

ÆGIS



Addressing threats that affect your bottom line

Volume 8 Number 9, September 2005

From the case files of

LUBRINCO

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

and

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

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

Need protection in Bogotá or other high-threat areas? Call us!

This month's features:

- **Special Announcement**

- 1. Asset Location and Due Diligence — You don't say...**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — And the Chinese have arrived!**
- 3. Executive Protection — Profiling**
- 4. Technical Issues — Hurricane activity for the next decade**
- 5. Real Stories from the Field — ICE: In Case of Emergency**
- 6. Book and Product Reviews — *With Winning in Mind***
- 7. Subscription/Unsubscription/Copyright Information**

L. Burke Files will be presenting a two day seminar on *Employee Fraud*
Queretaro, Qro. Mexico October 6&7 for IPACITEFO <http://www.ipacitefo.com/>

L. Burke Files will be presenting a one day workshop on *Fraud Prevention for Corporate Treasury Professionals* at the Association for Financial Professionals annual conference in San Antonio, Texas, on October 9th. http://www.afponline.org/pub/conf/annual_conference.html

1. Asset Location and Due Diligence — You don't say...

“You have the right to remain silent.”

That phrase is familiar to almost everyone – particularly those who have been arrested – in the past four decades. The so-called “Miranda warnings” are routinely pronounced by real and fictional police officers every day. The Fifth Amendment to the U.S. Constitution guarantees Americans the right against self-incrimination. But TV cops often say those magic words sooner than the law demands, since the protection only applies to the interrogation of suspects in custody. There are myriad exceptions, too, such as the “excited utterance” rule or a deathbed confession. Laws vary in this country from state to state.

There are some general rights you have under the Fourth Amendment, besides that of remaining silent. While you can be searched with relative impunity at borders, before boarding a commercial airline, or by private security personnel as a condition of entry onto private property, you can otherwise just say “No.” Thus in New York City, when random searches of people entering the subway – a timely response to the problem of this being an election year – were instituted, it was made clear that if you didn't want to be searched you could say, as politely as is humanly possible, “Officer, I do not consent to any searches. I'm going to exit the station,” and turn around and leave the station.

Much the same holds true with identifying yourself. While you must produce identification on demand if you are driving on a public roadway, in most circumstances you needn't do so. If you are being issued a summons, even for some minor offense, and do not choose to identify yourself, you may be held until you are identified by other means, so that it is clear that the summons has been issued to the right party. And in cases where an area has been closed off for crowd control purposes – say because of a parade – for all but residents or those with legitimate need, you may be asked for ID to confirm your residence. While you can certainly refuse to show your ID, the police can certainly refuse you admittance.

Keep in mind, however, that the police are no more lawyers than are we, do not like resistance of any sort, may not be experienced enough to deal with the event, and may decide to search you in any case. If this happens you should not resist, but, rather, say, again as politely (you don't want this to escalate to violence against you) as possible, "Officer, I am not resisting and I do not consent to any searches." You will have the opportunity to deal with the legality or illegality of the search later.

As common sense should tell you, the police may conduct a search without a warrant if you give consent, if there is some illegal item in plain view, if you are being arrested, or if there is an emergency situation requiring swift action to prevent imminent danger to life or serious damage to property, or to forestall the imminent escape of a suspect or destruction of evidence.

The most common concern of corporate lawyers on this subject is what company documents are protected. Unlike government agencies, a private business cannot stamp "Confidential" or "Top Secret" on its papers. Even the best physical locks or encryption software will only stop unauthorized snooping. But what can you do when a government agency wants to take a peek at something you'd rather keep hidden? Turn them over. Obviously, within the constraints of legal requirements to store certain documents for a certain period, if you have a written policy on how long other documents, electronic and paper, must be kept, and documents are destroyed on that schedule, the legitimately destroyed documents are non-discoverable.

