



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 5 Number 11, November 2002

From the case files of

The LUBRINCO Group

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

and

Financial Examinations and Evaluations, Inc.

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

Due diligence outside North America and Western Europe? Call us!

This month's features:

- 1. Due Diligence — Assessing *know-your-customer* vulnerability**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — OPSEC: Operations or security?**
- 3. Executive Protection — John Wayne as a role model, or how to die sooner than you should**
- 4. Technical Issues — Know your sender, know your caller, and know that they know you**
- 5. Real Stories from the Field — Warning signs**
- 6. Book and Product Reviews — Find It Online 3rd Edition // Limited Liability Organizations // Inside the Tornado**
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Assessing *know-your-customer* vulnerability

There has been some concern on the part of both financial institutions and financial gatekeepers, that know-your-customer regulations would ultimately mean that huge amounts of money will have to be spent in the exercise of due diligence on every customer and in every transaction. This is not true.

We start with the understanding that no matter how good one is and how careful we are, mistakes will be made and something will eventually slip through. As unfortunate as this is (and often disastrous, as the resource-rich agencies such as CIA and FBI can attest), there is no way to close all avenues. What we can do, however, is have procedures in place that, when observed carefully, will prevent someone's slipping through who could have been filtered out with reasonable effort.

With know-your-customer procedures, as with all risk management, you want to take action where there is risk – risk equating to *likelihood* times *cost*. Put simply, if the cost of a failure is not high, then the risk cannot be high, and thus the cost of exercising due diligence should be appropriately low. As an example, this editor recently needed a hundred dollar bill to give as a present to a child for his birthday. The bank at which the five twenty-dollar bills were exchanged required a full-page form to be filled out. We have not seen this in any other bank. On a guess, this bank is drowning in paper, which will hinder compliance efforts against those who actually do present a danger. Their misdirected – but well-intentioned – efforts open them to the possibility of real losses.

You need to determine where you face risk that is sufficiently high to result in serious consequences to the company, and to devote the bulk of resources to that issue. The non-financial equivalent is the stealing of pens: While the probability of someone taking a pen from the office is high, most serious businesses would not devote as much effort to protecting pens as to protecting laptops. Our view is that know-your-customer procedures should be addressed with a similarly common-sense approach.

2. OPSEC, Economic Espionage, and Competitive Intelligence — OPSEC: Operations or security?

The identification and protection of critical but not trade-secret (or classified) information is known as OPSEC (short for *operations security*). In some cases, we have seen OPSEC being ignored within corporations because it was not clear who should be doing it. On one hand, the work

“operations” indicates it is an operational issue, and should perhaps be handled by someone in operations. On the other hand, the word “security” indicates that it should be handled by the security department. In other cases, its usefulness as a management tool is not understood and there is no perceived “need” for OPSEC, which is, in any case, still a fairly new concept in private industry, and virtually unknown outside the US, as far as we can determine.

Although these problems *could* be in theory handled, and in a perfect world *might* be handled by a security department, they generally aren't. We cannot think of a single high-risk problem where **The LUBRINCO Group** has ever been called in by an organization's security department, nor where have we been asked by the senior manager who hired us to work with the security department. Normally, security departments get short shrift and have been shoehorned into very limited areas of work dealing with physical security.

To illustrate the point, let's say your company is planning to invest \$50,000,000.00 in a business venture in China (an area in which we provide services). In theory, you could turn to your security department to oversee the exercise of due diligence, but you probably won't for a variety of reasons. Likewise, who are you like to call on first if an employee becomes violent? Human Resources, into whose bailiwick this falls as a personnel issue, or Security into whose bailiwick this falls because someone could get hurt? No matter what the org-chart says, prudence tells you to call Security. And how likely are you to call the people that handle the one issue to handle the other?

