



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 5 Number 1, January 2002

From the case files of

The LUBRINCO Group

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

and

Financial Examinations and Evaluations, Inc.

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

Business in Bogotá or other high-threat areas? Call us!

This month's features:

- 1. Due Diligence — The press and the police**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — The prospective-employee lie**
- 3. Executive Protection — Protecting the fast-living**
- 4. Technical Issues — The 13th annual survey of salaries and bonuses in the security/loss prevention field**
- 5. Real Stories from the Field — National ID cards**
- 6. Book and Product Reviews — Marquis Private Jet Card**
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — The press and the police

Contributed by journalist Terry Phillips (newsman@ix.netcom.com). Contributed articles do not necessarily reflect the viewpoint of the ÆGIS e-journal. While this was written with law enforcement in mind, the advice given is appropriate for everyone who deals with reporters, and, thus, we felt its inclusion was warranted here.

Ever since the first scribe applied a chisel to a stone tablet, there has been a natural tension between journalists and law enforcement agents. Reporters want to reveal as much information as they can, while those responsible for security prefer to limit the leaking of what they know particularly if such facts are confidential or sensitive.

But as most professionals on both sides know, the news media can (and often do) serve the interests of law enforcement and vice versa. Whether it's a beat cop, a homicide detective, or a private security agent, a smart officer will want to develop and maintain good working relationships with responsible journalists. (Yes, there really are some out there!)

Here are a few basic ground rules to keep in mind when dealing with the ladies and gentlemen of the press.

1. Be honest. Never, never, never, NEVER lie. If you don't want to tell a reporter something, say so. But do NOT tell him or her something that is untrue. It will destroy your credibility. You can say "no comment" or "I don't know" or "I'd rather not say right now." Say anything you want as long as it's not false.
2. Be careful. Always, always, always, ALWAYS assume that you are speaking "on the record" when you speak with a journalist. You might be able to get reporters to respect confidential information. (Most good ones do.) But there's no guarantee. And if someone reports something that you said "off the record," it's still your responsibility.
3. Be smart. The media can be helpful in getting important information to the general public. So, when you have something important to say, don't be afraid to ask the press for help. But avoid the temptation to make every case sound like the crime of the century. If you exaggerate often enough, you'll be dismissed like the boy who cried wolf. Remember to protect your credibility.
4. Be open. Make yourself as available as you reasonably can to answer questions. Even when you think that you have nothing newsworthy to say, some reporters might want to clarify what they already know. If

you shut out the media, they might report something inaccurately. And bad public information can make your job harder.

5. Finally, be a human being. Whether it's a sound bite for a national network or a quote for a small town newspaper, you'll communicate more effectively if you speak like a regular person. Avoid the clichés of police jargon. When you talk with journalists, keep in mind that you are not filing an official report. You're talking to your neighbors.

2. OPSEC, Economic Espionage, and Competitive Intelligence — The prospective-employee lie

A pharmacy conglomerate had plans to expand. They specialized in *compounding*, the age-old process of assembling different active ingredients with flavorants and a delivery vehicle, such as salve, capsules, or liquid medicine (for chemotherapy, hormone replacement therapy, nutritional supplements, and veterinary prescription). Most pharmacies now do little or no compounding, instead dispensing already-formulated medicines into little jars with labels.

The acquiring pharmacy hired a CI specialist to find some basic information about each of the pharmacies they were considering acquiring, seeking to learn their gross sales, number of pharmacists, number of pharmacist assistants, specialty in compounding, ownership of the business, and if they owned the buildings they occupied. The CI specialist studies this problem and came upon an idea.

The CI specialists decided to lie to the people from whom they wanted the information, and gathered the names addresses and phone numbers from an association directory. He then called each of the people on the list. Using the pretext that his new wife had been offered a job in the area and that he was a former EMT, had just obtained a Pharmacy Assistant degree, and was wondering if he could fax his resume for possible consideration.

As he and the person at the pharmacy spoke, he than began to mine the person on the phone for information, asking questions that should not have been answered. "How big is the pharmacy?" (Answer) "Wow, I will bet you have 5 pharmacists and 10 pharmacy assistants" (answer with a correction of the number of pharmacists and assistants). "That is just the size of place I was looking to get some work. I guess with that size the owner owns the building too - huh?" (Answer on who owns the building). "What is the specialty of the pharmacists?" (Answer). "That good: That's a good field to be in these days. Listen - I hope I am not too nosy but is the owner going to

stay in business for a while. It sounds like with the business being around so long they may retire soon.” (Answer). “Gee you’ve been a great help now what’s the fax number to respond to?”

