



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 7 Number 12, December 2004

From the case files of

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

and

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

Intellectual property being stolen or at risk? Call us!

This month's features:

• **Special Announcement**

- 1. Due Diligence — Product Recalls**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Sarbanes-Oxley, OPSEC, and valuation of intellectual property**
- 3. Executive Protection — Avoiding frivolous medical lawsuits**
- 4. Technical Issues — Caesar's wife and Caesar's voting machines**
- 5. Real Stories from the Field — Sexual harassment policy as a tool, II**
- 6. Book and Product Reviews — Second Wave Enterprise Resources Planning Systems // Business Owner's Legal Guide**
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Product Recalls

Most products made do what they say they are going to do, but some have flaws or defects or are mislabeled in such a way that they can be hazardous or deadly.

We were reminded of this recently when we went to a daycare center and saw a travel play pen that had been recalled many years ago because, when improperly assembled, it had caused the death of something on the order of a dozen infants. The manufacturer had done the right thing and had recalled the product as soon as they learned how the portable crib caused injury. And yet, here it was in all its glory. When we showed the owner of the daycare center how the crib had killed, she was shocked and immediately pulled the children out of it, broke it so it could never be used again, and threw it out.

But some owners simply never learn about the recall products, whether it be childcare products, cars, lawn equipment, appliances, et cetera. This means that some end up being sent to the local thrift shop or end up in some other second-hand market.

So what do you as a business owner need to do?

Obviously, as a manufacturer you need to actively try to assure that your products are safe, and take timely action if they are not. The question of timeliness is interesting. In the excellent business writing course authored by Peter Vogel and offered at Learning Tree, one of the questions posed is this: What should a business writer do in writing the product information for a product that has been discovered to be flawed, but is slated to be repaired? Since business writers are at the bottom of the corporate food chain, you can imagine what a struggle it was for those higher up the food chain at Merck when dealing with early contradictory information regarding Vioxx. One wonders whether, in hindsight, the folks at Merck think they should have acted earlier.

As a manufacturer, you have to be concerned about more than just your designs. You also have to be concerned about the materials you use. If you use welding rod, for example, some welding rod that has been recalled may work just fine for hobby work, but may no longer be acceptable for welding

high-temperature steam pipes. This is stuff you need to know, so you need to schedule appropriate checks with those bodies that regulate the items.

As a business you need to have a list of the equipment and products in your office and plant, with their model number, and have someone check every so often that the products you use do not represent a hazard.

For a retail environment you need a full list of all of the items you sell and have on stock, and know if they have been recalled.

If you run a day care operation, it is very important for the health and safety of the children – and in terms of your liability – that you know what physical goods and toys and snacks have been recalled.

If you run a rental car agency, you need to know what vehicles have been recalled, and whether those recall issues have been dealt with, and whether compliance has been documented! We suspect the old law enforcement saying that if something makes you look good, but wasn't documented, it never happened.

For owners of airplanes, there are a lot of airworthiness directives that require compliance in some timely manner. As pilots we can tell you that, if there is no documentation of compliance with a mandatory AD in your logs, you may well have serious problems somewhere down the line.

Here are two sites that deal with recalls:

- US Government listing of private sector recalls for consumer products, motor vehicles, boats, food, medicine, cosmetics, and environmental products:
<http://www.recalls.gov/>
- FAA Airworthiness Directives
http://www.airweb.faa.gov/Regulatory_and_Guidance_Library/rgAD.nsf/MainFrame?OpenFrameSet

2. OPSEC, Economic Espionage, and Competitive Intelligence — Sarbanes-Oxley, OPSEC, and valuation of intellectual property

An OPSEC program can be a big help in valuation of intellectual property. This is largely because OPSEC gives management a new way to look at their intellectual property.

There are a number of ways that IP can be valued. One can, for example, look at development cost, or replacement cost, or the cost if lost.

OPSEC, on the other hand, looks at cost not *in vacuo*, but in term of the *risk* to the enterprise.

