



ÆGIS journal

Addressing threats that affect your bottom line

Volume 12 Number 3, March 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

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

This month's features:

- **Special Announcement**

- 1. Asset Location and Due Diligence — AML outside examinations**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Ghostnet**
- 3. Executive Protection — Gun safeties**
- 4. Technical Issues — Certifications in the Security Profession**
- 5. Real Stories from the Field — The two-second rule**
- 6. Book and Product Reviews —**
A Military Guide to Terrorism in the Twenty-First Century
- 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.oceceexhibitions.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 — AML outside examinations

As longtime readers know, we have a long history of locating concealed assets in fraud (which largely move from the United States to exotic places overseas), and, somewhat more recently, of developing AML programs (largely in exotic places overseas). Our goal is to develop AML programs that are not only compliant, but that also address the crimes they are supposed to detect, and that don't impede the flow of business.

Considering the nature of our domestic and international fraud and AML experience, it was only a matter of time before we moved to the arena of performing the mandatory independent AML examinations required of many financial gatekeepers, and the repair of defects found. If you have such a statutory requirement, we hope you will engage us to assist you with this.

It is important to understand that AML is a core competency for us, so that your team will be made up of experienced people. And that we bring to it not only an understanding of compliance issues, but also an understanding that AML is about fraud and other financial crimes. This means we can help assure that you are not hit with a cease-and-desist order for having a program that was developed for form rather than substance; that was aimed at merely being compliant rather than at stopping crime.

Besides those financial gatekeepers that at present have AML requirements under the Bank Secrecy Act, there are also a host of industries that will soon have these requirements to meet. The most vulnerable of these include hedge funds, futures commission merchants, private equity funds, and unregistered investment funds.

If your company falls into these categories, we hope you will hire us, so you can be ready to drop these systems in place when these requirements are extended to you.

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

If you haven't just fallen off the turnip truck, you know that cybercrime is a serious and increasing problem. Many governments consider cyberspace to be a strategic target, and devote serious resources to attacking these targets (the United States, Israel, and the United Kingdom being considered the most sophisticated, with China not far behind). And many criminals, both organized and independent, consider cyberspace to be a legitimate target for their criminal enterprises.

In truth, however, while we all buy anti-malware programs for our machines and centers, and read about one worm or virus or another, most of us have little understanding of how this all works, or its implications. A new report from the Munk Centre for International Studies at the University of Toronto and The SecDev Group in Ottawa will help put this in perspective.

The report, *Tracking GhostNet: Investigating a Cyber Espionage Network* (<http://www.f-secure.com/weblog/archives/ghostnet.pdf>), shows that their investigation, originally aimed at what was believed to be Chinese attacks on Tibetan government in exile computers, “ultimately uncovered a network of over 1,295 infected hosts in 103 countries. Up to 30% of the infected hosts are considered high-value targets and include computers located at ministries of foreign affairs, embassies, international organizations, news media, and NGOs.”

While the story of GhostNet is interesting in itself, it is significant in that “It demonstrates that the subterranean layers of cyberspace, about which most users are unaware, are domains of active reconnaissance, surveillance, and exploitation.” If you are involved in cybersecurity, this is a must-read.

3. Executive Protection — Gun safeties

A friend recently saw a security video on television in Hawaii in which a jewelry store was being robbed (he didn't know when or where it took place). The owner had been robbed before, and had gotten a gun, which to my friend's untutored eye appeared to be a double action semiautomatic pistol.

On this occasion, the bad guy, looking suspicious and acting suspiciously, was moving around the store. The store owner drew his gun and waited. Eventually the bad guy pulled a gun from his pocket and turned to face the store owner. Seeing the store owner's gun the robber started firing, emptying his gun into the store owner (who, by the way, apparently lived). And the

store owner? Well, apparently in the stress of the moment he forgot to disengage the safety on his weapon, so it wouldn't go bang.

The function of a gun safety on older semiautomatics was to insure that the gun would not discharge if dropped. The design of recent modern semi-automatics prevents that from happening. In addition, the safety also functions as a de-cocker, lowering the hammer safely when the gun is cocked. Glock has a safety built into the trigger, so that it won't discharge unless you are, in fact, pulling the trigger. People who carry single-action semiautomatic pistols with a round in the chamber and cocked carry them with the safety engaged, as the light pressure needed to pull the trigger demands this. People who carry double action semiautomatic pistols carry them with the safety disengaged (and tend to have a gunsmith remove other unsafe safeties likely to get them killed, like a magazine disconnect).

People with modern revolvers don't face this issue. Modern revolvers have a mechanism that will prevent discharge of the weapon if dropped.

The bottom line is that under stress you tend to act differently on the range than you will in a violent confrontation, and that we feel that a gun you carry should have as few impediments to going bang as possible.

On the other side, some make the case that you *want* a safety in case the gun is wrested from you, and your assailant doesn't know enough about guns to disengage it. This is the basis for the enthusiasm of those not familiar with guns and their use for "smart" guns that will only fire if *you* are the one pulling the trigger of your gun. As an example, modifications can be made on Smith and Wesson revolvers (<http://www.tarnhelm.com/magna-trigger/gun/safety/magna1.html>) that prevent them from firing unless you are wearing a magnetic ring. While "smart" guns appear to have some merit, we believe the risk outweighs the merit, and that "smart" guns increase the likelihood of your ending up dead. Because of this risk, you will see that police departments will reject use of "smart" guns, and so should you.