OPSEC presents the same kinds of issues. The logic is that there is “something to be protected – albeit something as intangible as information – so there is some justification for thinking of it as a security issue. We would argue, however, that it is largely a management issue: Identifying what is critical to the company and how the organization's actual adversaries might wish to acquire this information and use it is something that only management is in a position to know and assess.

Is your security department in a position to determine what precisely represents the company's “crown jewels?” The answer to this question lies largely in what your security department does. If what they do is largely handle physical security, and if most of their budget and time goes to guards and monitoring and alarm systems, then the likelihood of their having the internal expertise to handle OPSEC is low. If on the other hand, areas such as financial planning and oversight, financial due diligence, and executive

protection are handled by security, then the likelihood is greater that this would be within their scope.

The real danger lies in *nobody* dealing with OPSEC, because nobody knows what it is or who should be handling it. For most organizations of our acquaintance, lack of an OPSEC program is costing them quantifiable losses of cold, hard, cash. Whoever handles OPSEC (and we have no practical or emotional attachment as to where it should be handled), it needs to be handled by someone.

3. Executive Protection — John Wayne as a role model, or how to die sooner than you should

We were recently asked by an executive about training in defensive shooting, which, in our mind, means point shooting, about which we have written in the past (May 2000). While we, ourselves, do not carry or keep a gun for self-protection, we do teach point shooting, which can greatly increase one's chances of surviving an actual gunfight.

The problem is that this person shouldn't be getting into gunfights. The scope of the problem became clearer when he discussed the two scenarios in which he envisioned he might use a gun: Getting out of the car when stopped, and when he heard something go bump in the night at home.

In (or, actually, out of) the car

The first scenario was one in which he was stopped by bad guys when driving, and had to get out of the car and shoot it out with them.

Common sense says that it is generally foolish to trade a projectile that weighs 2000 pounds or more for one that weighs 250 grains or less.

The reason for this is that, as it happens, cars are very effective killing machines. In the U.S. alone, about 42,000 people a year are killed in or by automobiles. There is no more effective killing machine than an automobile (we exclude iatrogenic injury and other medical issues here, as well as the difficult issue of suicide by whatever cause.). As a comparison, 57,000 Americans died in the war in Viet Nam. And although Americans own more guns than automobiles, there are only 9,000 firearms deaths per year in the U.S. (although, in fairness, four times as many Americans die from gunshots than from SUV rollovers). Bottom line, running someone over with your car is a more effective way of making them stop doing bad things than is trying to hit them with a teeny bullet coming out of a wavering gun at the end of your shaky hand.

When you are in a car you want to stay in it if you can. You want to keep moving, and, if necessary, you want to use it as a weapon. Usually you have some initial period of time – frequently measured in seconds – in which you can use the car to drive away. With training you can move most blocking vehicles out of your way (we ignore here the airbag issue), and driving the car straight at a gunman usually makes him rethink his short-term plans.

The bad news is that if you are being ambushed, you will apparently not have noticed all the preparation that led up to the ambush, and may not be mentally prepared to run someone over, or drive your car through another car. And we may soon be watching the TV movie of the event, which will be entertaining to us, but less so for you and your loved ones.

Still and all, it is never too late to turn over a new leaf, and if the option of not being captured or killed seems attractive to you, then it is probably worth taking some new and daring steps toward your own survival. In this case one of the training courses in emergency driving, where you get to ram cars out of the way and do other really cool things, is a very good idea.

But what if you already have a driver? On a bet, your driver has probably never had the appropriate training. Plus, your driver is going to hesitate before wrecking a car that costs more than he earns in a year. You, yourself, may not be too happy to run someone over, either, but you may be less happy being kidnapped or dead, or having your family kidnapped or dead, and more willing to take the risk.

In terms of dealing with realistic risk, emergency driving training (which is like defensive driving training, but with the protective skills included) will be one of the best investments you can make, helping to keep you alive in both high risk and low-risk situations. Get training *now* in emergency driving techniques, and leave shooting for a leisure time activity!