We are not lawyers, nor do we play lawyers on television. But here are some general principles for when a police officer or a prosecutor or a judge asks you questions you do not wish to answer.

- No one is above the law.
- Ignorance of the law is no excuse. We might not always know what the law says, but we are subject to it nevertheless.
- Once the judicial system has made a final ruling, we are legally bound by it, unless the decision is reversed or overruled by a higher court at some future date.
- Many citizens enjoy special privileges. The law protects most conversations between attorneys and clients, doctors and patients, clergy and confessors, as well as between spouses. However, all of these are subject to some limitations. For example, a lawyer may not advise someone to commit a crime with impunity, independent of whether the conversation is protected.

As an interesting side note, the California 2nd District Court of Appeals ruled on August 15th in favor of an attorney who made anonymous calls to police implicating her former clients in an alleged car theft ring. The appellate panel found that, in doing so, the attorney didn't violate her clients' constitutional rights, as the police did not seek out the information. The clients may have civil cause for redress in the case, and the California Bar Association may take punitive action, but at this moment it does not appear that the attorney committed a criminal act in making anonymous calls. It is not, by the way, unheard-of for a physician or attorney to place the public good above client confidentiality, and pass anonymous tips to the police. It is, however, rare that the anonymity is breached.

In addition to the above-mentioned privileges, there is another special safeguard against government intrusion. The majority of states have some form of shield law protecting the confidential sources of journalists. However, at the time of this writing, there is no national shield law for news reporters. That's why a writer for the New York Times was jailed recently for refusing to give a federal grand jury the identity of her sources.

One nagging question connected with shield laws of journalists has provoked fresh controversy: who qualifies as a news reporter? With the emergence of blogs, pod-casting, and the like, the definition of journalist is potentially very broad. Some have advocated the creation of a personal privilege where the duty to protect confidential conversations extends to all citizens. However, in this era of hyper-sensitivity over terrorist threats, security demands will probably continue to outweigh individual freedom. Don't expect any legislature or court to broaden this right anytime soon.

This example of the jailed journalist leads to the ultimate alternative: civil disobedience. If you do not wish to testify before a duly authorized government agent or legal body, you can choose instead to spend time behind bars. And it is not just refusing to answer questions that can lead you to jail in the name of principle. We recall the case of David Gutknecht, brother of a Peace Corps chum, who, back in the 60s was against the war in Vietnam. He was eventually called up for his physical. As it happens, he was deaf in one ear, which would have made him an automatic 4F. However, he believed that if he went for his physical, knowing that he was 4F, he would be giving his tacit approval to the process, and, thus, the war. He therefore, knowing full well that he was 4F, refused to take the physical. And the local draft board, knowing full well that David was 4F, sent him off to Leavenworth Federal Prison. This left us with the Gutknecht standard for

making ethical decision which might produce annoying consequences: What would David Gutknecht do in this situation.

The first lesson taught in law schools is that legal advice is worth exactly what a client pays for it. Our best free advice to you is this: when in doubt, consult a lawyer. If you don't like what you hear, ask another. And if you are still unhappy, follow your own instincts. But always be prepared to pay the consequences.

2. OPSEC, Economic Espionage, and Competitive Intelligence — And the Chinese have arrived!

We have, in past issues, noted that the foreign press has devoted a lot of space to economic intelligence gathering by the Chinese, while there has been virtually no mention of it in the American press. While the optimistic view might have been that the Chinese had somehow overlooked the U.S. as a potential information source, the reality is otherwise.

The United States loses an estimated \$300 billion a year to competitive intelligence, theft, and economic espionage, with the average loss being \$50 million in a manufacturing environment and \$500,000 in a non-manufacturing environment. It has become increasingly clear that China has been responsible for an increasing portion of these losses.

The SEC has recognized the impact of these losses, and has said that, under Sarbanes-Oxley, internal controls have to be in place to track the costs and impact of economic espionage and theft of intellectual property.