Risk is calculated as:

$$\mathbf{RISK = PROBABILITY \times IMPACT}$$

where

$$\mathbf{PROBABILITY = THREAT \times VULNERABILITY}$$

so that risk decomposes to

$$\mathbf{RISK = THREAT \times VULNERABILITY \times IMPACT}$$

Threat—Threat comes from specific competitors or adversaries. If there is no threat, there is no risk. But the numbers tell us that there is a real threat—that a specific individual or organization has the desire, the skill, and the intent to acquire your critical information.

Vulnerability—Some targets are more vulnerable than others, generally thorough neglect because the entire issue has been overlooked. If vulnerability is lowered, risk will be lowered as well.

Impact of the theft—How damaging is the loss of “smart” assets? If the impact is low, you don’t care. If it is high it is cause to worry.

What does this mean in terms of valuation? It means that managers have a new way of looking at IP, and a new way of looking at cost. Thus, if you have a patent that is costing you, over its lifetime, \$80,000 to protect, and the risk in the case of its loss is substantially less than \$80,000, the patent may not be worth protecting. And if you have a thousand patents with no real value, and over their lifetime each of them is costing \$80,000 to protect, you have the potential to save the company a lot of money.

By the same token, when you factor the threat and vulnerability in with the financial impact, you come up with a different scale of measurement that may well be more reasonable compared to other methods.

Thus, while OPSEC is designed to allow you to identify and protect information, its very nature gives you the side benefit of more realistic evaluation, independent of any protective steps you take.

3. Executive Protection — Avoiding frivolous medical lawsuits

As anyone who was not in a coma was aware, one of the big talking points of the recent American presidential election was frivolous medical lawsuits which drive up the cost of medical insurance.

Frivolous medical law suits fall into two categories.

The first category is lawsuits that have no foundation in fact or law. These are not much of a concern, as they virtually never make it to court.

The second category is lawsuits that end up in a substantial penalty. These lawsuits generally revolve around iatrogenic injury – doctor induced injury. Since iatrogenic injury is responsible for something on the order of 180,000 to 210,000 deaths a year, our goal is to give you some hints on avoiding being a participant in a “frivolous” lawsuit.

Now, keep in mind that medicine, while much advanced over where it was during the American Civil War, is still largely in its infancy. There are many conditions under which someone may die even if there is no error. As an example, this editor’s father went in for surgery at age 90. He was a very high-risk candidate, and there was a high probability that the outcome would be death, balanced by the sure knowledge that without surgery he would be a quadriplegic. At first the surgery seemed successful, and the day after the operation we were told he would be discharged the next day. Sadly, the next day he suffered an embolism, and was dead the day after. While unfortunate for us, this was clearly no one’s fault.

On the other hand, a young woman of our acquaintance – roughly half the age of our father – went in for the same procedure, a cervical laminectomy, and, due to scandalously bad aftercare, died. A lawsuit – which would have been doubtless termed frivolous – would seem to have been appropriate. In this case, however, fairly direct threats from representatives of the medical facility induced the family not to sue.

As an example of a “frivolous” lawsuit avoided, largely by luck, another of our acquaintance was going in for eye surgery, in this case on his RIGHT eye. Due to a delay in the conclusion of the operation preceding his, he was left to wait in the hallway. To kill time, he looked through his chart and discovered that he was scheduled to have his LEFT eye operated on. He brought this to the attention of his nearby aide, every nurse who walked by, the janitor, and, finally, his doctor. Had he not caught this, he would have been functionally blind, and involved in a “frivolous” lawsuit.

With iatrogenic injury being considered by some to be the third leading cause of death in this country, a lot needs to be done before you put yourself, or those for whom you are responsible, into the care of a well-meaning, but not necessarily sober or competent, practitioner of medicine.

For a start, try to find a medical practitioner who at least *seems* competent (keeping in mind that just because a doctor is your kid brother doesn’t automatically make him an idiot, no matter what your childhood experience leads you to believe). It is neither inappropriate nor foolish to get and check on references, and to ask about failures, as well as successes. When we

check on medical backgrounds for those few hospitals prudent enough to actually check the credentials of those they hire, roughly one out of seven is immediately disqualified!

