

ÆGIS e-journal



Addressing threats that affect your bottom line

Volume 6 Number 10, October 2003

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:

- **Special Announcement**

1. **Due Diligence** — You can fool some of the people all of the time, which is enough to make a very good living...
2. **OPSEC, Economic Espionage, and Competitive Intelligence** — Active versus passive adversaries
3. **Executive Protection** — Personal locator beacons
4. **Technical Issues** — Mobile phones for a blackout, or a working weekend abroad
5. **Real Stories from the Field** — Being polite when the alternative will make things worse
6. **Book and Product Reviews** — *Sticky Fingers*
Microsoft Security Notification Service
7. **Free-Subscription/Unsubscription/Copyright Information**

**1. Due Diligence — You can fool some of the people all of the time,
which is enough to make a very good living...**

In order for fraud to be successful, you need two co-operating parties, the fraudster and the willing victim. This was again brought to our attention recently when we were called regarding money lost in an investment group. The amount lost was what we define as substantial, and the investment was conservative. While it is not impossible to lose a lot of money with conservative investments – ask anyone who owned Lucent – it certainly should be harder, and always merits a close look when it happens.

The manager running the investment said he was outraged at the loss, and insisted that he would oversee recovering the missing funds. This is nice, but, as a rule of thumb, it is inappropriate to have someone who might reasonably be suspected of causing the loss to be allowed to conduct the investigation. If the potential suspect is a bad guy it gives him a better chance of covering his tracks and getting away with it. If he is innocent and the money is not recovered, it unnecessarily leaves a suspicion that he might have been involved. Like Caesar's wife, those investigating a possible criminal matter should be above reproach, which is why, in the September *e-Journal*, we recommended that new CEOs taking over a company where there was a suspicion of fraud turn the investigation over to some outside, unaffiliated, entity or professional.

In this case, the manager hired a recovery agent to help with his investigation. Unfortunately, this still left control of the investigation in the hands of the manager, who was one of the most likely suspects. Worse still, the agent hired was one about whom there had been newspaper articles alleging participation in widespread financial fraud in many countries. These allegations might or might not be true: We have no certain knowledge one way or the other, and our opinion is not particularly germane to the focus of this article. What is germane is that the situation presents four disquieting possibilities, each of which should leave the investors with an uncomfortable feeling.

1. The worst-case possibility is that the manager is a fraudster and that the agent hired to help is a co-conspirator. (In this case the investors can kiss their money good-bye.)

2. The manager is honest and the recovery agent is crooked. (In this case the recovery agent will make recovery difficult or impossible.)
3. The manager is crooked and the recovery agent is honest. (In this case the manager will make recovery difficult or impossible.)
4. The final possibility is that the manager has bad judgment but is honest, and that the recovery agent is honest. (Here we are left with the *appearance* of impropriety, but no direct and active impediment from the combined (manager/recovery agent) recovery team to the determination of whether the funds had been lost or misappropriated, or to the possible subsequent recovery of funds.)

No matter which possibility turns out to be the reality, we do know, beyond the shadow of a doubt, is that when sums of money equivalent to the GNP of a small country have disappeared, the appearance of propriety is vitally important (particularly if the money is never recovered). This seems sufficiently obvious that one must ask why a group of investors able to collectively cough up this large an amount of money would let someone who should be considered a suspect manage the recovery of their missing funds.

The best explanation for this anomalous behavior turns out to be *cognitive dissonance theory*, which says that when there is a conflict between your beliefs and your actions it is easier to change your beliefs than your actions. We frequently see cognitive dissonance theory at work when dealing with spousal abuse. It is psychologically easier for the abused spouse to say the abuse is ok because they love the abuser (They must love them. Why else would they put up with the abuse?) than it is for them to admit that they might be victims, and make the appropriate changes to their behavior.

In the case of the missing investment money, it is psychologically easier for the investors to say the manager's conducting the investigation is ok because they trust the manager (They must trust him. Why else would they put up with the obvious impropriety?) than it is for them to admit that they might be victims, and make the appropriate changes to their behavior.

Obviously, in any group there will be some people who will want to eliminate all doubt, and ensure that not only the reality but also the appearance of propriety is maintained. Whether or not an actual fraud has been committed, those who have become exemplars of cognitive dissonance theory in action typically outnumber this group, and the voices of the rational minority will be swiftly and firmly quashed.

