

ÆGIS



Addressing threats that affect your bottom line

Volume 9 Number 6, June 2006

From the case files of

LUBRINCO

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

and

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

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

Asset location in fraud, theft, and divorce? Call us!

This month's features:

- 1. Asset Location and Due Diligence — Change through participation**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — When should you call the FBI?**
- 3. Executive Protection — International stalking countermeasures**
- 4. Technical Issues — Pen registers**
- 5. Real Stories from the Field — 5.11 Tactical Gear**
- 6. Book and Product Reviews — Zero Halliburton Luggage**
- 7. Subscription/Unsubscription/Copyright Information**

1. Asset Location and Due Diligence — Change through participation

While we are all familiar with takeovers of public companies, hostile and friendly, we are less familiar with cases where participation can be a tool used to change a private organization whose purposes conflict with those of some subset of members. In some cases the changes sought may be for good, and in other cases it may be for ill. We are interested here only in the technique of gaming the system to effect change, not in the reasons for change.

We will give two examples of different approaches to hijack the system, each of which incorporates several similar incidents, as this gives a fuller view of the techniques used.

Change through demographics

An organization had been formed to de-program children who had become involved with cults. Some members of these purported cults arranged to bring into the de-programming group people who were not openly affiliated with the cults. Eventually most of the members of the de-programming group were *sub rosa* members of the programming group, much the way some civil rights organizations in the 1960s seemed to be primarily made up of FBI agents.

The organization soon became non-functional – at least for the purposes for which it was intended. Was the group doing the programming evil, and was the group doing the de-programming good? Or was it the other way around? We don't know, but we do know that the group became ineffective through changing the demographics of the membership.

Change through insurgency

In another case set, a member of a not-for-profit professional organization became convinced that the leadership of the organization was serving some purpose not of benefit to the members. This eventually morphed into the realization that this was a conspiracy extending also to most of the senior administrative staff.

He got himself elected to the board, where his behavior in trying to deal with this was such that he was eventually forced to resign by an open vote of the membership. Following classical insurgency tactics, he instituted a series of lawsuits against the organization and its directors, along with continuing serial strings of accusations, even after the accusations had been disproved. The combination of these was visible enough to cause many of the corporate

members – the lifeblood of such organizations – to withdraw sponsorship, as well as draining the limited financial and staff resources typical of the not-for-profit organization. It also confused the membership, many of whom apparently believed that, if there were so many accusations, must not there be some truth behind at least some of them?

Eventually the entire board, which had responded to this series of attacks in a high-minded pre-9/11 manner, resigned when an overused D&O insurance policy was cancelled. A new board was elected, including the deposed former member and a substantial number of people connected to or co-opted by him. The organization went into bankruptcy, and will end in the same way that countries unprepared for insurgency generally end.

Was the board evil, and was the group trying to co-opt it good? Or was it the other way around? We don't know, but we do know that the organization became ineffective through unwillingness to respond effectively to repeated attacks.

Each of these cases should remind you that participation can be positive or negative, depending on the goals of the parties involved. And that the actions and response of an administration are significant in allowing the members of an organization to be swayed to support one partisan group or another.

2. OPSEC, Economic Espionage, and Competitive Intelligence — When should you call the FBI?

Companies that choose not to implement an OPSEC program face a substantial eventuality of substantial losses from competitive intelligence, theft, and economic espionage.

The mindset of companies that wish to avoid this issue is such that it greatly reduces the likelihood that they will ever be aware that they have been ripped off. They will lose market share, find it harder to compete against those who are using their R&D cost-free, and even close divisions or go out of business without knowing the cause. It generally requires something roughly equivalent to being repeatedly hit over the head with a baseball bat before the cause of their losses intrudes on their consciousness.

However, in some small number of cases the problem becomes so egregious that they may at some point realize that they are being ripped off. What do you do if you find yourself in this position? The traditional approach is to try to put together a group, either internally or through use of consultants, to figure out what has gone wrong and how to address the problem.