While this editor favors revolvers, if you carry a double action semiautomatic that has an external safety, and don't want to find yourself wondering why it doesn't go bang when bullets are whizzing your way, think long and hard before engaging it.

4. Technical Issues — Certifications in the Security Profession

Contributed by Jerry J. Brennan, Managing Director & Founder of Security Management Resources (<http://www.smrgroup.org>) (Jerry@smrgroup.com). Contributed articles do not necessarily reflect the viewpoint of AEGIS.

Frequently, we are asked if a particular certification would improve an individual's career and marketability. Unfortunately there is no easy answer. As an industry we have not done a very good job of defining the various security job functions in a realistic fashion. Further complicating this is the arbitrary and capricious nature of the position descriptions published by security professionals when they are looking for staff. We continually see requirements in position listings that have no relevance to the role they are recruiting for. This makes it more difficult for the certifying agency to identify which body of knowledge they will measure.

Recently, Security Jobs Network, Inc. reviewed 40,300 professional level openings that were collected and listed on their website from Jan 1999 to mid July 2008. The CPP designation was chosen because it is one of the older and most recognized designations in the industry. It also and represents that its holders are "Board Certified in Security Management." So how did the marketplace respond?

Year	Total # Listings	CPP	%	
2008	2187	110	5.02%	*22-Jul-08
2007	3431	147	4.28%	
2006	3741	139	3.72%	
2005	3709	151	4.07%	
2004	4316	146	3.38%	
2003	4073	109	2.68%	
2002	4349	120	2.76%	
2001	4288	110	2.57%	
2000	5625	166	2.95%	
1999	3453	84	2.43%	

There is no silver bullet when it comes to advancing your career. Most organizations seek to fill positions with qualified individuals who have a record of accomplishments in the security management focus area of the position being filled. In addition, organizations like to hire people whom they believe will fit into the organization's culture and who can best engage

effectively with the managers and individuals with whom they will need to interact. The higher up the career ladder you progress, the more true this becomes. Do you see the world's leading organizations require their "C" level executive to be "certified" in a particular field? How often have we seen organizations recruit senior level government executives to head security organizations? Are they any less capable leaders because they don't have a particular certification? The point we wish to make is that in general, certifications were designed to measure someone's knowledge in a specific practice area. These tended to be in relatively narrow areas of expertise and also required a specified level of continued education to maintain the certification. This is true across many careers fields from medicine to automotive repair.

These can be valuable programs to advance the sector they represent. The common threads that we have observed for those certification programs that become standards within their professional field, are: They are integrated into the our recognized degree and/or certificate educational programs; have specifically defined the body of knowledge they seek to measure; stay focused and up-to-date in that specialty field; are generally used to measure knowledge in practicing or operational level positions within a field or career path and are widely accepted by the hiring organizations because their materials are relevant to position specific job requirements.

Our recommendation is to choose your educational and certification programs carefully. Ensure that the program has clearly defined course material and test objectives that realistically measure relevant knowledge in a given practice area. For those candidates in the beginning or mid-point of their career, certifications can help set you apart from other candidates, however, no certification is an indication of your ability to lead a program at a senior level of management and any such claim is misleading. Having a lot of initials following your name will not advance your career if you cannot demonstrate a record of accomplishments, maturity, competence, and a wide range of interpersonal, non technical skills to a hiring authority.

5. Real Stories from the Field — The two-second rule

Recently a gun ~~nut~~ enthusiast of our acquaintance called, and read an excerpt from a book which recommended, in essence, that your gun should be accessible within two seconds at all times. Since the average American has a violent encounter once every eighty-five years, this makes no real sense for the majority of us.

However, roughly 1.5 million heart attacks occur in the United States each year with approximately 500,000 deaths. Costs related to heart disease exceed 60 billion dollars per year. And, more to the point, chewing (not swallowing) an uncoated aspirin right away, at the first sign of chest discomfort or distress, can reduce the amount of damage to the heart muscle during a heart attack.

As it happens, we don't have a gun accessible to us within two seconds – or two minutes, for that matter – but we always carry aspirin with us, and probably have it accessible, if not within two seconds, certainly in under fifteen seconds. In general we carry easily soluble chewable baby aspirin, and give (or would take) four of these when needed.

If you are concerned about your personal safety and survival, we would recommend that you add carrying aspirin to the list that includes fastening your seat belt, not smoking, not having unprotected sex, and not drinking (or using a mobile phone) while driving.

6. Book and Product Reviews

A Military Guide to Terrorism in the Twenty-First Century

U.S. Army Training and Doctrine Command

182 page Acrobat file

<http://www.fas.org/irp/threat/terrorism/index.html> or

<http://www.au.af.mil/au/awc/awcgate/army/guidterr/>

One of the things the military does well is research. *A Military Guide to Terrorism in the Twenty-First Century* is certainly an example of this, and will be of interest to anyone who deals with terrorism or is interested in terrorism. It is a comprehensive, inclusive overview.

While by definition aimed at the military, this does not, in fact, limit its utility. As an example, those who deal with protection will find that Appendix A, which deals with the terrorist planning cycle, will serve as a good refresher, and a reminder of the importance of regular surveillance operations against their own facilities or principals.

If you have an interest in knowing about terrorism, this free download is a great resource with which to start.

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.
 - Statutory mandated AML independent examinations for financial gatekeepers
 - 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.
- **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 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 March 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.