The response from industry to both the losses and to the SEC requirements has been indifference. One economics professor noted that business magazines with which he corresponded have no interest in anything dealing with solving the problem, which mirrors our experience. The *American Management Association* said in conversation that the area was of no interest to their members. And if you speak to the *Public Company Accounting Oversight Board* (<http://www.pcaob.com/>) about the implications of the SEC's stance, you will be told that your inquiry has been received.

In spite this overwhelming indifference on the part of corporations and the business press, recognition of Chinese information acquisition efforts in the U.S. is finally making its appearance in the press. Unfortunately, some of the figures being quoted are patently absurd. Thus, one sometimes hears that there are 3,000 Chinese front companies in the U.S. When you pry a bit, it turns out that while there are 3,000 Chinese companies, of which only a dozen or two are thought of as front companies.

How comforting should the smaller numbers be? Well, in truth the media classifications are not meaningful because, to a large extent, and as happens with most information loss to economic espionage, competitive intelligence, and theft, the information is actually being given away, or left so unprotected as to be abandoned to anyone who wishes to acquire it. In the words of Paul Moore, who was the FBI's top China analyst from 1978 through 1998, "It's the mundane, day-to-day contacts that are killing us, not the exotic spy operations."

Much, if not most, of this information loss is preventable, and even for a large company, \$50 million or \$100 million that is lost needlessly is money that could have been better spent elsewhere.

3. Executive Protection — Profiling

One of the discouraging things in life is the realization that not everyone is honest. Some people lie, and it is always a battle to figure out when people are lying. There are a number of approaches to dealing with this issue.

One is technological, best exemplified by the lie detector. As is often noted, the efficacy of the lie detector is highly dependent on the operator. As an example of the potential problems with lie detectors, one person we know was given a pre-employment lie detector test back in the days when this was allowed, and not hired because the lie detector revealed that he had previously been incarcerated, which was wrong. On the other side of the coin, someone else of whom we know cheerfully volunteered to take a lie detector test, and that the test conclusively proved his innocence of something of which he was, in fact guilty.

Interrogation by a skilled interrogator, according to a recent discussion we heard, is accurate about fifty percent of the time. "Hard" interrogation by a skilled interrogator, according to this same roundtable of experts, is accurate about fifty percent of the time.

One can, in fact, do significantly better than fifty percent in some criminal cases through use of the Reid method of interrogation, but there are some caveats to this. First, the Reid method is inappropriate in cases where the subject is likely to be influenced by the interrogator. Inappropriate subjects include the young, the not-too-bright, and those from cultures where fear of authority will induce them to confess to things they haven't done. And because we know that innocent people often confess for a wide variety of reasons, the Reid method also confirms confessions by getting confirming information that only the criminal would be able to know.

The Reid method has been criticized by Amnesty International (http://www.amnestyusa.org/amnestynow/false_confessions.html) for using social engineering to get people to confess by providing the suspects with a socially acceptable reason to confess. While this may seem to be a reasonable fear, it doesn't make sense if you think it through. Imagine, for example, that you, gentle reader, have been falsely accused of sexually abusing your young grandchild. Is there any socially acceptable reason that could be presented to you which would convince you to confess to this crime? We rather think not!

What does this have to do with profiling? Well, in many circumstances we need to look at people and decide whether they are likely to be bad (or to *do* bad things). Profiling can be a good tool to increase the likelihood of your being right.

Now, when we speak of profiling, we don't mean making a decision based on sex, race, or national origin. What we mean is looking for **behavior** that is indicative of being a risk. This is essentially the legal standard that needed to be met for a *Terry stop* (*Terry v Ohio*, 392 U.S. 1 (1968)). In a *Terry stop*, police officers could detain you for a short period – not sufficient to be considered an arrest – and frisk you, as long as they could articulate some causal factor which rose to the level of reasonable suspicion that you were involved in a criminal activity. We distinguish this from measures designed for electioneering or PR purposes, where the only function of the measure is to give the impression that something is being done.

