



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 2 Number 10, October 1999

From the case files of

The LUBRINCO Group
<http://www.lubrinco.com/>

and

Financial Examinations and Evaluations, Inc.
<http://www.feeinc.com/>

Concealed assets in fraud, theft, and divorce? Call us!

This month's features:

- 1. Due Diligence — Background checks on doctors**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Keeping insider information off the web**
- 3. Executive Protection — Getting your client to listen**
- 4. Technical Issues – The politics of encryption / The Skimmer**
- 5. Real Stories from the Field — Bank and the volcano**
- 6. Book and Product Reviews — Online Competitive Intelligence**
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Background Checks on doctors

This article is beating a point to death about doing background checks before you hire someone. A new book, *Blind Eye: How the medical establishment let a doctor get away with murder*, documents the story of not just one, but 80 or more deaths. This makes Dr. Michael Swango the nation's worst serial killer. Swango is currently in jail, not for murder, but for filling out false paperwork! Swango had had at least one conviction for poisoning and spent a year and a half in jail, but none of this was reflected in the state's medical licensing board records; none of this was reflected in the AMA data base; and not one of the hospital that hired him after his release from prison did a PUBLIC RECORDS background check. Not one questioned him on the 18 month gap in his resume. Aaaaah! Swango continued to kill at those hospitals, including a VA hospital. When he was discovered, the hospitals apparently were more concerned about being sued for wrongful termination than about the murders he had committed. These same hospitals also compounded the problem when they wrote glowing letters of recommendation for Swango, so Swango could work at other hospitals.

We cannot recommend strongly enough that every single hospital and medical practice *not* depend upon the medical establishments records. They are useful, but are in no way comprehensive. Public records must be checked in all of the jurisdictions where a physician has practiced including local courts, county courts, and federal courts. This is for doctors that are going to be employed, affiliated with, or have requesting privileges at a hospital or other medical facility. The few hundred dollars a hospital or medical practice would spend on a background check may well save tens of thousands of dollars later.

Most hospitals insist that they are insured for such risks, and they are. However, I know of two hospitals that began comprehensive background checks on their physicians and cut the hiring liability portion of their insurance premium by \$75,000 and \$280,000 respectively. Further, in the five years one hospital has been doing this no suit for hiring liability has prevailed. In the other hospital no hiring liability suits have been brought. Even so, the deductible on these policies are \$200,000 each. The hospitals spend \$500 and \$700 a month on background checks and now proudly crow to the public that they have the best physicians in the business. Hello, Marketing (I mean patient intake)?

In fine, you shouldn't be lulled by the fraternity of doctors. They are not all honorable. They are not all equal. They are a cross section of the population. Most are excellent and care to their very core about what they do. At least one, however, used his license as a license to kill.

8. OPSEC, Economic Espionage, and Competitive Intelligence — Keeping insider information off the web

In CI we want information. Sometimes that information is not available. This can be for any number of reasons, including the fact that, from the company's point of view, it is insider information which should be protected, and *shouldn't* be available.

Sadly, many people are overly helpful and have more ego than common sense, and, in some cases, information (which they legitimately know) becomes like money burning a hole in their pocket. Even more sadly, many of these people find their way onto technical forums on the internet.

Internet forums are a mixed bag. They can be extremely helpful in terms of getting information on how to do things, soliciting the opinions of others, and in getting people to share opinions and expertise. The opinions expressed need to be taken with a grain of salt, of course, as the mere presence of an opinion, or of a position forcefully stated, does not necessarily indicate real expertise.

None the less, most forums end up having a number of participants who work for companies involved in the forum's area of interest. These people are there because the forum's subject interests them, and because they wish to share their knowledge. This is, in fact wonderful, and can be extremely helpful for the other participants.

From a corporate point of view, however, it can be a problem. On occasion the participants become too involved in the discussions, and forget what information is confidential. They may then identify themselves publicly as working for a specific company, or, in some cases, may selectively do this in private emails.

In either case, it will often become obvious to the careful observer that some participant has expertise, and for which company he uses this expertise. Once that is established, it is not uncommon to see these participants being drawn out by questions until they are revealing — often to the public at large, facts which can only be considered protected insider information.