Second, get second and third and fourth opinions until you are satisfied that you have some feeling regarding what might be right for you. When we were studying for our Masters in developmental psychology, we heard a lot of horror stories about misdiagnoses. In one case, a girl complained of stomach pains and withdrew from most school activities. She was sent to the best specialist in New Jersey, who found nothing, and was finally diagnosed as being school-phobic. This may not sound like much, but is, in fact, about two steps away from being locked in a dark closet forever. The third opinion sent her to Mass General, who found the physical problem, which was easily cured. In another case, a boy on a US air force base mentioned to his mother that he had been hearing voices. He was diagnosed as having childhood schizophrenia – another lock'em-in-a-closet problem. The third opinion discovered it was treatable epilepsy.

Third, do a lot of research. Nobody is going to have more interest in you and those under your care than you, and little medical literature is beyond your comprehension. Keep in mind that diseases like porphyria that are rarely seen are not generally thought of as being the problem, and if your doctor has not kept up with the literature you may end up with the correct diagnosis. Obviously some doctors are competent, current, and innovative, and do think outside the box. But, even so, don't rule yourself out as a researcher and diagnostician.

Finally, try to minimize possible bad consequences. We recall being told that roughly one in three hospitalizations comes from unfortunate – and preventable – drug interactions. Make sure the pharmacist knows everything that is being taken, and is checking to make sure that the combination won't kill you. We knew one woman who had an allergy to some medicine who would query the nurse about what she was being given, and, if she had any questions whatsoever, refused to take the pills without her doctor checking them first.

By the same token, if you go in for surgery, make sure that it is clear, no matter how drunk your surgeon might be, what is being operated on. When a friend of ours went in for knee surgery – we had an acquaintance who came out of minor arthroscopic knee surgery dead – we recommended that she write “operate on right knee” on her stomach, and “operate on other knee” on her left knee. She said that this was silly and insulting to the medical

staff. She was astonished when, just before her operation, the nurse wrote “operate on other knee” on her left knee. Since many frivolous lawsuits involve operations on areas other than what was specified, making sure the busy surgeon knows what needs to be done is neither insulting nor silly.

Equally, if something seems radically wrong – like the doctor appears obviously drunk or incompetent, consider delaying surgery until conditions are better.

With some luck, you, and those under your care, will go through life with no serious contact with the world of modern medicine. And, if you do, the likelihood is very, very, very high that the interaction will be uneventful and satisfying. But the exercise of due diligence in this arena can help assure a happy outcome in those rare cases where you face needless risk.

4. Technical Issues — Caesar’s wife and Caesar’s voting machine

In this day and age it is important to understand why it is difficult to write a bug-free computer program. An easy example will show you the problem. Imagine that your company makes triangles, and that you want to computerize their testing. So you ask your crack programmer to write the testing code. The requirements are that the triangle tester will type in the lengths of the sides of the triangle, and that the program will tell you if it is an equilateral triangle (three congruent sides), an Isosceles triangle (two congruent sides), a scalene triangle (no congruent sides), or not a triangle.

How do you test for it not being a triangle (meaning you can stop if the object isn’t a triangle)?

- Well, certainly if the length of one side is greater than the length of the other two put together, then it isn’t a triangle.
- And if there are other than three sides it is not a triangle.

So now that we think it is a triangle, what do we do?

- To test for an equilateral triangle we might say that if A equals B, and A equals C, then it is an equilateral triangle.
- To test for an isosceles triangle, we might say that if A equals B but not C, or A equals C but not B, or B =C but not A, then it is an Isosceles triangle.
- To test for a scalene triangle, we might say that if A is unequal to B, and A is unequal to C, and B is unequal to C, then it is a scalene triangle.

So with these five tests we should be done, right? Actually, no. To cover all cases there should be something on the order of seven more tests.

The bad news is that a reasonably good programmer will probably come up with seven tests, leaving six undone. The good news is that these seven tests will cover most cases, and you might go forever without hitting the missing six cases. Or you might hit one of them in which case the program will break or give you a false answer. After all, if you hadn't tested that no side was greater than the sum of the other two sides, your program would have told you that a 3 by 4 by 8 object was a scalene triangle!

So now we have a program that is about as simple as a program can be, and for which even a good programmer is likely to leave almost half of the possible cases untested for. This means that in a complex program the likelihood of it being bug-free – with all cases tested – is in the slim to none category, with the real answer being a lot closer to none than to slim. Unlike Caesar's wife, no computer program can ever be completely above reproach.