Our repeated experience indicates that this approach is not fruitful, and that the first action should be to call the FBI. For most large organizations, the likelihood is that the Director of Security is a former FBI Special Agent, a former Secret Service Agent, or a former high level member of a major police department, so that the ability to directly contact the FBI is already in place.

The FBI is very good at what they do, and will be able to manage the job of finding, tracking, and shepherding the process of catching the bad guys and bringing the case to the federal prosecutor. They have resources and skills not available within the private sector, and substantial expertise in this area. Plus, they have the authority of the law behind them. As one Secret Service agent noted when they took over a case from us, “when the Secret Service knocks on your door it makes a greater impression than when LUBRINCO knocks on your door.” Putting all of these factors together, the FBI represents your best bet in terms of getting this particular instance of criminal activity to stop.

Keep in mind, however, that prosecution is not as cost effective as preventing the problem, in part because your failure to take preventive measures reduces the options available. As an example, if you have ignored SEC mandates and failed to implement an OPSEC program (or some equivalent, if there is such a thing) you have arguably abandoned the trade secret status of your information, which closes off several otherwise-promising avenues. Plus, you lose control of the process once you turn it over to the FBI, and their goals are not necessarily your goals. And, as with most events that end in court, it is likely that you are going to come away from the experience less whole than you would like. For example it is not unlikely that whatever happens in court will appear, from your perspective, to be merely a token slap on the wrist. This being the case, as the criminal prosecution goes forward your company will simultaneously need to be preparing a civil suit to attempt to get restitution once there is a criminal conviction in place.

While this particular instance of theft can be made to stop, unless you learn from the experience and institute an OPSEC program you will continue to be vulnerable. Indeed, experience indicates that if one instance has been discovered, there are likely one or two other attacks from other adversaries going on at the same time. After all, there is more than one lion in the jungle of international commerce, and many of them are likely to have been aware of your corporate indifference to protecting your intellectual property and sensitive information, and to have been willing to take advantage of this.

3. Executive Protection — International Stalking countermeasures

Contributed by Henrik Bramsborg, Bramsborg Security & Safety (bramsborg@bramsborg.com). He is the managing director of Bramsborg Security & Safety, a security company based in Denmark. Bramsborg Security & Safety, <http://www.bramsborg.com>, have been quoted or profiled in several Danish media as the “Danish stalking experts.” Henrik is a stalking- and surveillance-detection specialist, and the author of several Danish books on security. Henrik is also an experienced instructor in personal protection, having trained NATO S-FOR forces, police officers, correctional facility officers, and private bodyguards. He holds a management degree and is a certified motivation instructor. Contributed articles do not necessarily reflect the viewpoint of ÆGIS.

Stalking as a term is a very young one. Actually less than 30 years. But as disease it is probably several hundred years old. Scripts from sixteenth century China tell a story about a female stalking an emperor statesman.

Today stalking has become a common problem in certain cultures. The attention to the disease is primarily drawn by the press, focusing on celebrity stalkers and the effect it may have on the celebrity. This is however not the only reason why it has become an everyday occurrence. Within the terminology of stalking lies acts as diverse as intelligence collection, sending love letters, surveillance, sending gifts i.e. jewelry, harassment and violence.

There are, in my opinion, only a few tools suitable to fight such a horrible disease. Since the individual carrying the disease, seldom perceive him/herself as sick, the society must assist. This is best done by law.

Whether committing the stalkers to psychiatric treatment or simply placing the stalkers in jail, it is the society in which the stalkers commit their crime that has to take responsibility.

As a security professional I have studied and been involved in stalking cases on several occasions. A few universal rules apply to most stalking cases when we try to help the victims of stalking:

If you find yourself being stalked, regardless of country:

Say NO once. Tell the stalker once and for all, that you want nothing to do with him/her. After that, avoid ALL communication. This is important when you go to trial later on.