Not all of the questions were answered and not all of the information was garnered in this simple way, but it was over 85% successful. Most of the rest of the information was obtained through professional licensing information, public records, and assumptions that could be made with some certainty from industry norms.

What was the cost? It came to under \$141.00 per pharmacy. Imagine the value of the information for decision making on what areas you will expand into. You will know who will be more sensitive to competition and who might be a good target for a buyout.

Note that the information came flooding out of the targets. The people answering the phones were not trained on what they should and should not say. There was no protocol on how to treat different types of calls or how to route calls. Those who answered the phones did what came naturally to them: They were helpful.

Preventing this kind of information loss is done with a simple protocol sheet that you can discuss with employees, and keep on a sheet near the phone. The sheet should cover how they should answer the phone, route calls, and deal with people who ask lots of questions. One of the best answers for a caller with a lot of questions I have heard is “Sir, I wish I could answer your questions, but this is a dynamic organization and I want to route you to the person who will have the most up to date information.” It not offensive, it is helpful, and gets the person answering the phone off the line and out of the position of answering a stream of questions or sounding rude.

A phone answering protocol might take as little as 20 minutes to write and type in a small business. It is a worthwhile 20 minutes.

3. Executive Protection — Protecting the fast-living

Some subjects being protected can be a bit more difficult to protect than others. A long-time client of one firm has a well-earned reputation of behaving like a nut, driving at high rates of speed (no he won’t let someone drive him), and having sex with lots of women, on the spur of the moment. The protection is mandated both by the requirements of his insurance carriers and by his own sporadic common sense. He deals in high-price jewelry for high-profile clients, so the insurance company does not want him to be ripped off, and the he does not want to be kidnapped.

The personality of a person that has made it this far in life is not a kind mild mannered person. They are not a sheep but rather a bull, a bull that is built to take chances and risks and to profit by them. Actually - many of them take risks because they like taking risks - it part of the nature of the beast. So how to protect a Randy beast? Well - it isn't easy.

An example of a not-atypical day with Mr. X.

Up at 5:30 to get to the store by 6:30. The store opens at 10:00, and during the pre opening hours all of the business in Europe is attended to, along with several meetings with advertisers vying for the advertising dollar. This is approximately 20 phone calls and 6 appointments. The matters discussed on the phone are usually about items of great value and how they are to be shipped. The phones are regularly swept, along with the whole store for bugs and listening devices. Phone numbers are cross-referenced in advance to the persons and/or business they repute to be (or are known sources or clients). All appointments are made at least three days in advance and the people are checked to see if they are with the company they claim to represent or they are known vendors for advertising.

10:00 to 2:00 is spent on the floor and greeting customers. Some customers have made appointments in advance and have been cross checked and verified that it is likely they have the funds to purchase those items contained in the private room (or they are known customers). All customers come through the front door. The front door leads into a dead zone, fondly called a mantrap, and the front door must close before the inside door can be opened. This feature cannot be overridden. All persons coming in to the store have their faces video-photographed and these are kept on file.

2:00 to 3:00 is set aside lunch with a client, friend, supplier, or vendor. Lunch is taken at random from a list of 12 restaurants in the area. Appointments are set in advance for the person to Meet Mr. X at the store and they go from the store to dine at one of the pre-selected restaurants. These 12 were chosen from a larger group for their food, style, and security layout. Other fine restaurants were excluded because of design and access. The restaurants are chosen at random with a 20-sided dice. 1-12: a restaurant is selected. 13-20: roll again.

3:00 to 4:00 is devoted to work on magazine shoot with models. Three armed protective specialists (two visible, one undercover) work with models and displaying the jewels for the magazine layout. All participants are

forbidden to take any containers (pocket, a purse, a soda can) into a zone established around the jewels, which includes the zone being photographed.

The model is to change and get ready elsewhere, and when the model is set at the location for the photograph, then and only then are the jewels placed on her. When the photograph is concluded the jewels are removed before the model leaves the zone.