The result is that, in cases of actual fraud, through manipulation of the majority to take advantage of their cognitive dissonance (Who among us wants to admit we were fooled?) the fraudster is likely to escape unscathed, and with profits intact.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Active versus passive adversaries

While active adversaries – folks actively trying to get information from you – should be an obvious source of concern, we are sometimes even less aware of passive (or sometimes inadvertent) adversaries. While an active adversary may well try to suborn someone to get information, often this is not necessary, as there may well be someone willing to give away the information with no understanding or knowledge that they are doing anything wrong.

In some cases this is our fault for giving someone the information. A prime example of this would be discussing sensitive matters in front of our family. It is not reasonable to expect much discretion from children, who may well repeat things they have heard. If *we* don't understand "need-to-know" restrictions, it is unreasonable for us to expect our families to understand.

In other cases it is our fault for not identifying sensitive information, and for not providing the education and training to our employees to know what they may or may not discuss. An excellent example of this was found in our article *The P&G/Unilever Caper* in the August 2001 e-Journal.

As with children, if we have not identified information that is sensitive, and that should not be discussed, it is not reasonable to expect that employees will be able to mysteriously discern what is or is not sensitive, or what may or may not be discussed outside the company. This is particularly true when dealing with situations in which people have been given license to talk. As an example, marketing people make their living by giving people information. Along the same lines, if someone is sent to speak at a conference – or even to attend a conference – it is reasonable to assume that they will exchange information with peers and conference participants. If no limits have been placed on what may be discussed, then they will quite reasonably feel free to discuss everything.

The bottom line is that without identification of critical information, employees cannot know what they are permitted to reveal and not reveal. In the average American company, roughly seventy percent of the assets are in intellectual property, yet most companies have no current and ongoing audits

of this intellectual property. Clearly, if the company is unaware of what it has and where it is stored, it is available to anyone and everyone. Employees cannot be expected to protect what the company has not chosen to shield.

You can do something about both passive and active adversaries, but not until you have taken the first step and identified critical information.

3. Executive Protection — Personal locator beacons

Occasionally we end up in places where we might have a life-threatening problem and really need to be rescued. This may happen if we are involved in a plane crash, a boat accident, a car accident in the desert, a hiking accident, or any number of other rare and unfortunate situations where we need serious emergency help.

In some places you can use your trusty cell phone and simply call out for help. During one of the U.S.'s smaller wars in the Caribbean, a few of our troops got trapped with no means of communication (something to do with every service having different radios operating on different frequencies). One of the soldiers had his cell phone and called his mother, who called Washington, who called someone local, who rescued them. Amusing as this is, if true, it is equally true that in many places there is simply no cell phone coverage. What then? One possibility is a satellite phone, but many of these are the size of a laptop computer, and some are relatively delicate.

An alternative is to have a personal locator beacon, aka a PLB. These are individually registered and astonishingly small devices that emit a signal on 406 MHz that is picked up by COSPAS-SARSAT satellites. The PLBs we recommend contain a built-in GPS system, so the satellites' receiving stations quickly – if you are between the Arctic Circle and the Antarctic Circle, the satellite geometry is such that the very first GPS location burst transmission should be captured – know three things: To whom the PLB belongs, where the PLB is (give or take 100 meters), and that you are actively (you have to take a series of steps like pulling a tab and pushing a button to activate the PLB) indicating that you are in trouble. At this point an appropriate sea-air-land rescue can be launched.

The signal will be transmitted for a nominal 24 or 48 hours, depending on the device. Frankly, if search and rescue hasn't launched within three hours of the PLB being activated, something is seriously wrong! In addition, according to a study done by the U.S. Coast Guard using Microwave Monolithics PLBs, it appears that once a signal is picked up (usually within 60 seconds of device activation), it is passed off to the appropriate authority

immediately, but not reported again. This means that once the distress signal has been picked up, the PLBB has largely done its job. However, the signal additionally sent on 121.5 can still be used for location by triangulation, or for voice transmission if included.

The devices, by the way, should not have been damaged by the incident. They are all water resistant to at least one meter and dropped tested on all sides from at least one meter.

PLBs should be used when you might otherwise die if not rescued soon. **PLBs should not be activated if no lives are at stake.** A rescue effort is always very expensive and puts the rescuers at risk. If it is felt that the use of the PLB was frivolous, expect at the very least to get a *VERY* large bill to cover the cost of the rescue effort!