How do you protect yourself from this? For a start, make sure your company has a written policy dealing with information given out during outside use of the internet. Second, have someone monitor the appropriate forums. Be aware that it may be best to have an outside company do this, as it can take, in our experience, somewhere between a half hour to an hour a day to monitor a handful of forums of interest. While this may or may not seem like a lot, most companies do not have the resources to allow a staff person spend an hour a day surfing the net. After a fast start, the monitoring tends to taper off.

And what do you do when you discover someone who has stepped outside the bounds? You have their manager explain to them that this behavior is unacceptable because it places the company at risk, and must be stopped.

Note, by the bye, that monitoring these forums allows you to do more than merely identifying information leaks. It also allows you to identify valid concerns on the part of your customer base: Concerns of which you might otherwise be unaware.

9. Executive Protection — Getting your client to listen

Protective service often boils down to identifying a danger and doing something about it, or, as has often been said “See something, tell someone, do something.” Can surveillance be detected? Can a threat be assessed or realized? When a risk is identified, it is then up to the operative to make the protectee aware of the risk, and of the need to take appropriate action. If the protectee will not listen, then what is the point of being there? If you are not listened to on one occasion, you will be ignored on other occasions, in reference to restaurants, cities, destinations, driving, schedules, drivers, personnel, inclement flying conditions, threat situations, and all else.

The difference between calling yourself a bodyguard and actually being an effective professional is whether you can persuade the client that something is wrong and to take appropriate action. Will you or can you say to a driver “You will NOT drive this car. Sir, I am NOT willing to let the driver handle this vehicle.” Will you or can you say to a driver “Slow down, or stop the car and I will drive.” Be aware the client may well say “Get out yourself, you’re fired.” If that be the case, then go, as you have outlived your usefulness.

Your main obligation as a protective agent is to assert yourself in a situation you believe to be a danger to the protectee. If a bodyguard is a former government agent or law enforcement agent with protective service experience, then they should have the confidence of that experience to navigate these treacherous interpersonal waters. For those who have not had

protective service experience, or whose experience is a week's course with a poorly chosen training company, and who cannot read the situation and assert themselves, the end result can be catastrophic. Think of the case of Princess Diana. How many cases are there of which we are *not* aware?

Can YOU say to a client? "Sir (or Ma'am), we are getting into a situation that is dangerous, and you need to stop and listen to me before we go any further. I am tasked with the prevention of serious injury and death, and you are paying me to give you this advice, and to get you to follow it."

If a client is not willing to adhere to your professional advice, then there really is no point in your being there. And if you are the client, and you are not willing to listen to your protective agent, you are either wasting a lot of money for show or you are putting your life — and possibly the lives of those around you — at risk.

10. Technical Issues — The politics of encryption / The Skimmer

The politics of encryption

Although international encryption policies are restrictive and outdated, these policies may be relaxed or made obsolete in the near future. Several countries have loosened their encryption laws this year. France has significantly relaxed its encryption policies, now requiring simple declaration rather than prior authorization to supply and use encryption systems. Germany has changed its stance on encryption, encouraging the technology as a way of protecting personal liberties. Germany's attitude towards encryption could represent a trend: "Law enforcement will begin to see that strong encryption prevents more crimes than it conceals." The U.S. is heading toward the elimination of government encryption laws, based on the outcome of the Bernstein vs. Department of Justice case in May. In the case, Professor Bernstein won by arguing that not being allowed to post encryption algorithms on the Internet for his cryptography course was a violation of his right to free speech. In addition, U.S. export laws may be relaxed if Congress approves legislation such as the SAFE Act, although it is likely that access keys, to be held by the government, will still be required. Currently, the most encryption-friendly area in the world is Latin America, which appears to have few laws that limit the export, import, or use of encryption technology. By contrast, Russia and some former Soviet states have some of the most restrictive encryption policies. All of these policies may soon be irrelevant because fast-paced technology is providing ways around the laws.

The Other side of the coin

Department of Justice officials last week defended their request that Congress update laws governing search warrants that reflect the growing use of encryption technology. The proposal asks Congress to grant federal agents greater access to sealed warrants, signed by a judge, permitting them to enter private property and install devices in private computers to override encryption software. More than 250 congressmen have already co-sponsored a countermeasure that would encourage the use of encryption and proscribe a proposal from the Clinton Administration to mandate a so-called back door in computer systems, one which would allow investigators to sidestep encryption. Not everyone agrees. Michael Fromkin, a law professor and encryption specialist at the University of Miami, insists that the agency's request would diminish privacy and allow police greater access to private property. Law enforcement officials counter that investigators will be ineffectual unless empowered to collect encrypted data. Justice Department officials emphasize that, like wiretaps, such warrants would be under tight control by the courts.

