



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 5 Number 7, July 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 — Beware of outgoing mail**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Spooks in the rag trade**
- 3. Executive Protection — What constitutes suspicious behavior? And what do you do about it?**
- 4. Technical Issues — On arming pilots**
- 5. Real Stories from the Field — How terrorism works, and what we should (and shouldn't) do about it**
- 6. Book and Product Reviews — Voicestream G100 iStream PC Card Science and Litigation**
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Beware of outgoing mail

When most of us think of criminals using the postal system, we generally think of *incoming* mail being a concern. Organizations have been spending a great deal of time, effort, and money to identify incoming packages that might contain explosives or biological weapons. This has opened up the possibility of a risk that has been overlooked by some mail departments: Outgoing mail. Well, *returned* outgoing mail, that is to say.

If you drop a package into a public mailbox, and it weighs more than 16 ounces, there is an increasingly great probability that the package will not be delivered. Rather, it will be slapped with a sticker saying it needs to be handed to a live postal worker at a post office, and then returned to whatever entity is listed on the return address as the sender.

A package weighing over 16 ounces is not suspiciously large. It can be a relatively full Priority Mail cardboard envelope. And, in truth, mail gets returned fairly frequently for a variety of innocent reasons (such as being misaddressed or lacking sufficient postage). So what happens when a small returned package hits your mailroom? If it has your company's return label, is your mail department suspicious? If it has a valid company label but no person's name on it, is it opened to see who sent it? If it does have a name typed on the corporate label, will it be returned to that person's office?

From the criminal perspective, co-opting the Postal Service in this way – making the USPS the unwitting participant in a crime – is qualitatively different from merely using them as the carrier of the package, and doubles the chances of success. Either the package is delivered, in which case the receiver needs to analyze the relative danger or innocence of the package, or it will now be returned, in which case the putative sender has to analyze its relative danger or innocence – something that most don't think about.

In either case, it is another factor that needs to be considered, and policy on this issue needs to be put in place within your organization.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Spooks in the rag trade

One industry that needs to deal with economic espionage is the fashion industry. Obviously, once a design hits the showroom it is easy for competitors to copy it. (Any legitimate – and some illegitimate – buyers get to see the designs.) But in the fashion industry, as in most other industries, the

problems start much earlier. And the earlier a competitor can get your designs, the more likely you are to see your designs introduced by your competitors.

The fashion industry is subtly different from other industries, in that in many cases the habit of design theft is so endemic that it is almost assumed to be the norm. Even so, there are three primary sources of loss. The first is an employee who moves from company to company, taking design information with him. A variation of this is a current employee who takes the design to a small production house, has samples made, and then has someone else take the samples to the buyers. In either case – employee or ex-employee – your design is sold before it hits your showroom.

Another area of leakage is an employee being bribed by competitors to sell your designs. As happens in many companies, the fashion industry is one in which people lower-down on the food chain are paid relatively modestly, put in long hours, and get no overtime. While the combination of wanting more money combined with resentment at what could be perceived as poor treatment might not induce employees to commit criminal acts, it might at least incline them not to report competitors who try to bribe them, particularly if there is no company policy on this issue.

A third area of leakage is out and out pilfering – people simply walking in and stealing. We have been in companies where there was no access control, and anyone could – and apparently sometimes did – simply walk in and take or copy anything they wished to have. We will not even discuss here the issue of tradesmen and cleaners who are given unfettered access to both designs and samples left unattended, and design documents that are discarded unshredded with no thought whatsoever as to their value.

There are a number of things that can be done to reduce the level of theft, none of which are unique to the fashion industry. The easiest to deal with includes the obvious steps of putting in sensible access control, having clauses in contracts which deal with this issue, shredding design documents and drawings rather than throwing them out, and making sure you know your employees, suppliers, and contractors.

That done, the normal OPSEC process will allow you to identify what information needs to be protected, and from whom. When you know what needs to be protected and from whom it needs to be protected, you can start deciding who should be able to see it (and who shouldn't) and when they should see it (and when they shouldn't). In addition, you can also put in the appropriate countermeasures to protect the designs from outside theft, as well as dealing with the issue of insider theft.