In the house

The second scenario our inquiring executive presented was hearing noises in the house and going downstairs to investigate, gun in hand. We recommend strongly against this: Some time ago someone was running rôle playing of this scenario, and, out of several ***thousand*** runs, only three householders exited the simulation alive. These are not good odds!

The reason the odds are so bad in doing your own house clearing is that you don't know who is in the house and what you need to do about them. If it is your child who has wandered in late, or a neighbor's child, or a housekeeper, or any of a host of other people who don't pose a threat, shooting them will

change your life immediately and drastically for the worse. If it is a bad guy, you are at a very serious disadvantage because you have to:

- Find the intruder.
- Figure out who they are.
- Decide if they are a threat.
- Decide what you want to do.
- Do it.

The bad guy, on the other hand, knows that anyone else is not him, and can simply shoot, with all of the intermediate, time consuming, decision steps totally removed.

So what should our guy do in this case, as an alternative to getting himself killed? He should gather everyone up into one pre-selected and prepared room (that has both an ordinary telephone, plus a mobile phone in case the phone wires are cut or the phone simply taken off the hook), lock the door, and call the police. It is not inappropriate to be behind something solid, with your gun pointing at the door, and if someone tries to get in, to yell, “I have a gun and have called the police.” If the response is “Oh, Daddy, don’t be so paranoid!” you may not have a serious problem after all. If it is intruders and they decide to break the door down you will likely be happy to have the gun, or to wish you had a stronger door.

As a side note, in many jurisdictions the police won’t knock down your door, so you will need to toss them a key. Since this is likely to be at night, it is a good idea to have a key attached to a Cyclume Stick, so the police can easily see it, and find it even if it falls in bushes or buries itself in snow.

If you are really concerned, or live in an area where an attack is a real possibility, it is also worth making sure your bedroom – or whichever other room you choose to make your safe room – has a strong door that can’t be easily broken down, and in some cases, you may want to build a fortified and secure safe room. And if you do build a safe room, don’t be so quick to rent the place to Jodie Foster....

4. Technical Issues — Know your sender, know your caller, and know that they know you

Who are you?

We have recently begun receiving spam e-mail from – of all people – ourselves! Well, that’s at least what it says in the header of the e-mail. This

has been a little puzzling, as we have neither Viagra nor low mortgage rates to sell. While the forging of header information is illegal in many states, it is easy to do and hard to police.

The danger of this is that if people see e-mail coming from us they may, not unreasonably, think it is from us. This is, of course, one of the ways certain viruses and worms work: They steal your address book and send out messages from your machine. In this case, this was not what was happening. It was merely spam.

Where are you calling?

We have issued prior warnings on camouflaged pay-per-call numbers. As an example, area codes in the Caribbean look just like American area codes, and use the same country code of 1. Some of these numbers because of the vagaries of international law, it is not required, in America, to identify itself as a pay-per-call area code. You might receive a voicemail, e-mail, or other communiqué with a message to call a number with an unknown area code. According to one source, if they keep you on the line a few minutes, a call to an international pay-per-call number could cost you as much as \$100.00! If you do fall for this scam, your local phone company will be of little assistance, simply because they won't want to get involved in your dispute and will say they are only providing the billing for a foreign company and then refer you to that company which will argue they have done nothing wrong. Check with the operator before calling any number whose area code you don't know.

Who knows whom you have called, and whom they have called?

Another issue in telephone calls is the fact that when you call someone, a record is kept of this. Why would you care any more about this than about other invasions of your privacy? Mostly you don't, but keep in mind that very sophisticated software exists to make tenuous connections clear. As an example, in Colombia, where the bad guys have more money than the government, modern data mining software is used to locate police informers, who can then be killed. While the connections are so tenuous and fifth-hand that they cannot be seen with the naked eye, if they, er, acquire all the phone records of a country and put them into their large and expensive computer to be massaged using very sophisticated software by their highly-paid and highly-qualified staff, they can come up with some very interesting conclusions, which will more easily help them decide whom to kill.

