



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 6 Number 7, July 2003

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 — The implications of hiring and firing**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Identifying the problem before you make drastic social changes to solve it**
- 3. Executive Protection — Tips for U.S. owner-drivers on being stopped by the police**
- 4. Technical Issues — Protecting home broadband connections**
- 5. Real Stories from the Field — Deciding whom to stiff**
- 6. Book and Product Reviews — *The Crooked Ladder: Gangsters, Ethnicity, and the American Dream*
*Menace to Society: Political-Criminal Collaboration Around the World***
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — The implications of hiring and firing

In the last few weeks we have come across several people who were let go for what appeared to be no particular reason. Of course there is *always* a reason, but it is not always obvious to the person being sacked. And without knowing the reason, one is forced to do a lot of soul-searching that may turn out to be fruitless, and might hinder the making of appropriate decisions.

In one of the cases it was known well in advance that the layoff was to take place. In desperation the man tried to avoid being let go: He came to work earlier, left later, took shorter lunches, and tried to maximize his productivity. As it turned out, there was absolutely nothing wrong with the work he was doing. It simply happened that the company wanted to hire someone else in an entirely different area, albeit within the same group, but there was a freeze on headcount. A relatively arbitrary decision was made as to whom to let go, and he was it. Would knowing this have helped him in any way? Not in terms of keeping his job, but it would likely have helped in negotiating his separation package. There is also the question as to whether the gains in the area where the new man worked would, long term, compensate for the losses caused by our person leaving.

In a more interesting case, a woman was let go when her boss was replaced. Again the reason was unclear until long after the event. In this case the new boss merely wanted a clean sweep of personnel, and to bring in her own people. Unfortunately, the job was a high-level technical job at which the woman was extremely skilled, and the company was forced to hire three new people to do the same work. The boss, who had little to no understanding of what was being done, was herself let go within a short period of time, and the company has suffered greatly because of the lack of productivity in this area, ending up folding a division.

More interesting still, largely because the story is practically archetypal, was a company that had a salesman who was wildly successful. The owner realized one day that the salesman was making substantially more than was he. Following an all too common path, he started restricting territory, cutting commissions, and taking all the usual steps to drive his best salesman away. He finally succeeded, and the company ultimately folded for lack of revenue.

In another case, a major American film maker decided that as a cost-cutting method it would offer people early retirement, and a lot of people took advantage of this. Rumor has it that among those retiring were many of the people who knew how to cook up one of their trademark film emulsions

Apparently, making film emulsions, like cooking, is as much art as science. While a claim can be made that this merely helped propel them into the world of digital photography, it should have been done by choice, not by chance.

The bottom line is that people are the most important resource of a company, and it is important to look carefully at what is being lost in a layoff, as well as what is being gained.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Identifying the problem before you make drastic social changes to solve it

Back in the late 1950s, two high school boys in Westchester County, NY, got into the habit, for reasons obscured by the passage of time (and the untimely death of one of the miscreants), of picking up empty beer cans on their way to school, and then tossing them into an abandoned room they had discovered above the auditorium stage, at the top of a ladder. Some years after they graduated, the room was discovered, and draconian steps were taken to assure that the drunken orgies which were obviously taking place would be stopped. For all we know, some of the rules put into place then are still in existence.

In a later instance, a wide-ranging (robbery, burglary, sexual assault, homicide) crime wave in a Westchester town on the other side of the Hudson, caused a revamping of local ordinances. It turned out that the gang responsible was one demented person, but the laws still stay on the books.

More recently, after the terrible shooting of 16 school children and a teacher in Dunblane, Scotland, a Home Office report said this was the isolated work of a lunatic, and that no action should be taken. Instead, essentially all guns (and pretty much all pocket knives, and all right to fight back) were taken away, which many feel was *part* (in Western nations, restriction of gun ownership is ALWAYS followed by an increase in violence) of turning the UK from having one of the lowest assault rates in Western Europe to one of the highest.