Keep in mind that until your designs hit the showroom, they are trade secrets. As such, if you take reasonable and appropriate steps to protect them, their theft is covered by *The Economic Espionage act of 1996*. This means that you can, if necessary, bring the Feds in to help when designs are stolen. However, we race to point out that it is much better to keep them from being stolen in the first place.

OPSEC is a process that could substantially reduce loss within the fashion industry, and with so little disruption and at such low cost as to go almost unnoticed. However, OPSEC is pretty much unknown in the industry, and so we expect to see losses continue unabated.

3. Executive Protection — What constitutes suspicious behavior? And what do you do about it?

One of the things that we have puzzled about recently is the instruction to employees and the man-on-the-street to report suspicious behavior. We encourage that attitude of alertness on the part of every citizen. However, those instructions need to be accompanied by some explanation of what constitutes “suspicious behavior” to allow the uninitiated to correctly recognize it! Suspicious behavior falls into three categories.

Suspicious things

One is the appearance of *things* in places where they should not be. As an extreme example, some time ago someone in Bogotá noticed a heavily laden (and driverless) truck sitting in an area where trucks don’t usually sit. This was reported to a police officer, who asked himself if there were anything happening in the area which should cause him to be concerned about the truck. He remembered that the head of F-2 (a government security service) would be driving past there. He called the bomb squad who found the truck to be filled with explosives.

Other objects that might be obviously suspicious would be things unaccountably left near an air intake in a building, or packages, boxes, or other containers in places where they shouldn’t be. As an example, a friend of ours was walking by an Israeli bank in Manhattan one evening and noticed a large paper bag sitting next to the wall outside the bank. He tapped on the window to attract the attention of a cleaning person and pointed to the package. The cleaner turned a bit pale, thanked him, and told him they would follow up on it. While it was probably someone’s abandoned Chinese

takeout, our friend did the right thing: He saw something, he told someone, and they did something.

Even when it turns out to be nothing bad, that doesn't matter. A friend in EOD (Explosive Ordnance Devices, also known as the bomb squad) tells us that no matter what he may say in the moment, he would much rather be called out every night on a false alarm than pick up body parts because someone didn't call for fear of looking silly.

Suspicious people

Besides objects that are suspicious, we need to deal with *people* who are suspicious. In this case, suspicious generally means one of three things.

Strange Behavior

The first and most obvious suspicious person is someone behaving strangely. Strangely may mean that someone is doing something unexpected, such as working in an area where work is not generally done. (Remember that wearing a uniform or carrying a clipboard does not mean the people are who they appear to be.) Or it can mean that you open the door at your local Stop-and-Rob (er, convenience store) and notice that all the customers are standing still, which could well be a clue that you shouldn't go in while the place is being robbed. Or it could mean that you observe, as did ferry operators in San Francisco, someone described as a Middle Eastern man who boarded a ferry to Alcatraz, but did not leave the boat when it reached the island. Instead, the man videotaped boat traffic and used a stopwatch to time the route. A suspicious person can also mean someone whom you don't know somewhere that only people you *do* know should be. Thus, if you see a stranger working at a terminal in your office, you should ask who they are, what they are doing, and tell someone about it. As an example, one company hired us to test their security. We observed the people going in and out. We then dressed much as they did, walked into the facility, signed onto their computer system using the default system passwords which had never been removed, and sent ourselves a lot of their critical customer data. Nobody asked who we were or what we were doing.

Correlation over time

Repeated sightings of the same individuals is the second thing that should also send your antenna up. For example, if you see the same people in or near the same place over time. You see people sitting on a bench in front of

your office one day. The next day, you see them sitting in a car near the office. The day after that, you see them at a newsstand near your office. This should be reported to someone.

Correlation over distance

The third variant on this theme is to see the same people in different places. You might see people working near your home in the morning. Later, you see them in a car near your office. Later still, you see them sitting in the same restaurant in which you are eating.