Collect evidence. It includes, but is not limited to; photographs, letters, notes, e-mails, voice mail, items sent as threat's or gifts, witness statements and cell phone SMS notes. Collect as much as possible. Do NOT destroy or alter evidence – it can backfire when prosecuting the stalker.

Get legal aide. Even if there are no stalking statutes available in the particular country you reside in, legal aide is the key to your salvation. A

(good) lawyer can tell you what is needed to get the perpetrator convicted. In my country, Denmark, we do not have a stalking law. We simply use a variety of different laws and statutes to keep the stalkers at bay (primarily harassment, threatening and trespassing offenses). A good lawyer will also help convince a reluctant police officer that the incidents you report are a serious problem.

Report to the police. Even if the twelve daily calls on your phone and the two letters you receive daily doesn't bother you, you should report it, via a lawyer. Chances are that the stalker will continue, and probably at a higher level. If the stalking turns grim, with violence involved, the police need to know the history in order to act correct. It will also help you, should you choose to move to another country, to have a copy of a restraining order, a report or a written receipt of you reporting a crime in case the stalker continuous in you new resident country.

Get security/safety and stay safe. If possible, get a personal protection specialist or another security specialist to protect you, at least during and right after the trial. Harden yourself by changing habits, car, style of clothes and social circles. Get self-defense training, get a dog, create a "safe room" in your residency and make sure that your neighbors know that you have a stalker following you.

Get in touch with a network of stalking victims. There are several on the Internet. It will help you keep your sanity and you will learn that your case is far from unique.

Several countries have laws against stalking these include USA, England, Scotland, Canada, Australia, Germany, The Nederland and Japan (to name a few). But a lot of countries have not yet discovered the "trend" among these socially inept criminals, and the consequence is that stalking in these countries is allowed to continue.

Should you need further information about stalking I suggest that you buy the two books: *Surviving a stalker*, by Linden Gross and *How to stop a stalker*, by Mike Proctor. There are several other fine books on the subject but these two combined, cover most issues.

Have you ever been stalked and wish to contribute to the "fight against stalking" please go to: www.stalkinsurvey.com and fill out the form. It is made by Leicester University and the results will benefit us all.

4. Technical Issues — Pen registers

ויאמר אל-נא יחר לאדני ואדברה אך-הפעם
אולי ימצאון שם עשרה ויאמר לא אשחית בעבור
העשרה:

Genesis 18:32

An increasing number of people are concerned about President Bush's Terrorist Surveillance Program. We feel that the issue merits some examination here not because of TSP itself or because of the politics involved, but because an understanding of how these issues are thought through helps us to understand how corporate senior management should approach similar issues where the propriety and impropriety – or the appearance of propriety and impropriety – are not entirely clear.

There are actually two (at least two of which we are aware) sets of activities in TSP that are being lumped together.

Warrantless wiretaps

The less interesting case is the use of warrantless wiretaps of calls where one party is outside of the United States, one party is a United States person, and it is reasonably believed that at least one party to the conversation “is a member or agent of Al Qaida or an affiliated terrorist organization.”

While we would personally be more concerned over being tapped by Anthony Pellicano, a vocal minority take the position that warrantless wiretaps of United States persons violates, at minimum, Fourth Amendment rights. The administration on the other hand believes passionately in the executive power of the President under Article 2, and of the Commander-in-Chief in time of war, which power they maintain to be free from all legal constraint. They have argued that the phrase “the President is authorized to use all necessary and appropriate force” in S.J. Res. 23, the *Authorization for Use of Military Force*

(http://yale.edu/lawweb/avalon/sept_11/sjres23_eb.htm) makes legal *any* action taken, and trumps the Fourth Amendment, as well as all others. For those who haven't read S.J. Res. 23, it says (emphasis ours):

SEC. 2. AUTHORIZATION FOR USE OF UNITED STATES ARMED FORCES.

(a) IN GENERAL- That **the President is authorized to use all necessary and appropriate force** against those nations, organizations, or persons he determines planned, authorized, committed, or aided the

terrorist attacks that occurred on September 11, 2001, or harbored such organizations or persons, in order to prevent any future acts of international terrorism against the United States by such nations, organizations or persons.

