

ÆGIS



Addressing threats that affect your bottom line

Volume 8 Number 6, June 2005

From the case files of

The LUBRINCO Group

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

and

Financial Examinations and Evaluations, Inc.

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

Asset location in fraud, theft, and divorce? Call us!

This month's features:

- 1. Asset Location and Due Diligence — “You can’t cheat an honest man...”**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Is the US more spy-free than Germany**
- 3. Executive Protection — Keeping fit**
- 4. Technical Issues — Planning for plan failure**
- 5. Real Stories from the Field — Psychological considerations**
- 6. Book and Product Reviews — Brute Force**
- 7. Subscription/Unsubscription/Copyright Information**

1. Asset Location and Due Diligence — “You can’t cheat an honest man...”

Most of the best frauds involve two willing parties. The first is the fraudster. The second is the victim, who is often a willing participant because of greed. Indeed, many fraudsters have assured us that fraud is difficult without a willing participant.

Greed takes a lot of forms. One form is to believe that a bargain any rational person would believe is too good to be true is actually true. Another is to go along with a deal that you *suspect* is shady, but decide not to question it. Another is to *know* that things are likely not on the up and up, but decide to go along with it anyway,

In general these kinds of fraud happen to greedy individuals acting on their own behest. However, it is not uncommon for individuals acting on the behalf of their organizations to equally be taken for a ride. Greed and cupidity, after all, remain greed and cupidity independent of whether they are on behalf of the individual or the organization.

As an example, some time ago, central banks in at least Latin America received correspondence purportedly from the Montserrat branch of a large U.S. bank that will remain nameless here. The correspondence said that there was a fund available for small (\$20 million to \$100 million) loans to developing countries. The fund was at a very low interest rate, and the only cost would be a nominal \$50,000 handling charge. This was a great offer from a reliable bank. It was an offer too good to turn down. Some would say that it was, in fact, an offer that was too good to be true.

As it worked out, a number of smaller banks wired off the handling charge (the code appeared to be quite legitimate), and sat back waiting for their loan to arrive. By the time the banks realized that they had been defrauded, the funds had gone through many, many, many subsequent transfers before disappearing forever.

Could the funds have been traced? Sure, but the fraudsters were smart in the theft, in the covering of their tracks, and most important of all, in their psychology. It would have cost more to find the missing funds than would have been recovered, so it made more sense to drop the whole matter. More to the point, the whole fiasco was so embarrassing that it was thought to be better to write off the small amount of the handling charge rather than to appear to be a fool.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Is the US more spy-free than Europe

In an article in <http://www.agentura.ru/english/Right?id=20050511152800>, it is claimed that there are roughly 130 intelligence officers from the SWR and the GRU performing economic espionage in Germany. Similarly an article in <http://business.iafrica.com/worldnews/439462.htm> notes that “A network of Chinese students coordinated from Belgium is believed to be carrying out industrial espionage in several northern European countries.”

Putting aside articles about spies from countries other than Russia and China hitting Europe, just these two should make you ask several questions. One of these might be “How likely is it that Europe is under attack by spies, and the U.S. is not?” Another might be “If Russian or Chinese spies are in the U.S., could my company be a target?” A third might be “How well-prepared is my company to deal with Russian spies? Or any professional spy from any other country, for that matter?”

The answer to the first question is that if spies are committing economic espionage in Europe, it is a safe assumption that they are also doing so here, and that there are more of them here than there are in Germany.

The answer to the second question is that your company may be the target of an attack if you make a product that would be of value to a foreign government. You could be the target of an attack if you make dual-use products, or products of military value,. You could be the target of attack if you make products for which there is not the infrastructure for development by the foreign government. You could be the target of attack if you make products that are also made in the foreign company (or would like to make them), and where, by stealing from you, development costs could be avoided. In fact, you could be the target of an attack independent of what you make or do.

Finally, how well are you equipped to deal with this? Well, that depends. One way to tell is to call the person who runs your company’s OPSEC program and ask which foreign governments are on their threat list.

What? You say your company doesn’t have an OPSEC program? In that case it is a fair guess that you are not equipped to deal with spies. And that you aren’t equipped to deal with competitive intelligence. And that you aren’t equipped to deal with theft. In this case consider your contribution to the annual \$300 billion cost of information loss a sort of voluntary tax – one that you are legally bound to report, according to the SEC.

3. Executive Protection — Keeping fit

Keeping fit is important for a number of reasons, including the fact that you feel better, you function better, and you are less prone to injury. As an example of the reduction of injury, it turns out that older people fall largely because they lose their balance, grab onto something for support, don't have enough hand- and arm-strength to support themselves, and fall.