Is it, by definition, suspicious if you see people behaving oddly, or the same people in different places or at different times? Yes! In the intelligence world, coincidence is seeing something or someone once, perhaps twice; three times is no longer a coincidence. It is an alert. Why? Because in order to do bad things, whether they be acts of terrorism, kidnappings, robberies, or almost anything else, there are at least two early stages in which the bad guys have to come out of the woodwork and look to see what is happening in the world they wish to enter and disrupt. In general there is a preliminary effort at surveillance in which unsuitable or uninteresting targets are eliminated. This is often done by low-level, relatively inexperienced people who are likely to be a bit obvious if you are alert. This is followed by a second period of surveillance, often by more experienced people, to firm up plans, establish routes and patterns of the target and identify opportunities.

If you see people behaving strangely, or the same people in different places or at different times are they, by definition, bad guys? No, but they are suspicious, and it is better to find out one way or the other, and as early as possible, if they are a threat.

Suspicious feelings

The final category of suspiciousness is a gut feeling that something is wrong. If something *seems* wrong, then there is a good (albeit not infallible) chance that something *is* wrong. We have, as civilized people, developed extremely sophisticated mechanisms for rationalizing these feelings away, but those protective animal instincts are still there and we unconsciously note and process signals that put our antenna up when something bad is going on. Ignoring these feelings can lead, literally, to disaster. Don't ignore your feelings.

In the end, the process of dealing with suspicion is a straightforward three-step process:

1. See something

2. Tell someone
3. Do something

In the wake of almost every disastrous event, when the pieces are put together, we discover that we had enough information to deal with the problem in advance, if only all the suspicious activity that had been seen by people had been reported and followed-up on. Sometimes, of course, this doesn't work, either because all the relevant information is not reported, or because it is not all in one place, or worst of all, simply because it is not followed-up on.

Mort Sahl, on one of his records, had a story about the FBI interviewing people in the apartment building in Greenwich Village where Colonel Abel lived (and yes, we do know he really lived in Brooklyn). If memory serves, the conversation always went something like:

“Did you know the man who lived in 301?”

“Oh, you mean Colonel Abel, the Russian spy?”

“How did you know he was a Russian spy?”

“Well, when he moved in we asked who he was and what he did, and he said he was Colonel Abel, and that he was a Russian spy.”

“Why didn't you report it?”

“Well, we figure, that's the Village for you....”

We should be able to do better than this in today's world., especially if we

1. See something
2. Tell someone
3. Do something

4. Technical Issues — On arming pilots

The arming of American commercial pilots has an interesting history. An FAA rule was adopted in the early 1960s to allow pilots to carry guns on planes. The rule required airlines to apply to the agency for their pilots to carry guns in cockpits and for the airlines to put pilots through an agency-approved firearms training course. No airline ever applied, and the rule was dropped in July 2001.

Pilots seem to be generally in favor of the option to have guns available. (There were at least two incidents in which armed pilots prevented

hijackings.) Many are ex-military and have some familiarity with guns, and feel that if they are responsible enough to be entrusted with responsibility for the plane and its passengers, they are responsible enough to operate a gun. Many appear to believe that, as happens with guns in the home, the mere possibility of the presence of a gun convinces bad people to look for some other way to cause trouble. They also know that if they were to deal with a problem, rather than flying the plane (although the co-pilot can fly), the plane isn't going to fall out of the sky. Even if they were to shoot a hole in the plane it still wouldn't fall out of the sky and the passengers won't be sucked out or subjected to catastrophic turbulence.

Airlines are not crazy about the idea of pilots carrying guns, because if one of their employees were to shoot a non-terrorist, the airline would face great liability. If we go to the official national fallback plan, where the plane is shot out of the air by an F16, the liability of the airline is substantially less. While the issue of liability could undoubtedly be addressed through legislation, it is unlikely that the airlines will ever be supporters of this idea.

For those involved with Air Marshals, having armed people on board is counter-productive on a turf basis. If you can field 90,000 Air Marshals you have a very significant agency with a very significant budget, and it is potentially destructive to have your headcount and budget eaten away by other agencies, pilots, or police officers.

Those who are against civilian ownership of guns in general are, well, against civilian ownership of guns in general, and feel that the presence of guns in the hands of anyone other than the government is simply wrong.