(b) War Powers Resolution Requirements-

(1) SPECIFIC STATUTORY AUTHORIZATION- Consistent with section 8(a)(1) of the War Powers Resolution, the Congress declares that this section is intended to constitute specific statutory authorization within the meaning of section 5(b) of the War Powers Resolution.

(2) APPLICABILITY OF OTHER REQUIREMENTS- Nothing in this resolution supersedes any requirement of the War Powers Resolution.

The War Powers resolution, which for the sake of brevity we have not included, may be found at <http://yale.edu/lawweb/avalon/warpower.htm>.

Since the Constitutionality of warrantless wiretapping of United States persons is receiving so much public scrutiny, we will forego addressing it here.

We must note however, that we are puzzled that this option – at best so fraught with the appearance of impropriety that its use must finally be addressed by the courts – would be chosen when there existed the option of going to a very accommodating Congress to make changes as needed to the FISA court, so as to allow the process to go forward with obvious transparency, legality, and oversight.

Pen registers

The more interesting case is the largely overlooked collection of *all* pen register data, which is the listing of who called whom. By the term all, we mean the pen register data for every long distance call made in the United States (there is some question as to whether local call data is always stored, though we would posit that if the pen register information is available it will be included), including every call you make and we make and everyone you know and don't know makes. While a 1986 federal law requires a court order for collection of pen register data for any given individual, a prosecutor does not have to justify the request, and judges are required to approve the request. Largely this is because you know that the phone company captures this information for billing (which is felt to reduce your expectation of privacy), combined with the fact that the uninitiated consider simply knowing who called whom to be relatively benign.

Benign as the warrant for a single pen register might be, Qwest apparently refused to provide the government, which had neither a warrant nor approval from the FISA courts, with access to *all* pen register data from of *all* of its 15 million customers after deciding the request violated privacy law.

From any perspective, large amounts of data that can be analyzed using modern data mining techniques are extremely attractive. Indeed, in the January 2006 issue of **ÆGIS** we discussed Admiral Poindexter's Total Information Awareness (TIA) data mining program, which was eventually shut down. TSP looks to be a start at reconstituting TIA under a slightly different set of letters.

But how valuable is pen register data itself, even if not combined with other information? In the November 2002 issue of **ÆGIS** we discussed the fact that the Colombian drug cartel purchased the pen register data for all of Colombia. Using sophisticated data mining techniques, the cartel was able to identify drug informers, whom they could then kill. While we don't know the size of the NSA's budget, nor how much of it is devoted to data mining, we like to think that that they have a greater institutional skill with computers than do the Colombian drug cartels, who spend only a fraction of their estimated ten to fifteen billion dollar annual revenues on data mining.

While everyone wants to stop terrorism, and we know that responses to attacks should not be the same as responses to challenges, our Constitutional protections were put in place to stem the history of abuse of power that has flowed through the millennia. The question becomes whether, lacking oversight, information and power would, once again, be misused. Imagine, for example, that a journalist was receiving leaked classified data, and that some of the information was passed via the telephone on switches for which pen register data was trapped. It would be but the work of a moment to connect the source with the journalist, no matter how many intermediaries were used. A few judicious prosecutions and major sources of embarrassment would be eliminated. While revealing classified information about government misfeasance or malfeasance might be as illegal as the misfeasance or malfeasance itself, we note that for minority party members of the Senate Intelligence Oversight Committee, reading the newspaper is the only way that they get the information required to do their jobs.

Plus, the logical train of thought in this era of inter-agency cooperation must surely be that if the results of data mining would help prevent or solve crime as well as deter terrorism, wouldn't it be criminal not to share this information with law enforcement? After all, while the Supreme Court has

said that “It is not better that all felony suspects die than that they escape,” does this concept really extend to other areas of search and seizure where there is no lethal force involved, but merely the likelihood of a sharing of information that may inconvenience criminals?