As noted above, the first distinguishing characteristic among PLBs is whether or not they include built-in GPS. The cost – those without voice communications are around \$1,200 – is low enough that it makes no sense for the corporate user to consider a system without GPS, particularly since GPS narrows your location from 1.3 kilometers without GPS to 100 meters with GPS! While PLBs also transmit on 121.5 MHz, (a common aviation frequency for which there is readily available triangulation equipment), if I am in trouble I want my rescuers to have the most precise location possible, which means GPS.

The second distinguishing characteristic is whether you have voice communications (available on 121.5 and 243 MHz). Voice communication is obviously desirable in many circumstances, particularly if someone is conscious and able to speak, but pushes the cost of the HR Smith model, which comes with voice communications built-in (it is also water resistant to 10 meters, and canon tested to 12 Gs, hinting that the unit has been designed to military specifications) to \$3,300. While this is certainly not an unreasonable amount to have with your \$100,000,000 executive in his \$20,000,000 aircraft when it crashes in the middle of nowhere, you should not feel unprotected with a PLB lacking voice communications.

We looked at four devices, all of which we would comfortably use, and all of which we are comfortable in recommending for your consideration. We have listed these in alphabetical order by company in the chart below.

The bottom line is that in many situations a PLB is very appropriate to have in your pocket or bag case of emergencies. If we have a detail where a PLB might be appropriate, would I fight for to have one? Of course. If you have

an emergency and someone will die because you don't have one, would it be worth way more than its cost to you? Absolutely!!!

Manufacturer	Model	Retail Price	Features	Web Site
HR Smith 	500-27	\$3,300	150 x 87.5 x 37.5 mm 7.1" x 3.4" x 2.2" 23.2 oz/48 hours Voice on 121.5 MHz, 243 MHz Waterproof to 10 meters Canon tested to 12 Gs	http://www.searchandrescue.com/
McMurdo Pains Wessex 	FastFind Plus	\$1,195	150 x 75 x 52.5 mm 6" x 3" x 2.4" 14.8 oz/24 hours	http://www.pwss.com/
Microwave Monolithics 	MicroPLB GX	TBD	148.75 x 58.75 x 27.5 mm 5.95" x 2.35" x 1.1" 9.5 oz/48 Hours Microcomputer controlled oscillator instant-on (think sinking ship). Burst delayed 50 seconds in case of accidental activation.	http://www.micro-mono.com
SERPE- IESM – KANNAD 	406 XS-2 GPS	N/A	152.5 x 70 x 36.4 mm 6.1" x 2.8" x 1.3" 11.3 oz/24 hours	http://www.serpe-iesm.com/

4. Technical Issues — Mobile phones for a blackout, or a working weekend abroad

Those of us who were in New York City for the August blackout were delighted to discover that mobile telephones – like landlines –worked (yes, we know on some intellectual level that other places also lost power, but we in New York City aren't all that aware of the rest of the world). However, as the blackout stretched on into the next day an interesting thing began to happen: The batteries in most peoples' mobile phones died.

We have long believed that the primary reason to have a mobile phone is to make calls. There are two things you need to do this. The first is access to the mobile network (i.e., you have a signal) and the second is a battery that isn't dead. For this reason we have traditionally used those Nokia 61xx and 63xx series handsets which allowed use of batteries of up to 3800 mAh capacity, which gave something like a month standby time or twenty hours talk time. This meant we could go away for a week, using a 6190 here or a 6150 in Central Europe or the Mideast (or a 6310i which is more efficient than the 61xx series and will last even longer, and would have been the perfect handset for business travelers for use in the U.S. and abroad if Nokia believed in quad-band handsets and had included 850 MHz), and never had to worry about re-charging the battery. We could certainly survive something as short-lived as a blackout without any problem, while everyone else's more modern handsets faded away.

Sadly, the era of long talk-time phones is gone, due largely to economic pressures. In the past, mobile phones were luxury items that were primarily aimed at the business audience, who were a chatty group. Now they are commodity items aimed at a wider audience, with business travelers being a niche demographic market scarcely worth addressing. Today you can buy a handset with a camera, with an MP3 player, with an FM radio, with a recorder, with a color screen, and with all sorts of fancy games, but you can no longer buy a handset that will get you through the weekend.

Nokia (who don't make a quad-band handset because they say that nobody other than Cingular is implementing GSM 850, somehow overlooking AT&T Wireless in the U.S., as well as entire countries like Colombia, Ecuador, and Panama), which used to be the company whose trademark was handsets that had long talk times, now considers that "ranges of 4-6 hours are the norm." Staffers at AT&T Wireless said that they were given high-capacity batteries (double the capacity of the existing BLD-2 and BLD-3

batteries) that gave a marked increase in talk time for the Nokia 6800 and 6200, but the good folks at Nokia say there is no plan to release them.