Those who are pro-gun feel that the presence of guns on planes increases the uncertainty of potential hijackers, inducing them to do something else. This group generally feels that pilots should be armed if they so choose, and that police officers should be allowed to carry their guns onboard. While some firearms instructors question the wisdom of this, noting that the average department has less than four hours of firearms training per year, this rather misses the point. The intention is not to have a gunfight; it is to make the target undesirable for criminals.

In fact, the issue is rather moot. We are clearly in no more danger today than we were on September 10th, and our needs did not mysteriously change on the 11th. If anything, the risk of hijacking has lessened, as passengers no longer believe that, when facing danger, they should sit quietly without resisting. Nobody, armed or unarmed, is likely to be able to take over an American flagship in the foreseeable future. We could easily close down all

inspection stations and allow anyone with a legally-owned gun, and with all the knives they usually carry, to get on planes with no decrease in safety, but probably without much increase in air safety, either.

Current air security, which appears to have been designed to give the impression of doing something, rather than to actually improve security, has more flaws than virtues. Indeed, airport heads recently went on record that bomb-testing machinery will be expensive, will soon be outdated, work poorly, and create dangerous congestion. A serious argument can be made that shutting down inspection stations would save billions in cost and would markedly speed up travel; and that many who have chosen to drive rather than fly might return to air travel, thus stemming the increasing number of travel deaths we anticipate coming from increased driving. But don't count on this happening soon.

5. Real Stories from the Field — How terrorism works, and what we should (and shouldn't) do about it

Terrorism is very much on everyone's mind these days. It is not our intent to discuss the politics of the Middle East here, the rightness or wrongness of any of the participants, or the nature of good and evil. Rather, it is to remind us that terrorism – criminal acts that deliberately hurt innocents for political reasons – is something we should not tolerate. We would also like to remind ourselves that the reaction to terrorism can be as destructive as terrorism itself, and that anti- and counter-terrorism policies must therefore be implemented with great caution.

While the *function* of terrorism is to terrorize, the *goal* is to change political behavior. There are two types of changes that might be desired by terrorists as a result of terrorism: Transforming a society and changing its views on some political issue.

Transforming a society

The first goal of terrorism is to transform in some way the country being terrorized. There are a number of reasons terrorists might wish to transform a society. One is to make the country more open to a political change desired by the terrorists.

How does this change take place? Countries that are the victims of terrorism tend to become more politically restrictive as they attempt to curtail the terrorists' use of available freedoms through increasingly intrusive police powers, and increasingly intrusive incursion into personal liberties, all in the name of protecting freedom. These restrictions always weaken freedom and

can eventually move democracies toward dictatorship. In many cases, as the country becomes more controlling, the citizens become more restive, more unhappy with the political structure, and more willing to consider change of political structure. This is particularly true as the civil rights of citizens are abrogated, and particularly true if the police or military start to use kidnapping and torture as investigative tools.

It is an unfortunate truth that there is a natural conflict between freedom and security, with citizens wanting more freedom and government wanting more security. This author remembers when Miranda came on the scene and many in the police world believe that they would never again be able to make a successful arrest and conviction. We see much the same philosophical conflict now, as we struggle to figure out how to deal appropriately with those criminals willing to use our own system against us.

Another goal of terrorism is to focus the attention of the targeted country inward, making it more isolationist. By removing its influence abroad, weaker societies can fall prey to the political masters of the terrorists more easily.

A third goal – vengeance – is that of the terrorist like Ted Kaczynski who is merely angry (or crazy), and wishes to cause terror in order to get even.

From the point of view of a democracy, the greatest risk of terrorism is neither the killing of its citizens nor the destruction of its infrastructure. Rather, it is the destruction of its social values that is most to be feared.

Influencing the decision making process

The second way change takes place is by causing citizens to make political decisions in hopes of ending the terrorism. The most obvious way this happens is by making the victims afraid, so they will walk away from an issue or change their policy. The danger for the terrorists is that they will make their victims angry, and that their anger will push them to find the terrorists and kill them.