The Skimmer

There is a really neat little item made in Taiwan about the size of a beeper. When you use your credit card to pay a bill, the Skimmer is then put into action. On the way to the register or out of your sight, someone can simply run your card with the magnetic strip through the Skimmer, which captures all of your information, including name, address, telephone number, card number, and credit limit. The Skimmer holds about 100 entries and the information can be downloaded into any computer.

Crooks can then use blank cards and become you in minutes. The Skimmer also has an erase button on it, so if caught, the crook simply hits the button and all the information is gone, leaving no evidence on which to prosecute. In the past, skimming your credit card required at least a laptop computer and a card reader.

11. Real Stories from the Field — Bank and the volcano

This story was relayed to one of our editors by a senior finance minister in the Caribbean. A while back, Monseratt suffered devastating eruptions from the volcano that formed the island. The island was covered in ash and rubble from the eruptions. Many of the island's banks are located inland, away from the coast and the destructive power of hurricane-generated storm

surges. Unfortunately, this put them closer to the ash and debris fall. One of the region's most prestigious banks was completely covered. The bank's officers were upset, but not worried about the vault and safety deposit boxes: As long as they were buried they were safe. After the volcano calmed down, experts were brought in to determine how best to access the vault and retrieve the safety deposit boxes and currency held in the vault. After much examination and decision making, the dig began. What they found astonished them: While they were using the most modern equipment to access the vault, locals using picks and shovels had cleaned out all of the bank's currency and every single safety deposit box. The locals gained access via a tunnel dug by hand.

12. Book and Product Reviews

Online Competitive Intelligence

Helen Burwell

Facts on Demand Press \$25.95

<http://www.brbpub.com/> 1-800-929-3811

This is a great book for the practitioner of competitive intelligence and those responsible for information security. The book takes the reader through the process of understanding competitive intelligence (CI) and CI uses, including using CI on your own company. It also has a thoughtful layout of how to plan a CI information gathering investigation. Planning may sound trivial, but without a plan and an objective how do you know when you have found what you need or when you are finished? The book is full of useful computer tools, internet tools, many a useful link. As a veteran investigator, editor, and book reviewer, I rarely come upon something that is both new and useful. Buy this book; read it; use the information, or be left behind.

13. Free-Subscription/Unsubscription/Copyright Information

•• AEGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 1999 by The LUBRINCO Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com) and L. Burke Files (LBFiles@lubrinco.com).

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

- **Protection of trade secrets and intellectual assets.**
 - Anti-economic espionage.
 - OPSEC: The identification and protection of information that would give your competitors and adversaries an advantage.
- **International financial investigations and due diligence consulting.**
 - Location and recovery of missing and hidden assets.
 - Establishing business relationships and strategic partnerships in Central and Eastern Europe, the offshore financial centers, Beijing and Shanghai, Central Asia, and Latin America and the Caribbean.
 - Anti-money laundering and financial fraud requirements under the *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001* and the *EU Revised Money Laundering Directive of 2001*.
- **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 **The LUBRINCO Group** and its services, or for the archive of all past issues of ÆGIS e-journal in PDF format, please go to <http://www.lubrinco.com/>.

To sign up for a **complimentary subscription** to ÆGIS e-journal or the ÆGIS e-journal PDF notification list, go to <http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to ejournal@lubrinco.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, follow the instructions on the mailing you received, or send an e-mail to ejournal@lubrinco.com.

If you know of anyone else who should be receiving ÆGIS e-journal, please send their e-mail address to ejournal@lubrinco.com.

If there is a topic that you would like to know more about, send it to ejournal@lubrinco.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* e-journal, send it as an attachment to an e-mail to ejournal@lubrinco.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* e-journal constitutes a license to The LUBRINCO Group Ltd, Inc., 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* e-journal, you may do so freely as long as appropriate source, copyright, accreditation, and link to the LUBRINCO website is included. This should be in the form

Article Title, from the October 1999 *ÆGIS* e-journal (© 1999 LUBRINCO & FEE), to be found at <http://www.lubrinco.com/>.

ÆGIS e-journal 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* e-journal 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* e-journal.

Please be safe, and be smart.