Only you can decide that, but the above three categories should certainly give you a starting place to figure out what you might actually need, and to make appropriate choices.

4. Technical Issues — Useful computer stuff

There are a number of programs and services that we have found useful over the years. Let us start with support issues. On several occasions over the past year or two we have had computer issues, and needed outside help. When we called Microsoft, it was something like \$150 for that incident. Instead, for support we opted to use iYogi (<http://www.iyogi.net/>). For \$139 a year you get unlimited access to their group of 500 Microsoft certified technicians. They have saved my home computer on several occasions. They throw in McAfee anti-virus software, but we prefer Kaspersky. iYogi includes a bunch of optimization software, but we prefer System Mechanic.

System Mechanic (<http://www.iolo.com/>) allows you to automate optimization of your system. It includes software that does almost everything, including defragmentation of your hard drive, optimization and compaction of your registry, and virtually everything else of which you can think. It should make you machine faster.

Password Safe (freeware at <http://passwordsafe.sourceforge.net/>) generates and stores passwords. You can use it to load Web pages and enter your user ID and password. While you need to know the Password Safe password, you will not need to remember the lengthy random passwords it generates.

SpinRite (<http://www.grc.com/sr/spinrite.htm>) checks your hard drive to make sure that each track can be read and written. It moves data from bad sectors to good sectors. If your drive fails, there is a good likelihood that SpinRite will be able to repair it, which is what happened when a hard drive developed bad sectors in the boot section. While System Mechanic has a similar function, we use this.

iBackup (<http://www.ibackup.com/>) allows you to automate on-line backup of your data. For \$9.95 a month it gives you 10 gig of storage. Our system backs up all changed data at 1am.

There are several good disk defragmentation programs, including one in System Mechanic. The best is probably Diskeeper (<http://www.diskeeper.com/landing/landing30.aspx?RIId=11200&Apid=PPS0005174&gclid=COvh-Zv19Z4CFchn5QodXykvKA>) with VOPT (<http://www.vopt.com/>) running second. Diskeeper runs constantly, and appears to use no resources automatically, the most-current version, which

we will discuss more fully, soon, in another issue, is claimed to eliminate about 85 percent of fragmentation before it happens. The technology is somewhat magical to us as laypersons.

Our personal favorite firewall/anti-virus software is Kaspersky Internet Security 2010. (http://usa.kaspersky.com/products_services/internet-security.php?icid=50000028). The antivirus definitions update frequently during the day, and we run a complete scan at 3am, including looking for rootkits. It includes the ability to scan your programs to see what needs to be updated for security reasons.

Out of concern for the possibility of my computer being stolen, we have installed PC Phone Home. There is also a version for the Macintosh. (<http://www.brigadoonsoftware.com/pcphonehome.html>). The buried software sends messages to an e-mail account of your choice with the IP address of any internet logon, allowing the police to track the location of the device.

To protect our data, we use encrypted virtual drives, in this case Private Disk (<http://www.private-disk.net/>). If our computer was stolen there would be no useful data available. To send encrypted e-mail and encrypted files we use PGP. We actually use one of the open PGP programs, FileCrypt Desktop (<https://www.veridis.com/pgp/products/filecrypt-desktop.html>).

We hope you will find these to be as useful as have we.

5. Real Stories from the Field — But I can get it cheaper...

One of the fascinating pieces of business is the cost of goods and services, with there often being several options at several prices. We face this issue frequently, because the work we do at LUBRINCO often seems similar to what others offer. But is it in fact the same?

A good example of this is independent testing and review of AML programs, which is mandated by law. There are a lot of firms that do this, and many of them are extremely competent, and cost less than we do. In fact, however, we do not do independent testing and review of AML programs *per se*. Rather, we do independent testing and review of AML programs where there is a concern regarding possible regulatory action, and help when a regulatory action has taken place.

Should this make a difference in your thinking? Yes. If all you want is to be able to demonstrate a bare minimum of compliance, then we would suggest that you should definitely *not* hire us: You can get the job cheaper elsewhere. On the other hand, if you want to make sure the regulators know

your firm is actually doing the proper job within your AML compliance program, rather than merely giving the task lip service, we should be among your first choices. And if you have actual concerns about a possible regulatory action, and avoiding them, and addressing them, then we should be at the top of your list.

In a recent case, a company solicited two bidders for independent AML program testing and review. One firm provided a bid for about \$6,000 for the job. The other was an estimated \$40,000. The company accepted the higher bid. The evaluation produced a number of troubling areas, all but one of which was rectified. In reviewing the work product provided by the independent provider selected, the regulatory examiners found that the program review identified and remediated all of the issues identified except for the one minor issue that was then still outstanding at the time of their examination. There was a minor action over the one outstanding issue, which was subsequently dealt with.

Was the investment of the extra \$36,000 worthwhile? Well, it saved the institution a huge amount of additional time, money, and grief. Based on this, we would conclude that it was definitely worth it.

6. Book and Product Reviews

Vigny Walking Stick

\$100.00

[http://www.combatcanes.com/ Info@Combatcanes.Com](http://www.combatcanes.com/Info@Combatcanes.Com)

As readers know, we have a particular fondness for walking sticks, canes, and umbrellas for defensive use. We were, therefore, excited to discover that Dirk Folmer of Combat Canes was making a Vigny cane replica. The original, of which we know of no existing sample, was made of Malacca, with a round metal top. Dirk's cane is made of Saynite, and the sample we have is black, with a large black ball on top, which is very comfortable to hold. It is slim, handsome, elegant, and non-threatening, which are desirable qualities in a combat cane.

While the craftsmanship is excellent, we have some issues with the weight of the cane. Malacca is very light, and we suspect that the top piece on the original was relatively light, because the whole theory of the Vigny school of using walking sticks was to have a light, fast, cane. This modern replica is a very substantial cane: It weighs over a pound, which makes it about three times as heavy as our Malacca, and heavier even than our Welsh Blackthorn, which is too heavy.

To put it into perspective, look at the weight of a sampling of our walking sticks:

Malacca cane 204 grams.

- Mahogany cane 276 grams.
- Ash cane 334 grams.
- Welsh Blackthorn cane 434 grams (too heavy for us and our target audience).
- Saynite cane 462 grams.

Does this matter? Well, we find it is too heavy to comfortably use for walking (granting that we are fairly frail), and WAY too heavy to generate the needed amount of speed, even using the ferrule end. What needs to be done? Somehow 100ish grams needs to be cut from the weight, to get it to be not much more than 350 grams. We suspect that the top weighs substantially more than 100 grams, and that by using another material, or changing the shape of the top, the weight can be lost. While the ball itself is extremely comfortable in the hand, if it could be made another shape, and 100 grams cut off, it would then be ideal.

Dirk Folmer, an extremely responsible and responsive person, listened to our concerns, and is working to reduce the weight by 100ish grams. We believe this will make his Vigny cane an ideal tool, and we strongly urge readers to contact him to order a walking stick.

7. Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2010 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 and program reviews 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 March 2010 **ÆGIS** (© 2010 **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.