There are many circumstances in which we face a threat, and would like to increase the chance of catching bad guys. Shoplifting is one, and catching criminals about to do bad things is another. In both of these cases, the bad guys will almost certainly be giving physical cues that something is amiss. These visual clues can be obvious to the trained observer, and would constitute reasonable suspicion for a field interrogation.

Note that suspicion of being a person of another race, or suspicion that someone might be of a certain religion, or of a certain age and sex does not rise to the appropriate level: What we are looking for are behavioral traits that the officer can observe and articulate, not hunches or biases.

For those in the profession of executive protection or counter-terrorism, we are aware of what these behaviors are, and a bit of searching on the Internet will give you more information than you actually wanted.

The problem, of course, is that learning to recognize these behavioral signs takes training and experience. Since most public-sector measures are designed, particularly in election years, to deal with the problem of

convincing people that something is being done, it is way more effective to have more intrusive measures, or to have technological solutions which can be plainly seen.

Nonetheless, in those areas where it is appropriate to be trying to stop bad guys from doing bad things, we must get past trying to solve the problem of looking as if we are doing something, and move toward actually trying to solve real problems. Profiling of behavior is well-proven, and serious consideration should be given to its implementation if you have responsibility for protection of a facility. Or if you are concerned about being able to avoid potential bad situations in your daily life.

4. Technical Issues — Hurricane activity for the next decade

If you know anybody who lives in hurricane areas, you know that they have been fleeing hurricanes more and more frequently than in the past. We have heard a number of explanations of this, with our three favorites being that it is the will of God (always a safe guess), or global warming (environmentally trendy), or our sisters-in-law's fault (most likely). While all of these explanations have a certain charm, the recorded history of weather patterns in this hemisphere indicate that multi-decadal tropical signals occur in 20 to 30 year cycles. Two or three decades are a long time, certainly long enough for most non-meteorologists to be unaware of the cyclical nature of hurricane ferocity. The last slow period ended in 1995. Or, to put it another way, we have been in high cycle since 1995, and will therefore be in high cycle until 2015 if we are lucky, and 2025 if we are unlucky.

Since we are going to be stuck in high cycle for another ten or twenty years, it behooves us to pay attention to the recommendations of the *National Oceanic & Atmospheric Agency* (<http://www.noaa.gov/>), or NOAA (sounds like Noah). NOAA is the federal agency that will, in fact, tell you when it is going to rain for forty days and forty nights.

NOAA recommendations are fourfold:

1. Know the dangers

Know if you live in an evacuation area. Know your home's vulnerability to storm surge, flooding and wind.

2. Develop a plan

Have a *written* plan based on the knowledge of your potential risk. At the beginning of hurricane season (1 June), check your supplies, replace batteries and use food stocks on a rotating basis.

3. Secure your home when a hurricane comes.

During hurricane season, monitor what is going on in the tropics (we favor <http://www.intellicast.com/>), and monitor NOAA Weather Radio. You can find information on NOAA Weather Radio at <http://www.nws.noaa.gov/nwr>, and a list of suppliers of weather radios at <http://www.nws.noaa.gov/nwr/nwrrcvr.htm>.

There are two levels of alert:

A HURRICANE WATCH issued for your part of the coast indicates the possibility that you could experience hurricane conditions within 36 hours. This watch should trigger your family's disaster plan, and protective measures should be initiated, especially those actions that require extra time such as securing a boat, leaving a barrier island, etc.

A HURRICANE WARNING issued for your part of the coast indicates that sustained winds of at least 74 mph are expected within 24 hours or less. Once this warning has been issued, your family should be in the process of completing protective actions and deciding the safest location to be during the storm.

4. Evacuate your home when needed

If a storm threatens, heed the advice from local authorities. Evacuate if ordered. Execute your family plan.