The moral here is that attempting to solve problems is a good idea, but only if the problems are real. As a rule of thumb, a single aberrant incident, no matter how horrifying, may not require any additional changes, and certainly may not require sweeping changes.

As it turns out, most problems faced by business can be dealt with through fairly basic methods. As an example, if you are prepared for fire and natural disaster, you have probably done everything you need to do to be prepared

for terrorism. If you have reasonable access control and separate shipping from receiving you probably don't have much of a theft problem. If you identify abused partners and have a plan and a hidden place off to which you spirit them if their insignificant-other shows up, you probably (assuming you are not in the retail business, or out on the street as a cop or some such) don't have much of a problem with workplace violence. If you do pre-hire screening of employees, from the CEO through to the janitor, and have identified critical information and have taken even minimal efforts to protect it, you probably don't have much of a problem with information theft.

If, however, you decide you have some specific problem, based on a single incident, or an incident that happens so infrequently as to qualify, each time, as a single incident, and make sweeping changes to deal with that, you can frequently cause more harm than good. As an example, forcing employees to change each of their many computer passwords every thirty days seems like a good idea, but, in fact, is counterproductive, since most employees will simply write the new passwords on a Post-It note and stick it on their terminal, in their pencil cup, under their desk-pad, or in their top drawer. There are, in fact, ways to deal with this issue, but choices that lower security are not always a productive idea.

In some cases, taking unnecessary actions can go from being counter-productive to being destructive. We have in the past mentioned a company of which we heard that spent a huge amount of money revamping their mail room and mail procedures to deal with a possible anthrax attack, while simultaneously cutting out their free employee flu shots (nobody has resources to do everything). Since something on the order of 20,000 Americans will die of the flu this year, the logic escapes us. And of course, the most discussed example is the TSA, formed to combat a once-every-thirty-years event, whose main results have been the draining of manpower from less well-funded agencies, an increase in travel deaths from folks who have decided to drive rather than fly, and, if one is to believe the whispers, to induce potential terrorists to think about acquiring some of our misplaced Stinger missiles from Afghanistan (we are given to understand they only cost \$250,000), in order to bypass that pesky airport security and simply knock planes out of the sky.

Bottom line: Before leaping to drastic solutions to your problems, make sure they really are problems, not one-time events that need to be handled before you go back to business as usual. And remember that if you smoke, drive without a seatbelt, live in Hurricane Alley, drink to excess, or don't practice

safe sex, you might want to re-think your concerns about criminals, socially disadvantaged criminal religious fundamentalists, and spies.

3. Executive Protection — Tips for U.S. owner-drivers on being stopped by the police

If you are stopped by the police while driving you should, in general, pull over, turn on the inside light if it is at night, take out your license and registration, roll down your window, and put both of your hands on the top of the steering wheel where they can be plainly seen.

While this is a good general rule, in certain cases it needs to be modified because of the number of robberies and assaults that take place each year by people pretending to be police officers. As an example of how serious this predicament can be, some time ago we attended a law enforcement seminar in which a case was discussed of a man who had killed an officer, put on his uniform, and driven out to find and kill other officers. Fortunately, the first officer who came along felt that something was amiss, and did not pull his car up next to what would have become a death trap.

The bottom line is that even though a person has a uniform, a badge, a gun, and a police car, they may not be cops. So what do we do?

This depends on where you are. If you are stopped by a police officer in Manhattan in the middle of the day, you will likely have a number of onlookers the entire time, providing you with some degree of protection. But what if you are in an area with nobody else around? In this case your level of risk is higher, and it may be a good idea to put on your flashers and drive, at a reasonable pace, toward a place where there are people. At the same time you can call 911 on your cell phone and tell the dispatcher where you are, what is happening, and ask if there is a legitimate police vehicle trying to stop you. If the answer, once they check, is yes, it is probably safe to stop, or to have the dispatcher tell the following car where you are planning to stop. If the answer is no, then it is probably prudent to ask to have an RMP dispatched to intercept you and the fake police car.