The other way this happens is to change the victims' belief structure, so that the terrorism turns them from being the terrorists' enemies to being their supporters. The term *Stockholm syndrome* was coined after four hostages were taken and kept captive for six days in a failed robbery in 1973 at a branch of Kreditbanken in Stockholm. During the rescue, the hostages actively resisted being rescued. After being released, they raised money for the defense of their captors, and refused to testify against them in court. It is this type of transfer of allegiance after an incident of captivity that is now termed the Stockholm syndrome.

How unique is this from a psychological view? Not very!

One of the techniques used to placate abusers is to try to keep them happy. Because of this, there ends up being a difference between the participants' beliefs and their actions. This conflict is a type of *cognitive dissonance*: a dissonance between thought and behavior. Cognitive dissonance theory tells us that when there is a clash between people's behavior and their beliefs, they will most easily adapt by changing their beliefs. We see this in everything from the way abused spouses ("Since I put up with this I must really love him") and children (if you aren't sure which is the abusing parent, put the child in a room with both parents: The parent to whom the child runs is likely to be the abuser) identify with their abuser, to the way politicians underpay their campaign staff ("since I am working so hard with so little reward I must really believe in him"), to captives becoming the allies of their captors. We also see it in the way people react to terrorism.

In the US, for example, one might have expected a near-total rejection of the Palestinian cause. In fact, while nobody is particularly happy about the destruction of the World Trade Center or the attack on the Pentagon, there is a shocking acceptance of the legitimacy of both the suicide bombings in Israel and the attacks on the US. Instead of being seen as criminal acts, they are discussed in some circles as a justifiable part of the political process. This extends from the government at the top, which has classified what happened as "an act of war" rather than treating it as a crime, down to the bottom, with the June 2002 Harpers noting that the Gallup Organization reports that a horrifying **five percent of Americans say that the September 11 attacks were "totally justifiable."**

Is this view likely to influence our dealings with terrorism? It already has.

Dealing with terrorism

How, then, should we deal with terrorism, particularly as a secondary target, such as we are when dealing with the Mideast? Sadly, nobody knows. We can look at examples of how terrorism has been dealt with in modern times, and still get no clues. Israel has spent a lot of time trying to deal with terrorism, and the bombs still keep going off. Even if you look at a strained example such as Nazi Germany attempting to crush resistance, we see that even in an environment bereft of social constraints these activities were not stopped

On the one hand, we know that we should not tolerate terrorism (though we do), nor those countries and individuals who sponsor it (though we do).

Unfortunately, nobody really yet has a grasp of how to implement these non-toleration concepts.

On the other hand, we also know that the conventional approaches to dealing with terrorism don't work very well (In a recent article in Newsweek, Jack Devine, a former CIA associate deputy operations director, is quoted as saying "The truth is that [with new homeland security] we'll improve defensively by maybe 7 percent or 10 percent."), but *do* cause social problems, which means we ought to be more than a bit chary about implementing conventional programs, which are likely to be socially destructive without producing any real benefit. Because of this difficulty, we need to stop taking action merely to give the impression that we are doing something.

Rather, we should be gathering the best and the brightest to try to find new approaches. We also need to be willing to try new approaches, and, if they don't work out, to rescind them and try again, rather than leaving failed and socially destructive policies in place.

In looking at possible measures to implement, we need to ask the five questions that should be asked when considering *any* security measure:

1. What problem is the measure trying to solve?
2. How can it fail in practice?
3. Given the failure modes, how well does it solve the problem?
4. What are the costs, both financial and **social**, associated with it?
5. Given the effectiveness and costs, is the measure worth it?

6. Book and Product Reviews

Voicestream G100 iStream PC Card (Type II PC Card) and GPRS Service
Voicestream Wireless

<http://www.voicestream.com/products/devices/cards.asp>

\$249.99

Service costs:

\$19.99 per month: 5 Megabytes (MB) (90 web pages or 850 e-mails) plus 300 Ping Pong™ text messages. \$5.00 per additional MB

\$39.99 per month: 10 Megabytes (MB) (180 web pages or 1700 e-mails) plus 300 Ping Pong™ text messages. \$4.00 per additional MB

\$59.99 per month: 20 Megabytes (MB) (360 web pages or 3400 e-mails) plus 300 Ping Pong™ text messages. \$4.00 per additional MB

It is our general policy to review mature products, rather than products on the cutting edge of technology. We are making an exception in the case of the *Voicestream G100 iStream PC Card*, because it appears that GPRS will increasingly become an option for the mobile transmission of data.