And we certainly understand the view that the Fourth Amendment hinders the work of law enforcement. Indeed, we still remember when Miranda appeared on the scene, how clear it was to some that nobody would ever be able to get another conviction in court.

This turned out to be the case neither when it came to Miranda nor in any other case where temporal exigencies prompted the abrogation of civil liberties. The benefit has not outweighed the costs. One would, for example, be hard pressed to believe that putting Americans of Japanese ancestry into camps during World War II was any more helpful, long term, than was Lincoln’s suspension of *habeas corpus* during the Civil war.

But isn’t it justified to intrude on the privacy of some innocents in today’s special and exigent circumstances, since without this we may not catch the bad guys? Unfortunately, we have many examples of people, up to and including many Presidents of the United States, who are unable to resist the temptation to misuse information.

Every generation seems to think that its problems are novel and pressing, and justify abrogation of civil rights. And that this abrogation will not be abused. However, most of the Amendments to the Constitution¹ serve a real purpose in protecting the people from the government and from themselves. And they serve this purpose largely because, when these civil rights are put aside, and when no oversight exists, governments are unable to resist the misuse of available information, and bad things happen.

And how this applies to us – and you

Privacy issues and issues of the appearance of propriety or impropriety are not faced only on the government level. We ourselves face these issues on a daily basis. For example, when doing recoveries of stolen assets, or in searching for witnesses, we often need to have access to information by Social Security number. This is clearly information that can be, and often is, misused, and so we recognize the need for oversight in this area, as well as

¹ Excepting, obviously, the 27th Amendment, proposed in 1789 and passed in 1992, by which time its provisions were covered by statute, and the 18th Amendment, which a) attempted to legislate morality, b) should have been dealt with by statute, and c) was repealed by the 21st Amendment.

our responsibility to the owners of the information: We do not necessarily give our clients information that we deem inappropriate for them to have.

Could we work without Social Security numbers? Yes and no. If we are doing a recovery of \$500 million dollars, the resources are likely there for us to get information using several approaches which might be less cost-effective. If we are doing a case where the client has been stripped of resources – a divorce case in which one spouse has taken all the assets, or a case in which we are trying to locate a deadbeat dad for an impoverished mother – and there is no money for extensive searching, then no, we are unlikely to be able to distinguish which of the thousands of John Smiths is the one whose assets we are trying to locate.

In terms of appearances, in an early case we were asked, in our capacity as licensee for Ross Engineering, to do some bug sweeping. When we did our customary background check on the potential client (we don't work until we know for whom we are working, and why they want us to do what we do), it appeared to us that he was a mobster. We declined to take the job. While it would certainly be legal for us to perform the sweep, we felt that working for people that we would prefer to see in jail would present the appearance as well as the actuality of impropriety. It is a decision that we have made many times since, and continue to feel that it is the right decision for us.

5. Real Stories from the Field — 5.11 Tactical Gear

It is always a pleasure to see products that are well thought out and well executed – particularly products we can use. Because of this, we were delighted when a friend called and asked us to take a look at the products from 5.11 Tactical Gear (<http://www.511tactical.com/>) in Modesto, California.

5.11 Tactical products are largely aimed at the law enforcement market, and include a variety of clothing items aimed at tactical and undercover officers. The products are designed by getting together professional users (we know one person brought in for this) and seeing what they need, and then working and re-working until the needs are satisfied.

Some of the clothing they make, such as jackets that hold a lot of things that normally might go on a duty belt, is useful to us professionally. However, we also use a number of their products in our everyday life. We are, for example, extremely pleased with their polo shirts because they are so well designed and so well made. Indeed, were we to look for embroidered corporate logo polo shirts, our initial call would be to 5.11 Tactical.

The company frequently has items on sale in their factory closeout section, and which can work out well if what they have on sale happens to be something for which you were looking anyway.