Now, as it happens, it is hard for *any* system to really be above reproach. As an example, if you worked in a store as a kid, you know that when taking inventory the count was never perfect. No matter how many times you recounted, you rarely got the same result twice, so management lived with some small amount of error in the counting.

The same thing happens with voting, where there is a certain amount of error in the system. It is generally estimated to be between two and four percent. This means that if the US were imprudent enough to get rid of the electoral college – one of the better inventions of the Founding Fathers, for reasons not actually germane here – and the popular vote was close, the winner would be decided by system error.

To see this more clearly, imagine that 118,557,170 Americans voted in the recent presidential election (which they reportedly did), and exactly 59,278,585 voted for each of the two major candidates (which they may have done). What would the final tally show? Well, assuming a four percent error rate, with an exact tie, the winner could get as much as 64,020,872 votes, and the loser could get as little as 54,536,298 votes.

In fact, in this election 117,340,048 votes were *listed* as being cast for the two major candidates. Again assuming a four percent error rate and an exact tie of 58,670,024 for each candidate, the winner could show as many as 63,363,626 votes and the loser as few as 53,976,422 votes.

How about if we said the error was an un-realistic two percent? In looking at a tie the winner could get as many as 61,649,728 votes and the loser as few as 56,907,441 votes. On the listed votes for the two candidates, the winner could show as many as 61,016,825 votes and the loser as few as 56,323,223 votes.

How about if we look at the most reliable system, not implemented anywhere during this election, which is a paper ballot punched or marked, and then machine-verified for readability? (As we recall, this method tests to having a one percent error rate.) With a one percent error rate, given a tie the winner could show as many as 61,649,728 votes and the loser as few as 56,907,441 votes. On the listed votes for the two candidates, the winner could get as many as 60,464,157 votes and the loser as few as 58,093,013 votes. On the listed votes for the two candidates, the winner could get as many as 59,843,424 votes and the loser as few as 57,496,623 votes.

In fact, in this election Mr. Bush was listed as having 60,383,548 votes and Mr. Kerry as having 56,956,500 votes. These results are well within the range of system error. What does this mean? Since some of the small number of third-party votes probably were in error, no matter how you cut it the popular vote was, sadly, once again assuredly compromised by system error in the voting systems as implemented.

Now, do electronic voting machines make this better or worse? We have to look at three factors.

First, are electronic voting machines sufficiently accurate in terms of knowing that when we push a button the vote will go where it should? Based on the triangle story, it should come as no surprise to know that these machines seem to be a bit buggy, and thus will be accurate some of the time; possibly most of the time; but not all of the time.

Second, are they more or less intuitive to use than pulling down a lever, or punching a hole in a piece of paper? To answer this, we asked one of the people responsible for the original implementation of Citibank's ATMs what kind of entry error rates they were getting. He pointed out that this was not an entirely fair question, as there was a live bank employee in each ATM location to help those unfamiliar with the system. What was the error rate with someone there to help? About fifteen percent! Thus, although most people are by now well familiar with ATMs and touch screens, there will certainly be some voters who are not familiar with them. Plus, have you ever punched the wrong thing in an ATM? We certainly have!

A third factor is how easily can fraudsters change the results? (For your amusement, look at <http://blackboxvoting.org/baxter/baxterVPR.mov>.) For a

start, since we know that the programming of the device will have bugs, an electronic voting machine without a paper trail makes no sense whatsoever: There is no ability to check what the machine, with its *de facto* buggy code, says. And we *really* don't want everyone using the *same* un-auditable electronic voting machines, particularly if the machines are networked, as they surely will be. This is because when a bug is discovered, and it can be controlled from a distance, the entire voting process could end up in the hands of some clever teenager abroad.

Was there any tampering with voting machines that lack paper trails in this past election? We have no reason to suspect there was, but note that the lack of audit allowed the following to appear on the Internet, casting unnecessary doubts in the minds of some about the process itself.