What do you do when you get to a place with people around you? You pull over, turn on the inside light if it is at night, take out your license and registration, roll down your window, and put both of your hands on the top of the steering wheel where they can be plainly seen. The officer may well still be angry when you explain why you didn't immediately stop, but you are in a way better position than you were with nobody around.

4. Technical Issues — Protecting home broadband connections

Broadband connections are very good for the user, and a definite improvement from dial-up connections. For those of us who started out with dial-up connections at 300 baud, 56K connections sound like a great improvement, but we so soon become spoiled by cable and DSL connections that we soon forget our dial-up pasts. Additionally, many users love the ability to stay logged on, with e-mail checked every few minutes, without worrying about being charged for connect time.

The down side to all this is that our longer connection times lead to greater exposure to data – or at least data about our Internet habits – being stolen over the same connections that give us such pleasure. You can see how vulnerable your computer is by using the testing programs *Test My Shields!* and *Probe My Ports!* On Steve Gibson's site (<http://www.grc.com/>). These two programs should be run periodically to make sure that newly installed programs have not compromised your security.

The most egregious invasion is someone capturing our IP address and being able to use the technology to directly steal information off our computers. In the days of dial-up, this was not much of an issue because we were never on for very long, and our IP address changed with each logon. How common is this? Well, we haven't done an analysis of the hits on our home machines, but one of our firewalls says that 42,194 intrusions have been detected since the firewall was installed, of which 19,034 have been high-rated.

How do we deal with this? By using a firewall, which is software that allows you to specify what can and cannot access your computer. We use *ZoneAlarm* (available as freeware or in paid versions) from Zonelabs (<http://www.zonelabs.com/>). We specify the kind of access that programs can have, and the kind of access that web sites can have. We can also control cookies, and even mobile code, which is programs that run from within the web page you have loaded. We leave javascript on, and turn off everything else. If we need to change this for some particular page, we have that option.

It also contains a feature that allows us to stop all Internet traffic, in or out, and when we are not actively doing something we enable this lock. And if we forget? Why, we have it set up to lock down Internet access when our screen saver comes on, which means that after a few minutes of inactivity the system will secure itself from the outside world.

How do potential hackers know how to find you? Well, one way is that web sites you visit capture a lot of information on you, and some of these will

display, to anyone that looks, a lot of information about you, including the IP address from which you accessed the site.

How do we deal with this? By using anonymous proxy servers, which are servers to which you send your request to see a site. Thus, when you type <http://www.boyscouts.com/> into your browser and hit return, the browser does not send your request to the Boy Scouts web site. Rather, it sends it to the proxy server, which sends the request, gets the reply, and sends it to you. The IP address tracked will be that of the proxy server, not your IP address. The software that allows you to do this (we use *Anonymity4 Proxy* from <http://www.inetprivacy.com/>) can also do things like block cookies, and give out false information about what kind of browser you use, what language you use, and a host of other factors. It can also cycle through a list of proxy servers so your requests are not coming from one place. Oh, don't forget to turn this off when doing updates: Software like Windows Update looks at the machine whose IP address has queried it, and will send back information on updates needed by the proxy server's machine, not yours.

Using proxy servers can slow down response, which is why they tend to be used with broadband connections. You can test to find which of the many available work fastest with certain sites. Obviously, for some sites you may choose a direct connection.

To make matters worse, many programs you download contain bits of code to send back information on what you do with your computer. In fact, some websites automatically install programs to track what you are doing, and others install cookies that track your web activity. Not only do these share information without your knowledge, all these extra programs can suck up resources. Now, you may think that this doesn't happen with "normal" web sites, but this is not so.