The sad part is that keeping in adequate physical condition is, for most of us, a matter of choice, with the tradeoff being fitness for time. The object, therefore, is to maximize the fitness (strength, aerobic capacity, and flexibility) while minimizing the time. For those of us entering our ~~declining~~ golden years – that is to say those of us over 50 – current research indicates that the shift needs to be from aerobic to strength training. Flexibility is always a given. Obviously, before you launch into any exercise program, you should have a quick chat with your physician to make sure there are no problems that would preclude this.

Flexibility

In terms of time, flexibility is the easiest to deal with. We have found the SynerStretch program from Health for Life (<http://www.healthforlife.com/>) to be excellent, and doing the stretching exercises takes under ten minutes a session.

With flexibility training, as with all exercise, keep in mind that you took a long time to lose flexibility, and that you should plan on doing your flexibility exercise for some time before you get flexible again. If you try to rush the process you are likely to injure yourself, not become flexible faster.

Aerobic Conditioning

Aerobics are the next easiest, as there are any number of possible ways to get aerobic training. If you do an hour and a half of aerobic training a week (three half-hour sessions, or six quarter-hour sessions) you should be fine. Note that we are talking about aerobic *training*, which means that you must monitor your heart rate to keep your pulse in an appropriate training range. This means you must have a heart-rate monitor. There are many such monitors around. We use monitors from Polar (<http://www.polarusa.com/>).

As you would expect, there are various approaches to figuring out the training range. The American Heart Association recommends calculating a

maximum heart rate by subtracting your age from 220, or 220-age. Thus, if you were 63 years old, your maximum heart rate would be 157.

They then suggest that the range to build endurance would be 50% to 75% of the maximum, or, for our 63 year old, a low range of $.5 \times 157 = 78.5$, and $.75 \times 157 = 117.7$. In practical terms this means you want to spend a half hour with your heart rate between 80 and 120. It will probably take five minutes to reach that heart rate, and you need to follow it with a five minute cool-down period, as you let the rate drift down toward normal.

An alternative approach makes the formula for maximum heart rate 210 minus half your age, from which you then subtract ten percent of your bodyweight, or $(210 - .5 \times \text{age}) - (.1 \times \text{bodyweight})$. Thus, if you were 63 years old, your maximum heart rate would be 163.

They then suggest that the range to build endurance would be 70% to 80% of the maximum, or, for our 63 year old, a low range of $.7 \times 157 = 114.31$, and $.8 \times 157 = 130.64$. In practical terms this means you want to spend a half hour with your heart rate between 115 and 130. (If you are losing weight, this formula suggests the fat burning rate to be 60% to 70%, or, in this case 95 to 115.) It will probably take five minutes to reach that heart rate, and you need to follow it with a five minute cool-down period, as you let the rate drift down toward normal.

Keep in mind that the cool down period is critical. If you get your heart really pumping and then suddenly stop exercising, you face the possibility of fainting or, worst case, dying, as your blood pressure plummets.

Getting quickly to the target heart rate range, maintaining the heart rate in this range for the specified time, and then tapering safely off to a normal heart rate all require some thought. There are a lot of options, starting with running and ending with various machines. Our personal favorite is the Nordic Track, largely because it puts so little stress on our knees.



Strength Training

Strength training can be the most difficult area to address, both in terms of the rich set of choices, and in terms of the fact that it is increasingly difficult to stay in top shape as one grows older. However, increasingly difficult does not mean overly difficult. In fact, even if one has allowed oneself to get out of shape, getting back in shape is more difficult than when one is 20, but, even so, not all that difficult.

We believe that the most effective way for to retain or regain your physical strength involves use of machines. One approach is to join a gym, which, of course, has a lot of virtues. The problem with a gym is that it can be overly time-intensive for the busy person. An alternative would be the home gym.

We opted for the home gym. We did this because, even though there is a gym two blocks from our office, we realized that by the time we strolled over to the gym, got dressed, and hit the machines we would already be finished exercising at the office. On the other hand, we know people who don't have the discipline to exercise without the social pressure of a gym, and, preferably, a personal trainer.

There are a lot of choices for home gyms. After a good deal of investigation we opted for the BowFlex, in our case the BowFlex Ultimate XTLU. As is normal in the world of technology, this was the top of the line unit when we bought it, but there is now an Ultimate II, which is somewhat different. This doesn't bother us in the least, as most of the exercises are the same, and we expect to be long dead before we exhaust the utility of the device.