4:00 to 8:00 pm is spent on the floor greeting guests. The client has allowed the model to stay and wear some other jewelry and has invited her out to dinner. Can't peel model off client.

The store has five security / executive protection people on duty, four visible at all times and one working the video equipment. Stations are rotated every so often, so there is no set schedule.

This is a time of high sales (especially from November 15 until Christmas Eve). Client is meeting and greeting customers. Client is wearing at any give time \$500,000 to 1.5 million in jewelry for display, and showing customers how nice it can look. It is an effective display and has sold several pair of \$15,000.00 cuff links in the last week.

Store begins tallying daily receipts. Most sales are checks or credit cards, not too much cash. It is all bagged and headed for the night deposit box across the parking lot. All non-cash deposits are made at night at the night drop box. All cash deposits are set in during the day at staggered intervals so as not to have more than \$15,000 in cash on site at anyone time. There is no set schedule.

7:30 model gets hungry and rubs against client for food (our cat does that!). It works on him as well as it works on us with our cat. Client decides to leave early with model and go to dinner. Client picks a new restaurant where it is impossible to get a table at the last minute. Staff calls, uses his name, and gets two tables. One-person advance to survey restaurant. One agent to ride with client and guest, and one to follow. Two remain at store and close up. Client throws out new agent from his car so he and the model are alone. New agent has to ride with the chase car. Client has fast European sports car and shows the model how fast he can go. Chase car keeps up, both violate most of the traffic code of the state, and a few things the state has not yet made illegal. Client, model, and two agents in chase car arrive at restaurant. Advance escorts client and model to table. Man ridding shotgun in chase car not breathing at all well - only second night on the job - he'll get better. Second table occupied by two-person EP persons. EP persons have apple juice in wine glass so as to fit in a little better.

Dinner drags on with model pawing client and client pawing model. Exterior EP man alerts detail that a city bus blocks one of the front exits of the parking lot. One interior man moves from the table to the front door while exterior man goes to see what is wrong with the bus. Bus is ahead of schedule and it waiting for the time to catch up to where he is now on the route. Exterior man leans forward (so all of the wire and shinny metal things can be seen) to say, very firmly, move so you don't block any entrance here or anywhere else. Bus driver moves 100 feet further down the street, with a smile. EP detail returns to normal stations.

Client and model finish dinner. He suggests a piano bar at a hotel nearby. EP team, as client gets ready to leave, again splits the team into the advance and the chase car. New guy just gets in chase car. The EP team is aware of this location and has scouted it before.

Advance arrives and gets two tables and two adjoining rooms. Client and model arrive, have a few drinks, and they go to one of the adjoining rooms. On the way to the rooms all jewelry is removed from model and Client. Client is not happy but knows the routine, pretends to make a fuss, but also gives EP detail his wallet. EP team is on station in hallway, in adjoining room and out side rooms. Adjoining doors are both unlocked but not opened.

12:00 midnight - two fresh members join Team, and two of the fellows on duty go home.

5:00 am some noise is heard and shortly thereafter the woman leaves the room, smiles at one of the EP men and asks "Is he always so much fun?" EP man answers "I don't know: He never taken me out to dinner." They both laugh and he orders a car to take her wherever she would like to go.

5:30 Client is awake and orders room serve for himself and the team.

6:15 Client is showered and dressed from a number of spare sets of clothes that he has in his car, office, home, and other dwellings. Client goes to office and arrives with new EP team for the day.

The client in the above day-in-the-life-of scenario is an amalgam of a few real clients. It is tough work, long hours and you are protecting someone who, while he knows he needs and wants the protection, lives a life style that is larger than life and will not give into curbing his life style. He has bought completely into security for his assets, and somewhat for his person. The protective specialist has to realize that this guy is a force of nature and must alter his methods to suit the client's behavior as best they can. It doesn't matter whether you like his life style or his morals (though nobody forces

you to work with clients you of whom you don't approve): The job is to keep him and the jewels secure.

4. Technical Issues — The 13th annual survey of salaries and bonuses in the security/loss prevention field

Contributed by Dr. Steven Langer, President, Abbott, Langer & Associates. (*slanger@abbott-langer.com* <http://www.abbott-langer.com/>). Contributed articles do not necessarily reflect the viewpoint of the *ÆGIS* e-journal.