How do we deal with this kind of spyware? There are a number of programs that scan for spyware, prevent its installation, or block its effectiveness. *AdAware* (<http://www.lavasoft.de/>) is one of the old warhorses in detecting datamining, aggressive advertising, and tracking components. We use it, originally starting with the freeware version, finally upgrading to a paid version so we could enable *AdWatch*, a feature that does real-time tracking. We simultaneously use the freeware program *SpyBot* (<http://security.kolla.de/>), which is designed to catch hijackers, spyware, malware, dialers, and usage trackers. *SpyBot* has a very fast scan, and, the first time you run it, you will probably be horrified to discover several dozen spyware programs and data mining cookies on your machine. Finally, we

also use the freeware program *SpywareBlaster* (<http://www.javacoolsoftware.com/spywareblaster.html>), a recommend companion to SpyBot, which is designed to prevent the installation of ActiveX-based spyware from webpages as well as blocking certain cookies. As an example of how widespread this phenomenon is, we note that SpywareBlaster alone has 512 items in its list!

If you install SpyBot (which we recommend you do), you may mysteriously find that you can't changes settings in Internet Explorer. There is a check box on SpyBot's Immunization page that says "Lock IE control panel against opening from within IE (current user). Un-checking this will allow you to make changes. Once you have made whatever changes are needed, you can check it again.

If you are concerned about the privacy of information on your computer, we urge you to be pro-active in defending your computer. While firewalls and anonymous proxy servers require some initial tinkering to meet your needs, we believe the effort is worth it.

Don't forget that, as with anti-virus software, updates need to be checked-for on a regular basis (we do this daily). If you put in the software but do not keep it updated you will have a very false sense of security!

5. Real Stories from the Field — Deciding whom to stiff

Playing hardball can no doubt have a place in business, but it is important to be sure that everyone is playing by the same rules.

In one case, a consultant did work for a company and submitted an invoice. After a suitable period of time he called and asked where his money was. He was told that while, in fact, the work he did was fine, and that while the invoice had been received, the company considered an invoice to be the jumping-off point for negotiation, and that if the individual wanted to get any money, he needed to made another offer.

After a bit of back and forth, the consultant said that if he weren't paid he would sue. This produced some laughter, and the assurance that, if there were a lawsuit, the company attorneys would bury the consultant in paperwork. The consultant assured the man that he didn't care about that: If he weren't paid he would *literally*, not figuratively, bury the other man. And he hung up.

A few minutes later the consultant's phone rang. It was his client, who wanted to know what the consultant meant by what he had said. The

consultant asked what the client was talking about, and the client said he meant what the consultant had said to him a few minutes ago? The consultant replied that he had no idea what the client was talking about, and that they hadn't spoken in a week or so. This didn't clarify things too much for the unseen listener on the client's end.

Our view on this (other than that we simply don't work for this type of client, and certainly not for this particular client) is that the matter comes down to being an issue of principle: Was it more important in principle for the client to screw the consultant or to stay alive? Obviously, the likelihood was that the threat was merely an idle threat in the spirit of the negotiations. While it could be neutralized, idle or not, either through legal action or through the criminal justice system, the monetary cost would be much higher than merely paying the consultant what was owed him.

Plus, if the incident made it to the papers, particularly with the consultant denying he said anything threatening, we are not convinced that the entire world would agree with the theoretically-injured party that sticking it to suppliers was actually taking the high road.

6. Book and Product Reviews

The Crooked Ladder: Gangsters, Ethnicity, and the American Dream

James M. O'Kane

Transaction Publishers ISBN: 0-7658-0994-X 196 pages \$24.99

<http://www.transactionpub.com/1-732-445-1245>

This book is a serious look on how crime in America has been, and continues to be, dominated by newly-arrived and/or excluded ethnic minorities. These are people who aspire to the American Dream, but don't have the skills – or the desire to get the skills – to make it in America. The book documents the rise and fall of many ethnic groups from the Italian, Jewish, and Irish mobs' rise and fall, to the current black, Puerto Rican, and Russian gangs. The book is primarily an overview of what has occurred, with a bit of applied sociology prognostication as to what the future may hold.