The BowFlex is an extremely effective and versatile piece of exercise equipment. This is important, because you need to change your exercise routine regularly. This means that you should do one routine for a month, then change to another for a month, then change to yet another.

One of the dangers with any piece of exercise equipment is over-enthusiasm. In this case, the risk is that you will use too much resistance. We ourselves fell prey to this, and for a short period of time, went through more discomfort that was reasonable. We learned our lesson from this, and, based on our experience, we **STRONGLY** urge you to keep the resistance to the point where you can do the appropriate number of repetitions cleanly, and without strain. This will allow you to gain strength without a needless amount of muscle and tendon pain.

Keep in mind that you are not in a race, and will be exercising for the rest of your life. There is no great benefit to causing yourself needless discomfort. If it took you ten or twenty or thirty years to get out of shape, there is no reason to think you should be able to undo this in two months...

The combination of aerobic exercise, flexibility exercise, and strength exercise can add decades of functionality to your life. This is worth the time and effort it will require.

4. Technical Issues — Planning for plan failure

We recently spoke at the CPM 2005 West conference. We arrived at our lecture room a few minutes before the previous talk ended. The speaker was wrapping up, and noted that when you made plans, it was prudent to make back-up plans in case your original plan failed. This is an important point, and, although we have discussed it in the past, it is well worth repeating. In this article, we will only talk about travel contingencies.

As an example of what can go wrong, some time ago we were in Teheran, and found ourselves needing to leave with some urgency. Leaving by plane, the most obvious choice, was, for a number of reasons, not possible, so our backup plan was to leave by train.

As it worked out, taking a train out became unfeasible, so our backup plan to that was to take a bus. In fact, this worked for us and we were able to make it safely out of Iran. Had the bus not worked we had several other plans, ranging from the pedestrian (walk across an unguarded border into Turkey) to the exotic (by camel to Afghanistan, which would have created a different set of issues).

How many sets of plans you need to have depends on what you are doing, and the consequences of plan failure. In a situation where the consequences are negligible, you may choose not to have any backup plans. If the consequences are more serious you may have a plan. If the consequences are really serious – someone may end up dead – you will likely have several sets of backup plans.

How serious is serious? Only you can judge. When we go out we habitually carry a small safety kit with us that includes a flashlight, gloves, rescue knife (February 2003 AEGIS), smoke mask (August 2004 AEGIS), and a whistle (September 2004 AEGIS). This is enough for normal use. If we plan to be somewhere that nobody could hear a whistle (like out hiking), we would likely throw in a personal locator beacon (October 2003 AEGIS).

When we go abroad to a place where we do not anticipate trouble, we usually plan to return by our return flight. If it is a place where there is a probability of a disruptive natural disaster or political problem, we may have a backup plan and a backup plan to that. If we are running a protective detail, we are likely to have several layers of backup plans.

Bottom line, in almost anything you do you should have a backup plan. And if it is important, you should have a plan for what to do if the first plan fails.

5. Real Stories from the Field — Psychological considerations

You have prepared for disasters. You are ready for almost everything. You have the data secured, employees are trained in evacuation and you have appropriate drills, your sprinkler system has just been tested and your security force and disaster team are brimming with pride.

And then they get tested, and you start to discover things overlooked.

In a building in the Midwest, a typical summer storm-related blackout occurred. Power went down, but the computer back up power supplies kept the system running. Emergency lights came on and the non-essential people left, as the emergency generator kicked in to power the key areas of the building including the data centers, executive offices, hallways, and the main lobby. The main lobby?

That's right, the main lobby was lit up like a Christmas tree, while all around was dark. The unseen halls were lit, the unseen data center was running, and the lobby stuck out like a sore thumb in the middle of a dark city.

The security and the disaster recovery people were so proud of their achievement that no one thought of it until a VP came down and said "Why are all those people outside staring at the lobby?"

Well one more light went on – this one metaphorical – and the lights were turned out in the lobby.

Now there is a slightly modified protocol – when the emergency system kicks in, keep safety lights on, darken the lobby except for emergency lights, and make sure all of the shades are drawn on the executive floor. (The data center has no external windows, and is not likely to become an attractive nuisance.)

Why was this change made? Well, in the test there was no real issue. But this was just a test. What if it were a real situation. In this case a well-lit lobby would become an attractive resting place for those trying to escape rain or snow. While in a regional crisis it might well be appropriate to shelter as many people as possible, in a normal crisis this would not be appropriate, and would potentially cause a lot of problems.