In addition, their customer support is excellent and forgiving. As an example, about two weeks after we bought one of their jackets they sent out an announcement saying that if we bought that particular jacket they would throw in their pouch kit containing 5 different holsters for various pieces of equipment. We called to say that we had just purchased the jacket, and they sent us the kit for the cost of shipping.

Good products combined with good customer care makes for a winning team. Take a look at their Web site and give them a try.

6. Book and Product Reviews

Zero Halliburton luggage

Zero Manufacturing, Inc.

<http://www.zerohalliburton.com/> 1- 801-298-5900

We travel a lot. (One editor is recognized by sight at the airline counter in his home town, and by some of the flight attendants - even overseas! - Oye!)

As with everyone that travels extensively, we have subjected ourselves to light luggage, heavy luggage, fragile luggage, and sturdy luggage. Among us, sturdy luggage has become the luggage of choice, with the aluminum cases from Zero Halliburton (<http://www.zerohalliburton.com/>) being the clear winners (we have touched on these cases previously in the November 2002, February 2003, and December 2005 issues of **ÆGIS**).

One of the virtues of sturdy cases is that they are, well, sturdy. As an example, this editor's first Halliburton case was purchased in 1965 for use as a carry-on bag while in the Peace Corps. Although a bit scuffed up, it is still in regular use. It is, however, considered somewhat dated as it does not have wheels. While not a big deal, all current versions are available with wheels.

Ignoring for this discussion briefcases (the example of which we got post-Peace Corps and still use), camera cases, makeup cases, and gun cases, other specialty cases, and suitcases too big for air travel (The reduced-to-50-pounds weight limit when checking bags knocked the 32 inch suitcase out. When traveling with paper or for several weeks you may be forced to take two smaller cases instead of one more convenient case, independent of the luggage.), their wheeled-with-pullout-handle luggage comes in four sizes useful to air travelers. The useful



sizes are the 21" carry-on (13 x 21 x 9), the 24" (18 x 24 x 9), the 26" (18 x 26 x 9.5), and the 29" (20 x 29 x 10).



In addition, suitcases useful for air travelers are made with wheels on the bottom in the 26" and 29" sizes. Which of these wheeled options you might choose is a matter of personal taste. While the version with the pull-out handles might seem more convenient, in fact we have had no problem rolling through the streets of New York during a transit strike or from customs to car to hotel in Istanbul or Buenos Aires or Hong Kong or Cairo.

Although the cases are near-indestructible (it is rumored that some years ago Algerian separatists emptied a plane of passengers and blew it up on a runway in France, and that the only recoverable items were Halliburton cases), occasionally repairs *are* needed. We had to replace forty-year-old latches on one case. And, after one trip on an airline now thankfully out of business, we had to bang out a dented corner with a ball peen hammer. More vexing, on older suitcases the internal dividers were held in place by clasps on elastic, and the elastic on one of our decades-old suitcases had lost its stretch. We brought it to Modern Leather Goods Repair Shop, Inc. in New York City, who, after three tries in several hours (and \$60) were still unable to even get the elastic sewn on to line up with the fixtures.

Putting aside these minor tribulations, you should expect that any Zero Halliburton case you buy will be happily used by you, and by generations far removed from you.

The price you pay for this is that the suitcases cost more than cheap luggage, albeit competitive with other fine luggage. A 21" carry-on, for example, retails for \$625. An equivalent leather Tumi carry-on retails for \$795 to \$895. The Louis Vuitton Pégase 50 retails for \$1,570.

Fortunately, luggage can always be bought at a discount, and the 21" Zero Halliburton carry-on is available for \$337.95 at Cambridge World (http://www.cambridgeworld.com/Zero_Halliburton_Bags/zerohalliburton_luggage.htm).

It has been the experience of these editors that in the long run, the best, most cost-effective choice in luggage for us is the virtually-indestructible aluminum Zero Halliburton case, and we recommend you give these cases serious consideration if you travel extensively.

7. Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2006 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.

- **Corporate counterintelligence.**

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, and 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 aegis@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 June 2006 **ÆGIS** (© 2006 **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.