What does this mean if you are a traveler interested primarily in making calls? If you don't need 850 MHz you may wish to look for a Nokia 6310i while they can be still found, or get some other handset and carry three extra batteries. And if you need 850 MHz? Then you should get whatever handset you like that includes 850 MHz, and carry three extra batteries.

5. Real Stories from the Field — Being polite when the alternative will make things worse

We all occasionally come up against people in positions of authority who are doing something which displeases us. In these cases there is a temptation to fight back. This is *generally* not entirely fruitful, as these people often have the power of government behind them, and, short term, there is not a lot you can do other than try to keep stress levels low.

Obviously, in a perfect world there would be no abuse of power, but ours is a less-than-perfect world, and power is routinely abused. Our current favorite was the family entering the U.S. that was delayed for several hours because one of the family members was on the suspected-terrorist list. While the father understood that a diplomatic passport was not actually *carte blanche* for terrorism, nor reason to abandon all administrative procedures, he did feel that someone should have questioned the likelihood of his five-year-old daughter actually being a terrorist, as opposed to there perhaps being another person with the same name. He was apparently very verbal on the subject. While his view might make obvious sense, his attitude cost them several hours of waiting before they were allowed into the country. The delay could have been avoided by being appropriately servile.

The situation was similar in the arrest of a pilot who had tweezers in his carry-on kit. He was told he couldn't take tweezers on the plane because they could be used to pick the lock on the cockpit door. He pointed out that this (holding up the key) was the actual key to the cockpit, and, since he would be the one flying the plane, having or not having tweezers made no difference. While nobody considered him a threat, they did consider him an arrogant annoyance, and eventually arrested him for moperly and dopery in the airways, or some such.

Two travelers recently did a small experiment. As they traveled, one would be very polite and compliant while the other would be argumentative and in a hurry. Without fail the one who was quite and compliant sailed through

security. The argumentative one was stopped and given a thorough secondary screening. It was security-as-retribution. At one of the checkpoints the cohort claiming to be in a hurry was singled out for further screening. After 14 minutes of standing around waiting for the secondary screening, he demanded a supervisor, and asked for expedited service since, by count, over 70 people had since passed through screening while he was still standing there. He was told to “shut up and we’ll get to you.” When the supplemental screening did occur the screeners moved slowly. Lest there be any doubt that this was abuse screening, we note that they asked him to remove his shoes, and, even though he was wearing no socks, they began to wand his bare feet with the handheld metal detector. Twenty-seven minutes after he had passed primary screening, he was cleared from the supplemental screening. The experiment was considered to be satisfactorily concluded.

This incident came on the heels of the revelation that a pair of foreign nationals had forged federal ID, and had, for a fairly substantial period of time on a substantial number of flights, politely approached security with their false ID, and had been being escorted, loaded guns and all, around the checkpoints and onto their planes. Putting aside the issues of whether randomly armed passengers make flying safer or more dangerous, and the issue of whether airport security is intended to be anything more than security theatre, this incident (discovered inadvertently when one of the men accidentally left his jacket and ID somewhere, and which the TSA noted did not indicate a compromise of their checkpoint system, as the checkpoints had been bypassed, not compromised), shows the importance of politeness.

A fluke, you say? It was reported that on 27 August 2003, two men dressed as computer technicians and carrying tool bags entered the intelligence centre at Sydney International Airport. After supplying false names and signatures, they were given access to the top-security mainframe room, where they disconnected two computers, which they wheeled out of the building. You can rest assured they were polite and friendly, not truculent.

Lest you think that only civilians suffer from abuse, in another incident a car full of men speeding down the thruway noticed that a New Jersey State trooper had stopped a driver, who was beating the stuffing out of the trooper. Being good citizens, they stopped and subdued the attacker. Other troopers showed up, and promptly arrested the helpers for illegal possession of weapons. The rescuing felons, still wearing their New York area police department shooting team uniforms, were on their way back from a police pistol match in Pennsylvania, and had neglected to properly store their weapons, unloaded and inaccessible, in the trunk of their car, as required by

New Jersey law. Astonishingly (we say astonishingly because a bust of six heavily armed criminals is a feather in any officer's cap, and very difficult to pass up), they (the helpful police officers) were not actually booked.