VoiceStream, owned by Deutsche Telecom, is a leading provider of GSM service in the US. ATT and Cingular are converting to GSM, and we hope to review their products when available. But at the moment, VoiceStream has the only GSM PCMCIA GPRS card we have encountered in our geographical location, supported by a national GSM network. Installation is easy if you are running Windows 98. You put in the CD and follow the directions. If you are running Windows NT, 2000, or XP, you will eventually call Customer Support and be told to download different software from the Internet. The card uses its own SIM.

The card worked rather well, connecting at what appeared to be roughly in the 20 to 28kbps range. There are five issues (actually three known issues, one experienced issue, and one technical unknown), which we assume will be dealt with over time. (We say assume because we sent several e-mails to Kim Thompson, VoiceStream's head of Corporate Communications, but never got a response, and assume they have no timeframe to report). These five issues are:

- The line drops roughly every 6 minutes. This is, according to technical support, a known issue.
- The software sets the DNS incorrectly, so you have to manually re-set the DNS in your browser. This is an ongoing process, as the software keeps resetting it every time you log onto the Internet. This is, according to technical support, a known issue.
- The GPRS implementation doesn't work with SMTP servers, so that you can use your regular email program to receive email from your POP server, but cannot send mail. In theory you can use your ISP's ASMTTP server with authentication, but in practice this cannot be done. This is, according to technical support, a known issue.
- We also had a problem with large downloads, which tended in our tests to arrive corrupted.
- GPRS packets *should* be encrypted between the modem and the GPRS gateway at the operator's domain. The algorithm is GEA2, a 56 bit stream cipher. The GPRS specification calls for GEA2 to be used on all "bi-directional" data communications between the GPRS Gateway

and the handset/modem. Because GEA2 can wreak havoc on corporate VPNs which use IPsec, some operators *say* they support GPRS security but in practice don't actually turn it on. We have no idea if this is an issue with VoiceStream.

Assuming that these problems are dealt with and that the connection speed goes up a bit, this technology will give mobile users a lot of freedom.

In terms of the pricing, experience will lead us to discover if the pricing is appropriate for the amount of data normally dealt with. At this point in time, the technology is too new for anyone to have enough experience with it to price it other than by a seat-of-the-pants guess. We note, however, that downloading the daily Norton AntiVirus update would consume over three megabytes each day there was an update. If you did nothing else with the service, this would cost you \$184 a month over the base of \$59.99. This means that the service is appropriate for reading e-mails, but not really priced for actual work. This pricing may be a deliberate choice, indicating that there is, from a technological point of view, insufficient bandwidth to allow a significant number of simultaneous multiple serious users. Since we were not able to speak with anyone from VoiceStream, we cannot know what their thoughts are on this matter.

Science and Litigation: Products Liability in Theory and Practice

Terrence F. Kiely

ISBN: 0849300258 480 pages \$69.95

CRC Press <http://www.crcpress.com/>

As a science buffs and litigation support experts, we have yet to see anything like this book. It is the most comprehensive treatment of the use of science in the courtroom we have seen.

While the focus of the book is on product liability, this does not detract from its usefulness in other fields in the courtroom. It gives a refreshing view on the acceptability of science and experts for courtroom use.

The primary audience for this book is those involved in insurance defense and product liability. But it is also one heck of a read for anyone who deals with science in the courtroom (such as police officials, prosecution and defense attorneys who encounter scientific evidence, and expert witnesses of any type.)

7. Free-Subscription/Unsubscription/Copyright Information

•• AEGIS e-journal 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) 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 2002* and the *EU Revised Money Laundering Directive of 2002*.
- **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 July 2002 ÆGIS e-journal (© 2002 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.