The composite security/loss prevention practitioner with the highest annual income (salary plus cash bonuses and/or profit sharing) is a Security/Loss Prevention Director or Vice President located in Ft. Lauderdale, Newark/Jersey City, Philadelphia, Boston, St. Louis, Los Angeles/Long Beach, or Chicago, or outside the metropolitan areas studied in South Carolina or Pennsylvania.

This composite “individual” is employed by a merchandising firm, a manufacturer of pharmaceuticals & related products, a security service, a manufacturer of chemical & allied products, a property/real estate management firm, or a financial institution with 2,500 employees or more and an annual security budget of \$2.5 million or more. He or she has responsibility for security/loss prevention for either the entire organization or a major division of the organization, has 10 or more years of experience and at least a Bachelor's degree, and reports to the Chief Human Resources Executive, the Chief Legal Executive, or the Chief Operating Officer/Vice President-Director of Operations.

A fair number of individuals in this group make well in excess of \$250,000 per year, although Security/Loss Prevention Directors and/or Vice Presidents as a group have a median income of \$71,848.

Far toward the other end of the income spectrum, Unarmed Security Officers/Guards have a median income of \$22,245 per year. The lowest-paid employees in this group are located in Los Angeles/Long Beach, Columbus (OH), Oklahoma City, Raleigh/Durham/Chapel Hill, or Norfolk/Virginia Beach, or outside the metropolitan areas studied in Pennsylvania, Mississippi, Kentucky, Louisiana, Arkansas, or Massachusetts.

This composite “individual” works for a security service, an educational institution, a hospitality organization, or a food/beverage/tobacco products manufacturer, in a position that requires little or no prior experience but does require a high school diploma. Such an individual may earn as little as \$12,000 per year.

These composites represent the briefest possible “boil-down” of the voluminous data provided by 197 organizations regarding the current salary, salary ranges, and cash bonuses and profit-sharing, and numerous demographic variables for individuals in 26 benchmark jobs in the security/loss prevention field. The end results of the survey, the most intensive and extensive ever attempted in this field, appear in Compensation in the Security/Loss Prevention Field, 13th Edition, a tightly-packed, 276-page, two-volume statistical analysis of compensation in this field. Copies are available for \$75.00 (for Part I - Security/Loss Prevention Directors/Vice Presidents) and for \$550.00 (for Part II - Other Security/Loss Prevention Jobs) from Abbott, Langer & Associates, Inc., Dept. ART, 548 First St., Crete, IL 60417; telephone 708/672-4200; fax 708/672-4674; <http://abbott-langer.com>.

It would be an exercise in futility to attempt more than a superficial overview of the survey results in this summary. However, some overall data can be presented herein and some comments on the relationship of the various demographic variables to income in the security/loss prevention field can be made.

Overall Compensation

In addition to the income of the two jobs already discussed, the median total cash compensation of some of the other 24 jobs included in the survey report is:

Physical Security Specialists - \$71,000

Security/Loss Prevention Managers - \$53,000

Computer Security Specialists - \$52,491

Classified Security Specialists “A” - \$45,845

Investigators - \$43,772

Console Operators “A” - \$31,899

Security Officers/Guards (Armed) - \$27,000

Supervisors of Security Officer/Guard Operations “D” - \$24,451

Vehicle Gate Control Supervisors - \$23,500

Store Detectives/Loss Prevention Agents - \$23,000

Naturally, these overall figures vary when geographic location, type of employer, size of organization and security/loss prevention budget, level of

education, length of experience, etc. are considered. Analyses by each of these variables appear in the complete report.

Certification Status

The CPP and CFE certificates lead to increased income for executives in the security/loss prevention field, although other factors may account for a portion of the additional income of holders of these certificates. For example, the median Security/Loss Prevention Director or Vice President who holds both the CPP and the CFE has a 37% higher income than those without either certificate.

Geographic Area

Most security/loss prevention jobs are compensated best in the largest cities and least well in the smaller cities and rural areas. For example, Security/Loss Prevention Directors and Vice Presidents are paid best in such locations as San Jose (with a median income of \$112,000), Los Angeles/Long Beach/San Diego (\$90,650), Chicago (\$77,000), Cleveland (\$76,295), Columbus (\$75,000), and Philadelphia (\$74,000); and least well in Oklahoma (\$30,000), Texas (\$36,250), and Georgia (\$42,000). However, this does not hold true for the entire range of jobs, with the “ranking” of cities/states varying by job.