Where have you browsed?

By the same token, unless you use a proxy server to hide who you are, you will leave traces of where you have been on the web. Do you care who knows what web sites you have visited? Maybe yes, maybe no. But it is something you should know about. You can look at <http://www.inetprivacy.com/welcome.htm> to see one anonymous proxy server program, and to find links about how anonymous your browsing is. You will be shocked at how much information you give away as you surf your way across the internet.

5. Real Stories from the Field — Warning signs

As part of our ongoing effort to help clients identify and deal with risk, we have been working to develop a protocol to help quickly pinpoint areas that merit further examination. What we are refining is a detailed checklist that we can go through with company management, accompanied by a physical inspection, covering a wide variety of areas where the company may have vulnerabilities. While there is little depth to the survey, this is appropriate, since what we are trying to identify are those areas that merit a more in-depth examination. This allows us to eliminate at the beginning those areas that may not be perfect, but are probably adequate, and concentrate on those areas which are sub-standard – or which are felt to be particularly critical. This allows management to make an informed decision as to where scarce dollars should be spent. Since this initial pass is wide but shallow, it can be done quickly and cost-effectively, and offers our clients a valuable resource at low cost.

The value of this tool has already proven itself in several cases in which we have spotted areas of significant vulnerability on the first pass, including one case in which we noted an area of great physical risk. As a result of the preliminary assessment, none of our client's staff was involved in the homicide that subsequently took place. If your firm is interested in participating in this experiment, please let us know.

6. Book and Product Reviews

Find It Online 3rd Edition

Alan M. Schlein

Facts On Demand Press ISBN: 1-889150-29-0 564 pages

<http://www.brbpub.com/> 1-800-929-3811 \$19.95

This is a neat book. Having used the *information superhighway* since the 2400 baud modem days, it was clear that one thing the Internet has needed was an information road map for the professional researcher. Search engines, while good, will miss a lot of the major information locations in the first ten plus hits if those information locations have low click through or usage rates.

The way the book is set up reminds us of good cookbooks: There is basic information about ingredients, recipes, and how to vary them, plus a good index. An appropriate amount of the book is spent on simple tasks such as the foundation for the searches and information organization. It is well worth the \$19.95 and will save you that and more directing you to the information you want, rather than merely what the weekend surfers like to see. Some of the useful things found with this book were translation sites (sites that will automatically translate web sites from one language into another), as well as good links for business information for both U.S.-based businesses and European and Asian businesses.

Limited Liability Organizations

William Price, J.D.

Specialty Technical Publishers <http://www.stpub.com/> (604) 983-3445.

Loose-leaf Binder \$390

CD-ROM \$390

Binder & CD-ROM \$590.

The LLC in the United States was first proposed by the Wyoming Legislature and passed into law in 1977. The LLC was to be treated as a corporation for liability issues and as a partnership for taxation issues. It was a transition from the Subchapter S Corporation, that had a limit on membership and size, to an entity with few limits. The publication covers new types of entities, how they can be used, and how they compare with other, more familiar types of entities, such as corporations, partnerships, and trusts. The tax treatment of the LLC is discussed for both U.S. federal taxes, as well as states that have different treatments. It gives a good discussion of litigation prevention that we have not seen in other publication. It is filled with comprehensive checklists for formation, operation, and tax issues.

The manual is heavily researched, and we learned a few things we didn't know about the history of companies. This may not seem like much, but many of the similar books submitted here on similar topics have been returned to their publisher un-reviewed since they missed the mark. If you

look into entities, form entities, or conduct due diligence on entities, this will be an important resource.

Inside the Tornado:

Marketing Strategies from Silicon Valley's Cutting Edge

Geoffrey A. Moore

Harper Perennial ISBN: 0-88730-824-4 272 pages \$17.