- According to several independent sources, about 80 percent of all votes in America are counted by only two companies: Diebold and Election Systems & Software (ES&S). The founders of these two firms, Bob and Todd Urosevich, are brothers.
- Walden O'Dell, chief executive of Diebold Inc., told Republicans in an Aug. 14, 2003 fund-raising letter that he is "committed to helping Ohio deliver its electoral votes to the president next year."
- Prior to being elected U.S. senator from Nebraska, Republican Chuck Hagel was chairman of ES&S. In 2002, he was elected in a surprise upset, with votes counted by ES&S machines. According to published reports, the Senate Ethics Committee had questions about Hagel's financial ties to ES&S.
- California banned the use of Diebold machines because the security was so bad.
- There were wide discrepancies between exit polls and official results in Ohio during the 2004 presidential election.

All of these could have been eliminated by using machines with paper trails.

Is it technologically possible to have a paper trail in an electronic voting machine? Well, we know that Diebold makes electronic cash registers that keep a paper tape of what is rung up so that the manager can verify that there is some relationship between what should be in the drawer and what is actually in the drawer. If the paper tape starts at the beginning and ends at the end you are pretty sure that you have all the transactions, and that if the tape is torn you may have a problem. This is the same logic behind not

allowing police officers to tear numbered pages out of their log books: We really want to know what was written in the missing pages. One assumes that if a Diebold cash register can have a paper tape, a Diebold voting machine could, too. And if a Diebold cash register can allow the operator to see what is on the inaccessible tape, a Diebold voting machine could, too.

So, assuming that the actual vote is stored on the paper tape, and that, as in the better electronic cash registers, the voter can see what is on the paper (but not get at it) to make sure it reflects their actual vote, this system should work relatively as well as a mechanical device that produces a paper result. The paper will be the actual voting record, to which we can refer if there is any question about the electronic vote.

Only testing can tell whether electronic voting machines with paper audit trails could approach the reliability of having the voter punch or mark a (preferably well designed) paper ballot and then, before it is put into the ballot box, put it into an electronic scanner to make sure it is readable. It at least gets rid of the hanging chad problem and its kin, and just leaves associated data-entry and normal system error.

So, bottom line, can we reasonably trust an all-electronic voting machine, particularly one where the official count is something transmitted by the device to another computer, and where there is no paper ballot that is verifiable by the voter before leaving the voting booth, and available for count later? At this stage in both the development of computers and computer security, we must regretfully say that electronic voting machines with no paper backup are, unlike Caesar's wife, definitely **not** above reproach.

5. Real Stories from the Field — Sexual harassment policy as a tool, II

In the January 2003 issue of AEGIS, we wrote about sexual harassment policy as a tool in the business environment. A recent case we observed indicates that in many states, with new laws dealing with domestic abuse, sexual harassment can be used for non-business purposes.

This case took place in New York City, where the man in question had a rent controlled apartment that was coveted by a neighbor. This man ran a small business from his first-floor apartment, storing product in the basement.

One day the man was moving cartons from the hallway to the basement. The woman came into the hall and started yelling about the hall being cluttered. She then picked up cartons and started throwing them around. The man grabbed her to stop her. She eventually went into her apartment and the man continued putting the cartons in the basement.

Unfortunately for our poor victim, the woman called the police to complain that she had been assaulted. The police arrived, and reasonably (albeit incorrectly) reasoned that the two neighbors might have been in a relationship, which meant that they had no choice but to arrest the man.

While he was being booked, the woman filed a restraining order. She then got into the habit of leaving her door open. Every time he entered or left the building after his release he, *de jure*, violate the restraining order by walking by her open door. She would call the police, and he was arrested several more times.

While it is his (and apparently his attorney's) hope that by videoing his comings and goings, and showing that he is merely going to and from his apartment, and that she is deliberately leaving her door open simply to get him arrested, his case will be dismissed. We suspect that it is equally likely that he will be forced to leave his apartment, and that the woman will end up getting it, with the building giving it to her at a low rent to avoid negligent-action litigation.

It is clear that violence is a bad option on many levels, and should be avoided whenever possible. We, ourselves, would go to extremes to avoid violence, and indeed have on occasion followed the sage advice offered by Monty Python to "Run away! Run away!" in situations where violence might have been justified, but was avoidable.

When it is not possible, however, it is critical that a police complaint be filed. And that YOU be the one to file it first, because the person filing the first complaint is the complainant (the good guy) and the person who doesn't file first is the defendant (the bad guy). You want to be viewed as the good guy.