Type of Employer

Security/Loss Prevention Directors and Vice Presidents fare better, on average, in manufacturing firms than in non-manufacturing organizations - 18% better. The median income of members of this group is highest in firms that manufacture chemical, pharmaceutical, & allied products (\$170,000) and electrical & electronics products (\$93,500); merchandising firms (\$91,600); banks and other financial institutions (\$85,000); and insurance companies (\$83,630).

The lowest median incomes for this group are found among those employed by museums and art institutes (\$30,000); security services (\$39,000); hospitality organizations (\$40,000); and state & local governments.

In comparison, Unarmed Security Officers/Guards fared best when employed by utility companies (\$36,044), manufacturers of paper products/printing & publishing firms (\$29,000); and state & local governments (\$27,496).

They did least well when employed by such employers as manufacturers of chemical, pharmaceutical & related products (\$16,600) and food / beverage / tobacco products (\$19,100); and educational institutions (\$19,800).

Size of Organization and Security Budget

Two of the most consistent determinants of income for Security/Loss Prevention Directors and Vice Presidents are the size of the employing organization and the total annual security/loss prevention budget. The median income of Security/Loss Prevention Directors and Vice Presidents rises dramatically from \$30,000 for those employed in organizations of fewer than 100 employees to \$110,500 of those in organizations with 25,000 employees or more. The median income of these individuals also rises dramatically from \$30,000 for those with annual security budgets of under \$100,000 to \$102,500 with budgets of \$2.5 million to \$4.9 million. The complete report also provides income data vs. external security services budget, proprietary guard services, and all other security functions budget.

Level of Education

The level of education attained is another important determinant of salary in the higher-level jobs. For example, Security/Loss Prevention Directors and Vice Presidents make 173% more with a master's degree (\$81,900) than with just a high school education (\$30,000).

Involvement with DOD/DOE Regulations

Involvement with Department of Defense and/or Department of Energy regulations has a significant effect upon the compensation of specific security/loss prevention jobs. For example, the median income of Security/Loss Prevention Directors and Vice Presidents on the basis of involvement with DOD/DOE regulations is as follows:

Operates under just DOE regulations - \$122,000

Not involved with either DOD or DOE regulations - \$71,022

Line of Reporting

The line of reporting for Security/Loss Prevention Directors and Vice Presidents is reflected in their level of compensation (although this may be a by-product of other demographic variables, such as type and/or size of organization). The median income of Security/Loss Prevention Directors and

Vice Presidents, in descending order by the function of their immediate superiors, is:

Chief Legal Executive - \$110,500

Chief Administrative/Corporate/General/Support Services Executive - \$91,000

Chief Human Resources Executive - \$87,114

Chief Audit Executive - \$85,000

Chief Financial Executive - \$82,006

Chief Executive Officer/President/Owner/General Manager - \$70,000

Chief Building/Facilities Executive - \$68,000

Chief Operating Officer/V.P.-Director, Operations - \$66,825

Plant Manager/Superintendent - \$30,000

5. Real Stories from the Field — National ID Cards

Reprinted from the 15 December 2001 CRYPTO-GRAM (<http://www.counterpane.com/cryptogram.html>) with permission of the author, Bruce Schneier (schneier@counterpane.com), CTO, Counterpane Internet Security, Inc. Contributed articles do not necessarily reflect the viewpoint of the *ÆGIS* e-journal.

There's loose talk in Washington about national ID cards. Although the Bush administration has said that it is not going to pursue it, enough vendors are scurrying to persuade Congress to adopt the idea that it is worth examining the security of a mandatory ID system.

A national ID card system would have four components.

1. A physical card that contains information about the person: name, address, photograph, maybe a thumbprint, etc. To be effective as a multi-purpose ID, of course, the card might also include place of employment, birth date, perhaps religion, perhaps names of children and spouse, and health-insurance coverage. The information might be in text on the card and might be contained on a magnetic strip, a bar code, or a chip. The card would also contain some sort of anti-counterfeiting measures: holograms, special chips, etc.
2. A database somewhere of card numbers and identities. This database would be accessible by people needing to verify the card in some circumstances, just as a state's driver-license database is today.
3. A system for checking the card data against the database.