If we were asked to recommend a book on marketing, and could only recommend one book on marketing, it would likely be this one. This book, recommended to us by the former head of corporate communications for a major telecom provider who prudently took his money and ran, provides the clearest insight we have seen into the cycles of technology change and acceptance that sweep through the modern business world.

The book is important because, if you do not understand how technology shifts affect the market, your business strategy is doomed to fail. After reading this book many things become clear, from the success and failures of various technologies to why certain companies have engaged in financial hanky-panky. Even for a small and non-technological organization such as The LUBRINCO Group, *Inside the Tornado* has helped us clarify our marketing strategy.

Moore breaks the technology adoption cycle into six pieces, which we quote directly from the book:

1. *The early market*, a time of great excitement when customers are technology enthusiasts and visionaries looking to be first to get on board with the new paradigm.
2. *The Chasm*, a time of great despair, when the early-market's interest wanes but the mainstream market is still not comfortable with the immaturity of the solutions available.
3. *The Bowling Alley*, a period of niche-based adoption in advance of the general marketplace, driven by compelling customer needs and the willingness of vendors to craft niche-specific whole products.
4. *The Tornado*, a period of mass-market market adoption, when the general marketplace switches over to the new infrastructure paradigm.
5. *Main Street*, a period of aftermarket development, when the base infrastructure has been deployed and the goal now is to flesh out its potential.

6. *End of Life*, which can come all too soon in high tech because of the semiconductor engine driving price/performance to unheard levels, enabling wholly new paradigms to come to market and supplant the leaders who themselves had only just arrived.

This is interesting, but why do we care? Because it turns out that as we go from phase to phase our sales, marketing, management, and production emphasis changes, and, if you are selling, marketing, managing, and producing in a manner inappropriate to the phase you are in, you will at best lose a lot of money or at worst be out of business. Essentially this comes down to a management issue. More to the point, it comes down to the fact that the management that succeeds in one phase may not be appropriate in another phase. Can you change your management style to match the phase you are in? Sure, assuming you are aware that there are different phases, and what is needed in each, and can change your temperament appropriately. If not, you are likely to do silly things, many of which can point you in the direction of being out of business or in jail over accounting issues.

There are some other issues regarding misunderstanding how one ought to deal with the new technological paradigm shifts. As an example, the executive who originally recommended the book noted that the book says that during the tornado period “This demand forces vendors into a mass-market mode where operational excellence is demanded in order to meet the “just ship” imperative without generating returned merchandise. Taking time out to customize a solution for a particular customer is anathema now, slowing down the tornado and introducing the risk of a glitch, so customer intimacy must take the backseat.” Somehow this has been interpreted as saying that you can get away with a shoddy product or poor customer service.

How common is this, and does it offer an opportunity for those who deliver good service to gain over those who provide bad service? We decided to see if we could find any issues of bad service from a single company that involved more than one of our staff members, indicating a systemic problem. We succeeded.

Some time ago one of the editors bought an Archos Jukebox Recorder from Gateway. This is a self-contained, battery powered hard drive that can be used to store data (you connect it to your computer with a USB cable, and it appears as a regular drive). It can also store MP3 music files – a lot of them – that can be played either with a headset or connected to a sound system. It worked well for a while, but then started having problems. We called Gateway who suggested, not unreasonably, that we contact Archos. We sent

Archos technical support an email. Then another. Eventually we called, and ended up speaking with their head of corporate communications, who said we should e-mail her and the head of technical support. As of the time this article is being written, over a hundred and thirty (130) e-mails have gone to Archos, without a single written response. We spoke to their competitors at SonicBlue and Creative Labs, who each said that it was their policy to deal with technical problems immediately, both to have happy customers and to make sure this was not a design problem that needed to be dealt with to prevent further, greater, problems.

While Archos was an interesting study in poor customer service, it is a small company and of no particular significance. Gateway, on the other hand, is a larger company. Gateway customer service said that while Gateway sells the Archos player, they take no responsibility for products they sell which are manufactured by others.