How had this been overlooked? In this case nobody had given thought to the psychological implications of a brightly lit lobby when all around was dark. Although the generator was capable of handling the lobby, in this case it was not a swell idea.

6. Book and Product Reviews

Brute Force: Cracking the Data Encryption Standard

Matt Curtin

Springer-Verlag ISBN: 0-387-20109-2 280 pages \$25.00

<http://www.springeronline.com/sgw/cda/frontpage/0,11855,4-102-22-45347046-0,00.html> 1-212-460-1500

For roughly twenty years, DES was the standard for encryption. It was felt by cryptographers that this 56-bit system was, in theory, too easy to crack. Of course, there is a difference between theory and practice, and when DES was put into place a supercomputer would have been needed.

With the passage of time, however, computers became more and more powerful, and, with the arrival of the Internet, it became possible to coordinate the distribution of workload where the solution to a problem involves the same program run many times with different data. That is to say, if a solution requires the same program to be run 10,000 times, it can be run 10,000 times on one machine, a thousand times on ten machines, and ten times on a thousand machines.

Brute Force describes the breaking of an unbreakable DES encrypted message by a cooperative effort among many users, on tens of thousands of machines. The book is well-written and interesting, but is useful in a larger sense in at least two other areas.

First, it gives the reader some idea of how encryption works, why it is important, and why strong encryption should be readily available. It also makes clear why encryption algorithms should not be “secret.” And it explains why it is better to have good encryption than to prevent it from being widely available.

Second, it gives the reader some idea of how powerful distributed processing can be. As a non-encryption-related example, we know of an investment bank whose yearly pricing model in the SWAPS and derivatives department took over six months to run. Actually, it was, in fact, habitually interrupted about then, and never ran to completion. By, er, acquiring the user IDs and passwords of every UNIX workstation on the system, the pricing model was made to run over a weekend, allowing it to be run weekly, not yearly, which in turn gave a competitive advantage.

Since encryption is such an important topic these days, this book provides some interesting background, an interesting story, and a lot of good food for thought, even for those not interested in encryption *per se*.

7. Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2005 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@feeinc.com).

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

- **Sarbanes-Oxley Section 404 OPSEC compliance.**
 1. American businesses lose \$300 billion annually to competitive intelligence, economic espionage, and information theft.
 2. Sarbanes-Oxley requires internal controls tracking the costs, and impact on valuation, of competitive intelligence, economic espionage, and information theft.
 - LUBRINCO provides private sector access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information from competitive intelligence, economic espionage, and information theft.
- **International asset location and due diligence.**
 - Location of concealed assets in fraud, theft, and divorce.
 - Due diligence to prevent fraud and loss in China, Central and Eastern Europe, Central Asia, the offshore financial centers, Latin America, the Caribbean.
 - Financial fraud and anti-money laundering program development and training for compliance with the US *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001* and the EU *Revised Money Laundering Directive of 2001*.
- **Protection of management, staff, and families.**
 - In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.
 - When traveling and living overseas.
 - When transporting items of substantial value.

LUBRINCO identifies and quantifies threats and vulnerabilities, and their associated risk, then manages the vulnerabilities so you can transfer or live

with the residual risk. We prevent disastrous financial loss to your company, and physical harm to you, your family, and your staff.

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

Subscription to **ÆGIS** is available for \$15 per year in North America and \$20 per year outside of North America.

To sign up for a **complimentary subscription** to **ÆGIS** or the **ÆGIS** PDF notification list, go to <http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to aegis@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 aegis@lubrinco.com.

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

If there is a topic that you would like to know more about, send it to aegis@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**, send it as an attachment to an e-mail to aegis@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** constitutes a license to **LUBRINCO**, and/or Financial Examinations and Evaluations, Inc, their assigns, associates, or affiliates, to abridge and/or edit said submission, and to copyright and publish/republish any submitted materials in whatever written and/or electronic form they may choose.

If you would like to go beyond normal fair-use in reproducing articles from this issue of **ÆGIS**, you may do so freely as long as appropriate source, copyright, accreditation, and link to the **LUBRINCO** Web site is included. This should be in the form

Article Title, from the June 2005 **ÆGIS** (© 2005 **LUBRINCO** & FEE), to be found at <http://www.lubrinco.com/>.

ÆGIS is a forum for the exchange of information, ideas, operating styles, theories, and related topics for corporate managers who make decisions about threats typically outside the expertise available in-house, yet which have the potential to affect their company's domestic and international bottom lines. Nothing appearing in **ÆGIS** should be construed as legal advice. The information provided is "general information," not "specific advice."

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

Please be safe, and be smart.