4. Some sort of registration procedure that verifies the identity of the applicant and the personal information, puts it into the database, and issues the card.

The way to think about the security of this system is no different from any other security countermeasure. One, what problem are IDs trying to solve? Two, how can IDs fail in practice? Three, given the failure modes, how well do IDs solve the problem? Four, what are the costs associated with IDs? And five, given the effectiveness and costs, are IDs worth it?

What problem are IDs trying to solve? Honestly, I'm not too sure. Clearly, the idea is to allow any authorized person to verify the identity of a person. This would help in certain isolated situations, but would only have a limited affect on crime. It certainly wouldn't have stopped the 9/11 terrorist attacks - - all of the terrorists showed IDs to board their planes, some real and some forged -- nor would it stop the current anthrax attacks. Perhaps an ID card would make it easy to track illicit cash transactions, to discover after the fact all persons at the scene of a crime, to verify immediately whether an adult accompanying a child is a parent or legal guardian, to keep a list of suspicious persons in a neighborhood each night, to record who purchased a gun or knife or fertilizer or Satanic books, to determine who is entitled to enter a building, or to know who carries the HIV virus. In any case, let's assume that the problem is verifying identity.

We don't know for sure whether a national ID card would allow us to do all these things. We haven't had a full airing of the issue, ever. We do know that a national ID document wouldn't determine for sure whether it is safe to permit a known individual to board an airplane, attend a sports event, or visit a shopping mall.

How can IDs fail in practice? All sorts of ways. All four components can fail, individually and together. The cards themselves can be counterfeited. Yes, I know that the manufacturers of these cards claim that their anti-counterfeiting methods are perfect, but there hasn't been a card created yet that can't be forged. Passports, drivers' licenses, and foreign national ID cards are routinely forged. I've seen estimates that 10% of all IDs in the US are phony. At least one-fourth of the president's own family has been known to use phony IDs. And not everyone will have a card. Foreign visitors won't have one, for example. (Some of the 9/11 terrorists who had stolen identities stole those identities overseas.) About 5% of all ID cards are lost each year; the system has to deal with the problems that causes.

Identity theft is already a problem; if there is a single ID card that signifies identity, forging that will be all the more damaging. And there will be a great premium for stolen IDs (stolen U.S. passports are worth thousands of dollars in some Third World countries). Biometric information, whether it be pictures, fingerprints, retinal scans, or something else, does not prevent counterfeiting; it only prevents one person from using another's card. And this assumes that whoever is looking at the card is able to verify the biometric. How often does a bartender fail to look at the picture on an ID, or a shopkeeper not bother checking the signature on a credit card? How often does anybody verify a telephone number presented for a transaction?

The database can fail. Large databases of information always have errors and outdated information. If ID cards become ubiquitous and trusted, it will be harder than ever to rectify problems resulting from erroneous information. And there is the very real risk that the information in the database will be used for unanticipated, and possibly illegal, purposes. There have been several murders in the U.S. that have been aided by information in motor vehicle databases. And much of the utility of the national ID card assumes a pre-existing database of bad guys. We have no such database. The U.S. criminal database is 33% inaccurate and out of date. "Watch Lists" of suspects from abroad have surprisingly few people on them, certainly not enough to make a real-time match of these lists worthwhile. They have no identifiers, except name and country of origin, and many of the names are approximated versions or phonetic spellings. Many have only approximated names and no other identifiers.

Even riskier is the mechanism for querying the database. In this country, there isn't a government database that hasn't been misused by the very people entrusted with keeping that information safe. IRS employees have perused the tax records of celebrities and their friends. State employees have sold driving records to private investigators. Bank credit card databases have been stolen. Sometimes the communications mechanism between the user terminal -- maybe a radio in a police car, or a card reader in a shop -- has been targeted, and personal information stolen that way.