Had our victim immediately called the police, rather than continuing to put away cartons, his life would not now have been turned up-side down.

6. Book and Product Reviews

Second Wave Enterprise Resource Planning Systems

Edited by Graeme Shanks, Peter B. Seddon, Leslie P. Willcocks

Cambridge University Press ISBN: 0521819024 468 pages \$55.00

<http://titles.cambridge.org/catalogue.asp?isbn=0521819024>

+44 (0)1223 326050)

Enterprise-wide software systems rank right behind the internet as the most important information technologies to emerge in the last two decades.

Companies that have invest heavily in enterprise software such as SAP,

Oracle, PeopleSoft, Siebel, and i2 Corporation do so to gain better access to information help them make informed decisions. The difficulty for the licensee is which product to choose, and how to integrate the right programs for the requisite needs.

This book gives an overview of some of the very difficult decisions facing anyone who is using, or looking to implement, software for ERP. It is both an excellent resource for those involved in planning, and for senior management of those firms looking to build or buy ERP software.

Since enterprises spend around \$100 billion per annum on these systems, did they get what they wanted, or should they have gone to a custom system? The conclusion is that most organizations *can* use the canned programs, but even the purchased systems require customization. Other enterprises, whose needs are so specialized as to preclude stock systems, recommend either using the canned ESS for divisions and using a custom platform for integration, or building from scratch.

Business Owner's Legal Guide

Kevin Johnson, Esq.

Knowles Publishing ISBN: 1-932498-11-7 \$150.00

http://www.knowlespublishing.com/Merchant2/merchant.mv?Screen=PROD&Store_Code=817&Product_Code=52 1-800-299-0202

The object of a business law reference is to have the small business owner understand the fundamentals without counsel. We have looked at many business law references in the past, but have not reviewed them because they were written way above most business owner's ability to understand.

This loose-leaf binder contains laws, rules, and regulations directed at the small business owner. It has the detail needed to support what is said, but is written in such a way that all who read it can understand what the author is trying to convey. It covers the different type of entities, contracts – many different forms of contracts – what to expect in litigation, and the pains of grown and downsizing. The guide is worth room on the shelf to lean on, or to educate the business owner on the basics, so they can know the questions to ask, and gauge the quality of the answers.

7. Free-Subscription/Unsubscription/Copyright Information

•• AEGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2004 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.

- **OPSEC: The identification and protection of information that would give your competitors and adversaries an advantage.**
 - Sarbanes-Oxley compliance.
 - Protection of trade secrets and intellectual assets.
 - ◆ Anti-competitive intelligence.
 - ◆ Anti-economic espionage.
- **International financial investigations and due diligence consulting.**
 - Location and recovery of missing and hidden assets.
 - Establishing business relationships and strategic partnerships in Central and Eastern Europe, the offshore financial centers, Beijing and Shanghai, Central Asia, and Latin America and the Caribbean.
 - Anti-money laundering and financial fraud requirements under the *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001* and the *EU Revised Money Laundering Directive of 2001*.
- **Protection of management, staff, and families.**
 - In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.
 - When traveling and living overseas.
 - When transporting items of substantial value.

LUBRINCO identifies and quantifies threats and vulnerabilities, and their associated risk, then manages the vulnerabilities so you can transfer or live with the residual risk. We prevent disastrous financial loss to your company, and physical harm to you, your family, and your staff.

For information on **The LUBRINCO Group** and its services, or for the archive of all past issues of *ÆGIS* e-journal in PDF format, please go to <http://www.lubrinco.com/>.

To sign up for a **complimentary subscription** to *ÆGIS* e-journal or the *ÆGIS* e-journal PDF notification list, go to

<http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to ejournal@lubrinco.com.

To subscribe to our AvantGo channel, go to http://avantgo.com/channels/_add_channel.pl?cha_id=1773

To be removed from the subscription list, follow the instructions on the mailing you received, or send an e-mail to ejournal@lubrinco.com.

If you know of anyone else who should be receiving AEGIS 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 AEGIS 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 AEGIS 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 AEGIS 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 December 2004 AEGIS e-journal (© 2004 LUBRINCO & FEE), to be found at <http://www.lubrinco.com/>.

AEGIS 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 AEGIS 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.