A pair of Los Angeles Sheriffs had it even worse. They were taken, in full uniform, from their fully-marked cruiser and proned-out on the ground at gunpoint until a supervisor who was a little less caught up in inter-agency rivalry showed up, at which point they were released. The result of this was a hysterically funny video prepared by LASD, and sent to LAPD, on how to identify a member of the Los Angeles Sheriffs Department.

The point of this is not that abuse of power happens: We take that for granted in this less-than-perfect world. The point is that, from a practical point of view, no matter whether you are a civilian or a law enforcement officer or a diplomat, you can't expect to slide your way out of these situations by being truculent or overbearing. You need to be prepared to go out of your way to be friendly and helpful and, most of all, patient, with every law enforcement and security officer that you encounter, and deal with any complaints or issues later, after the fact, not after being arrested.

6. Book and Product Reviews

Sticky Fingers: Managing the Global Risk of Economic Espionage

Steven Fink

Dearborn Trade Publishing ISBN: 0-7931-4827-8 368 pages \$26.00

<http://www.dearborntrade.com/> 1-312-836-4400

Before we started reading *Sticky Fingers* we thought it was a book about economic espionage. Although anyone dealing with this issue of economic espionage should read this book, it is really more about crisis management after the fact than about economic espionage *per se*.

Fink takes an interesting historical view of the Economic Espionage Act of 1996. The EEA was written in that unhappy period that came between the fall of the Soviet Union, which took away a lot of the justification for many agencies' existence, and the attacks of 9/11, which was arguably the best thing to ever happen to most agencies. Overseas, intelligence agencies were re-tooling their spies to steal commercial secrets rather than retiring them (bureaucracies don't willingly cut staff or close their doors), and in the U.S. the FBI was casting about for some way to use its people once the Red Menace disappeared (bureaucracies don't willingly cut staff or close their doors). And so, according to Fink, the EEA was born.

His discussion of his involvement with the Avery Dennison trial is instructive on many levels, not least of which is bringing up the question of whether you should go to the Feds if you are the victim of espionage, or just accept your losses.

Why would you not go to the Feds?

- The publicity won't do you a lot of good: There is little way you can escape looking foolish.
- The FBI has its agenda, which will not be the same as yours.
- You will lose all control of the investigative, prosecutorial, and public relations process.
- If the country conducting the espionage is an important trading or military partner, the likelihood of the Feds choosing to create an international incident to protect your profits is, er, low.
- While the FBI is the best in the world at many things, it is not clear that going to trial over theft of intellectual property is one of them.

Going to the Feds or not going to the Feds is not an easy decision to make, but it is one that you should make well before a crisis hits you.

And, in fact, there are a lot of decisions relating to the management of an economic espionage incident that are better made before the fact rather than after the fact. This book will help you make these decisions, as well as help you plan in advance for many of the things that will happen as a result of being the public victim of this crime.

Steven Fink has a lot of hard-won experience as a crisis manager, and it is always better to learn from someone else's experience rather than learning from your own mistakes.

Microsoft Security Notification Service

Microsoft

<http://register.microsoft.com/regsys/pic.asp>

Whenever a major worm or virus sweeps through the world, it usually turns out that the offending vulnerability (usually a Windows vulnerability) has been known for a relatively long period of time, and that there were available patches from Microsoft to deal with the problem, and prevent it from actually becoming a problem.

While the updates are posted at sites such as <http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/>, many people don't know about this site, and, frankly won't bother to look at it in any case.

For those who would like to make the effort to keep the security of at least their own systems current, Microsoft will cheerfully send you, for **free**, an e-mail whenever there is a security update. You can sign up for this service at <http://register.microsoft.com/regsys/pic.asp>.

What does this mean in practical terms? It means that whenever there is a patch available to address a vulnerability, you will know about it, and have the option to apply it within hours of its release, before it is a danger, rather than waiting until after it makes the headlines, or you find strange things happening on your computer.

Be aware that bad people send out notices purporting to be from Microsoft: We got one claiming to be from "MS Customer Services" which contained a virus, according to our virus scan. How can you be sure that the document you get is from Microsoft? The security bulletins come as PGP signed documents. You can download the signature from <http://www.microsoft.com/technet/security/notify.asp> and import it into your PGP key ring. This way you can validate the document as being actually sent from Microsoft.

If computer security is a concern to you, you should sign up for this free service from Microsoft.

7. Free-Subscription/Unsubscription/Copyright Information

•• AEGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2003 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 2003* and the *EU Revised Money Laundering Directive of 2003*.
- **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 2003 *ÆGIS* e-journal (© 2003 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.