The criminal road for these minorities is one of crime, legitimization, success, and replacement by a new group. The author argues – we believe correctly so – that what we have today is what we had yesterday, and what we will have tomorrow. As long as there is a market-dominant majority, the minorities feeling excluded will choose to climb a ladder of success, but to use a crooked ladder to go around the wall instead of over the wall. A good

read for anyone trying to put a face to the causes and support of modern gangs, and how modern gangs can evolve into modern mobs.

Menace to Society: Political-Criminal Collaboration Around the World
Roy Godson, *et al*

Transaction Publishers ISBN: 0-7658-0502-2 301 pages \$29.95

<http://www.transactionpub.com/> 1-732-445-1245

This book is a collection of papers dedicated to the demonstration of the Political Criminal Nexus (PCN). Growing up in Chicago we never needed a book showing us the connection: It was in the street with the Aldermen, and in the local bar where jobs were meted out to the politically faithful.

But what is not widely known is that many *countries* have a substantial criminal element hiding behind the facade of legitimate government institutions. Colombia, Hong Kong, Mexico, Nigeria, Sicily, Taiwan, Turkey, and the Ukraine are the particular subject of this volume's work. Several countries that were missed include virtually every other former communist nation, Bolivia, Burma, Peru, Venezuela, and half of all sub-Saharan nations.

In many of these nations there is no developed infrastructure for commerce, so commerce goes to those businesses that can curry favor with those in power. In many cases those in power use this power against their opposition (for example Mugabe in Zaire inciting riots against his opponents), to stay in power. This is not a new tale for those of us who work in international due diligence and law enforcement. Rather, it is an old and sad tale that often ends in violence, as those in power use every resource to remain in power, leaning for aid on those elements of society that have benefited most from their favors: The criminal elements aligned with the government. It is always a question as to which is the dominant party in the PCN, but the truth is that, over time, they become co-dependant.

This is a darn fine piece of work in terms of both documentation and research, as well as in the presentation of the material. We think it is worth well more than the published price. It is a good read for anyone interest in these sorts of problems, and a good explanation of why some governments do the things they do.

7. Free-Subscription/Unsubscription/Copyright Information

•• AEGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2003 by The LUBRINCO Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com) and L. Burke Files (LBFiles@lubrinco.com).

The LUBRINCO Group provides services in three high-threat areas, too specialized to be dealt-with in-house, that can adversely affect domestic and international bottom lines.

- **Protection of trade secrets and intellectual assets.**
 - Anti-economic espionage.
 - OPSEC: The identification and protection of information that would give your competitors and adversaries an advantage.
- **International financial investigations and due diligence consulting.**
 - Location and recovery of missing and hidden assets.
 - Establishing business relationships and strategic partnerships in Central and Eastern Europe, the offshore financial centers, Beijing and Shanghai, Central Asia, and Latin America and the Caribbean.
 - Anti-money laundering and financial fraud requirements under the *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2003* and the *EU Revised Money Laundering Directive of 2003*.
- **Protection of management, staff, and families.**
 - In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.
 - When traveling and living overseas.
 - When transporting items of substantial value.

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

For information on **The LUBRINCO Group** and its services, or for the archive of all past issues of AEGIS 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 2003 ÆGIS e-journal (© 2003 LUBRINCO & FEE), to be found at <http://www.lubrinco.com/>.

ÆGIS e-journal is a forum for the exchange of information, ideas, operating styles, theories, and related topics for corporate managers who make decisions about threats typically outside the expertise available in-house, yet which have the potential to affect their company's domestic and international bottom lines. Nothing appearing in ÆGIS e-journal should be

construed as legal advice. The information provided is “general information,” not “specific advice.”

The solution to any problem is highly dependent upon the precise facts involved. Thus, before making any reliance upon anything said here, you should consult with an appropriately skilled professional. Opinions expressed by contributors are not necessarily endorsed by the publisher, and may be presented to encourage a dialogue among subscribers. The publisher and any re-publisher cannot be held responsible for any loss incurred as a result of the application of any information published in *ÆGIS* e-journal.

Please be safe, and be smart.