Finally, there are insecurities in the registration mechanism. It is certainly possible to get an ID in a fake name, sometimes with insider help. Recently in Virginia, several motor vehicle employees were issuing legitimate drivers licenses in fake names for money. (Two suspected terrorists were able to get Virginia drivers' licenses even though they did not qualify for them.) Similar abuses have occurred in other states, and with other ID cards. A lot of thinking needs to go into the system that verifies someone's identity before a

card is issued; any system I can think of will be fraught with these sorts of problems and abuses. Most important, the database has to be interactive so that, in real time, authorized persons may alter entries to indicate that an ID holder is no longer qualified for access -- because of death or criminal activity, or even a change of residence. Because an estimated five percent of identity documents are reported lost or stolen, the database must be designed to re-issue cards promptly and reconfirm the person's identity and continued qualification for the card.

Given the failure modes, how well do IDs solve the problem? Not very well. They're prone to errors and misuse, and are likely to be blindly trusted even when wrong.

What are the costs associated with IDs? Cards with a chip and some anti-counterfeiting features are likely to cost at least a dollar each, creating and maintaining the database will cost a few times that, and registration will cost many times that -- multiplied by 286 million Americans. Add database terminals at every police station -- presumably we're going to want them in police cars, too -- and the financial costs easily balloon to many billions. As expensive as the financial costs are, the social costs are worse. Forcing Americans to carry something that could be used as an "internal passport" is an enormous blow to our rights of freedom and privacy, and something that I am very leery of but not really qualified to comment on. Great Britain discontinued its wartime ID cards -- eight years after World War II ended -- precisely because they gave unfettered opportunities for police "to stop or interrogate for any cause."

I am not saying that national IDs are completely ineffective, or that they are useless. That's not the question. But given the effectiveness and the costs, are IDs worth it? Hell, no.

Privacy International's fine resource on the topic. Their FAQ is excellent:
<http://www.privacyinternational.org/issues/idcard/>

EPIC's national ID card site:

http://www.epic.org/privacy/id_cards/

Other essays:

<http://www.csl.sri.com/users/neumann/insiderisks.html#138>

<http://www.cato.org/tech/tk/010928-tk.html>

<http://www.aclu.org/library/aaidcard.html>

<http://slate.msn.com/?id=2058321>

<http://www.cato.org/pubs/pas/pa237.html>

http://members.aol.com/_ht_a/xowie/idcard.htm

<http://www.free-market.net/spotlight/idcards/>

<http://www.securityfocus.com/news/286>

<http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2830138,00.html>

6. Book and Product Reviews

Marquis Private Jet Card

Marquis Jet Partners, Inc.

<http://www.marquisjet.com/> 1-866-538-1400

There are a number of reasons why an organization or an individual might want a plane at their disposal. Unfortunately, planes don't come in Cracker Jacks boxes. Traditionally, one could buy or lease a plane, or share ownership with a fractional ownership plan.

The problem is that buying, leasing, or fractional ownership which begin at a minimum of five-year commitment and ranges anywhere from between \$500,000 and \$750,000 and up. This is a one-time cost to buy into a five-year contract. Once that money is spent, the client is given access to the plane, and is still charged an hourly rate for flying, monthly maintenance fees and other costs (fuel, plane transfers, etc.). When the contract is expired, the client also is charged a resale fee. For many, particularly when first putting their toe into the general aviation pool, this is a very difficult decision indeed, and one potentially fraught with long-term financial peril.

An appealing alternative is the *Marquis Private Jet Card*.

You start by looking over the Marquis fleet (which is actually the NetJets fleet) and decide what kind of plane you are likely to use. Planes include the Falcon 2000, Hawker 800XP, Cessna Citation V Ultra, and Cessna Citation X, so you can carry between 7 and 10 people on a flight. That done, you buy a Private Jet card for somewhere between \$109,000 on the smaller jets and \$225,000 on the bigger jets. This gives you 25 hours of time on that class of plane. Scheduling is on demand, but you need to give ten hours notice. As you would expect, Marquis is also equipped to handle related travel needs, such as hotels, dinner reservation, and almost anything else you would expect in this circumstance.

The benefit of this service is that you have a fixed commitment with full FAR 135 service. Thus, if you were a professional athlete or rock band, and weren't sure you wanted to make a financial commitment of half a million dollars for a five year period that might extend beyond your career, this would be an excellent option. By the same token, if your company wasn't sure it wanted to take on the responsibility and cost of running an aviation department, this

would be a good, limited liability, way to discover if having a jet at your disposal was, in fact, cost effective for the organization.

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 January 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.