5. Real Stories from the Field — ICE: In Case of Emergency

Some time ago we got a call from a friend who does training in hospitals. He told me that a number of people had called him, and told him that it was now becoming common for emergency rescue personnel, when dealing with an unconscious person, to look for a cell phone. If the person had a cell phone, they would look for a name preceded by the letters ICE, which stood for In Case of Emergency. We have subsequently received calls and e-mails from others in the field with the same message.

We did a little looking into this, and it seems the practice actually started in Great Britain in April, in conjunction with Vodafone's annual Life Savers Awards. The program really took off after the July bombings in London that killed 56.

While we hope that neither we nor you ever have any need for these numbers to be used, we think this is a good idea. The upside of being identified in an accident exceeding the downside of having anyone who

finds or steals your handset know who your emergency contact might be. We have programmed our cell phones accordingly. We would therefore urge each of you take the few minutes needed to change the name of the emergency contact in your phone to have ICE as the prefix.

6. Book and Product Reviews

With Winning in Mind

Lanny Bassham

Mental Management ISBN: 1-885221-47-9 166 pages \$12.95

<http://www.mentalmanagement.com/> 1-972-899-9640

As a child, Lanny Bassham was an aspiring but rotten athlete in every sport he tried. One day a friend suggested he try rifle shooting, an Olympic sport that didn't require you to be tall or strong or fast: All you had to do was stand still. By the time he was finished, he was an Olympic Gold Medal winner, and two time world champion.

On his way to the top he noticed that 95% of the winning was done by 5% of the competitors. These were not necessarily the competitors with the most natural talent or the greatest physical skills. Rather, they were those with the best mental management skills.

Bassham spent years refining his mental management skills, and turned them into (aside from his gold medal) a training program that is appropriate for anyone that is trying to accomplish some goal. Any goal, and not just athletic goals. This system is distilled in his book, *With Winning in Mind*, and will be the best \$12.95 you will ever spend if you have a goal you wish to achieve. Or if you have a child whose goals you want to help them be able to be able to achieve. Or friends who have goals you would like them to achieve.

We have bought copies for ourselves (they tend to be borrowed, with the borrowers unable to let them go), and on the occasion by the dozen to give as gifts. We have given them to people as wide-ranging as athletes, businessmen, cops, models, dancers, and actresses. In every case the book has been extremely helpful. We most recently gave a copy to competitive fencer (foil) Meredith Baskies, who read the book on the plane to a competition in Germany. One anecdote happened to address a problem she faced in being too excited to sleep well the night before a match. Based on the book – which she felt was written specifically with her in mind – she got a good night's sleep, and awoke refreshed and prepared for the day's matches.

We consider *With Winning in Mind* to be on our very short must-read list, and that it should be on yours, too.

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) and L. Burke Files (LBFiles@feeinc.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.

- **Sarbanes-Oxley Section 404 OPSEC compliance.**
 1. American businesses lose \$300 billion annually to competitive intelligence, economic espionage, and information theft.
 2. Sarbanes-Oxley requires internal controls tracking the costs, and impact on valuation, of competitive intelligence, economic espionage, and information theft.
 - LUBRINCO provides private sector access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information from competitive intelligence, economic espionage, and information theft.
- **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, the Caribbean.
 - Financial fraud and anti-money laundering program development and training for compliance with the US *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 **LUBRINCO** and its services, or for the archive of all past issues of **ÆGIS** in PDF format, please go to <http://www.lubrinco.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, go to <http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to aegis@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**, please send their e-mail address to aegis@lubrinco.com.

If there is a topic that you would like to know more about, send it to aegis@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**, send it as an attachment to an e-mail to aegis@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** 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 **LUBRINCO** Web site is included. This should be in the form

Article Title, from the September 2005 **ÆGIS** (© 2005 **LUBRINCO** & FEE), to be found at <http://www.lubrinco.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.