Lest you think that this was one isolated fluke, another of the editors of this journal had purchased a computer from Gateway, which wouldn't work with broadband. Gateway customer service insisted the serial number on the machine didn't show as being sold, and refused to help. The machine was dumped and replaced with one for which customer service was available.

Finally, one of our editors had purchased a Gateway computer whose monitor died two years after purchase. This was out of warranty, and clearly not within the responsibility of Gateway, which nonetheless suggested that the monitor be taken to one of their stores in Manhattan for out-of-warranty repair. The address was given; the monitor lugged down to a taxi and brought over to the store, which said they didn't do repairs, and that it needed to be brought to a different store. It was put in another taxi and, three quarters of an hour later, reached the next store, which said, sorry, we don't service monitors, nor will we throw it out for you.

We suspect that Gateway has mis-estimated both the importance of customer service and their position in the paradigm-shift cycle. On the off chance that this was an industry standard, we spoke with Dell, who said that they believe they would have tried to deal with each of these problems in a manner that would have been satisfactory both to them and to the customer.

It is interesting to note that there is now an *expectation* of poor service. As an example, a guitarist mentioned on a public forum that a set of strings had peeled and said how angry he was about this. We asked if he had called the manufacturer, and he said that the thought had never even crossed his mind. At my suggestion he called the manufacturer, E. & O. Mari (maker of La

Bella strings), who, of course immediately replaced them. We suspect this guitarist will be quick to recommend La Bella strings in the future.

As another example of good service, this author purchased a Halliburton case in 1964, and recently one of the clasps failed. A call was made to Zero Halliburton (current manufacturer of the cases) with the intent of buying a new clasp. It arrived, free of charge, a few days later. As an interesting side note, we have heard that some years ago a plane captured by terrorists was emptied of passengers and blown-up. The only surviving usable articles were three Halliburton cases. We use these cases extensively, with, as noted, some of them being nearly half a century old.

But Halliburton is not the only company that makes things that last and provides good service. A friend bought a Louis Vuitton hatbox at an auction. The case, made in the 19th century, had long since lost its key. Vuitton, upon being given the lock number, replaced the key promptly, at no cost, even though its owner was perfectly willing to pay for it.

This kind of behavior, one way or the other, is part of a corporation's culture. This author once did work for Simmons Corporation, manufacturers of Beautyrest mattresses. At that time, the head of the company would meet early Monday morning with the company's treasurer, general council, and the rest of the executive staff to personally review every letter of complaint that had come in, and to follow up on past complaints to see that they were settled to the satisfaction of the customer.

And if we were a corporation that needed commercial printing, we would speak with Proof Perfect in New York City, which goes way beyond normal customer service in producing happy clients satisfied with a job well done.

Finally, we note that Gateway, Archos, and other such New Economy companies are just that: New. Many of them – just look around – have not survived even 10 years. Customer service is not an outdated concept. Halliburton, Louis Vuitton, etc. are still around and still in business. There is a message here somewhere....

7. Free-Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2002 by The **LUBRINCO** Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com), L. Burke Files (LBFiles@feeinc.com), and Terry Phillips (TPhillips@aegisjournal.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.

- **Identification, valuation, and protection of intellectual assets and critical information.**
 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 is the leading private sector provider of 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.aegisjournal.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 subscribe@aegisjournal.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 unsubscribe@aegisjournal.com.

If you know of anyone else who should be receiving **ÆGIS**, please send their e-mail address to subscribe@aegisjournal.com.

If there is a topic that you would like to know more about, send it to editor@aegisjournal.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 editor@aegisjournal.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 **ÆGIS** Web site is included. This should be in the form

Article Title, from the November 2002 **ÆGIS** (© 2002 **LUBRINCO** & FEEINC), to be found at <http://www.aegisjournal.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.