



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 7 Number 6, June 2004

From the case files of

The LUBRINCO Group
<http://www.lubrinco.com/>

and

Financial Examinations and Evaluations, Inc.
<http://www.feeinc.com/>

Concealed assets in fraud, theft, and divorce? Call us!

This month's features:

• **Special Announcement**

- 1. Due Diligence — What companies can learn from Abu Ghraib**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Offshore outsourcing as an information radiator**
- 3. Executive Protection — Arrival identification**
- 4. Technical Issues — Bluejacking and bluesnarfing**
- 5. Real Stories from the Field — Competing with ourselves**
- 6. Book and Product Reviews — KEYController**
- 7. Free-Subscription/Unsubscription/Copyright Information**

Read *How Not to Tell All* by Richard Isaacs in the May 2004 issue of *Security Management*

L. Burke Files will be speaking at the
2nd Annual International-Caribbean Offshore Business Convention
10 June 2004, Dominica

<http://www.samuelgroup.com/cprmg/offshore-convention.html>

1. Due Diligence — What companies can learn from Abu Ghraib

Rumors and complaints had been floating around for at least half a year before the pictures from Abu Grahیب were made public, causing great embarrassment and turmoil. We think that there are three lessons that companies can learn from this incident. These lessons are based on the mantra of high-threat protective services, which is applicable over a wide variety of activities. This mantra is:

- See something.
- Tell someone.
- Do something.

Lesson one: See something

Exercise due diligence

Seeing something is prefaced by *foreseeing* something, which we generally identify with the exercise of due diligence.

We define due diligence as any action that, if you fail to take it, will open you to a charge negligence because you either knew of the risk or should have known of the risk. While some tend to think only of financial due diligence, we believe due diligence extends to every area. Thus, if you have a young child and a swimming pool, you ought to be able to envision the danger of your child falling in and drowning if you do not have a fence. If you have a parking lot, and the area is dangerous, you ought to be able to envision robberies taking place at night if there is no supervision. If you are a financial institution, you should be able to envision that someone will want to launder money through you. If you have a prison – and in particular a prison in a war zone – you ought to be able to envision abuse.

Once you are aware of the potential for a problem, the exercise of due diligence demands that you take preventive measures to try to ensure that the potential problem won't become an actual problem. As an example, we have a client in an industry that has historically demonstrated the potential to take

advantage of desperate customers. This company has written rules against this. In addition, they discuss the issue regularly in meetings. Finally, they hire us as secret shoppers, to go to their offices and see if we can get their staff to make claims they cannot fulfill, which would, were we actual clients, be to our disadvantage. While it is certainly possible that some employee could still do something against company policy, it is clear that this would be an aberration within a given office, not a systemic problem encouraged by senior management or the corporate culture.

The bottom line is that everyone on staff should always be thinking about potential problems, and how to head them off. And that someone in senior management should be making sure that the company's commitment to good behavior is an actual part of the corporate culture, not something said with a knowing wink. We ourselves have a rule – one of our core values – that we will not work for bad people, and will not do bad things (both of which are possibilities that are, by definition, part of our business). Because of this, when we are approached to do a job we need to know who our final client will be, and why they want us to do what we are being hired to do. We have turned down jobs where the client seemed unsavory, or because we believed the potential client had no right to the information they sought.

Watch for problems that occur in spite of your good-faith efforts

While the exercise of due diligence will go a long way to eliminate problems, they can still happen. Because of this, people and institutions need to be ever vigilant. This vigilance can be, and in many cases should be, institutionalized. As an example, police departments have internal affairs people looking for police misconduct. Intelligence agencies have counter-intelligence people looking for traitors. Construction sites will sometimes have a non-construction civilian wandering around to make sure that what is being done looks sensible: Should there really be urinals in the ladies' bathroom? Shouldn't there be rebar in the hole before you pour cement? Auditors will look for anomalies like employees who have no benefits. The International Red Cross provides scrutiny of prisons.

The object is to have someone who can spot anomalies that are not being hidden. And to spot bad things that are being hidden.

Lesson two: Tell someone

In virtually all cases where there is a serious problem, someone saw something that could have prevented the problem, had they but told the right

people. As an example, on 30 November 1989 heavily-guarded Deutsche Bank director Alfred Herrhausen (but not his driver) was killed by a bomb while being driven to work. Killing someone in moving car with a bomb, without killing anyone else, is tricky because the car is moving, so you can't simply judge it by eye and press a remote control button. In this case, a trench was dug across the street, a cable was buried, and a sensor was installed. Now the remote control merely needed to activate the device after the lead car passed. A lot of people saw the installation performed, but the right people weren't told.

Lesson three: Do something

Whenever a problem is discovered, there are several questions that must be asked in deciding what action is to be taken.

Is it serious?

Obviously, there are lots of things that can cause problems. Some are serious, and some are not, and it is not always that easy to tell the difference. If you see some water on a carpet it could either indicate someone spilled a glass of water, or that a pipe has burst. If a kid gets into a fistfight it could be adolescence or an indication of a problem with bullies or gangs. If you smell gas, has the pilot light gone out, or is there a broken gas main in the street seeping in through the sewer pipes? If a prisoner is abused is it a single guard that needs to be removed, or is it something more?

Is it systemic or unique?

While solving a problem will have many common elements independent of whether it is a unique problem, or an indication of a systemic problem, there is a lot more to be done if the problem is systemic. That is to say, you have to get to the heart of the cultural issue, and change that before you can have some confidence that the problem will occur less frequently. We ourselves are a suspicious lot by training and temperament, and tend to subscribe to the "once a coincidence, twice a conspiracy" approach.

What are the PR implication

In certain cases merely solving the problem is not sufficient, because there is a social, emotional, or public relations piece of the problem that must be *recognized* and dealt with. When this is the case, you need to own the problem, rather than merely reacting to it. Issuing a quiet press release without emphasizing its importance because you don't recognize its

importance can turn you from being a hero who found and fixed a problem into a fool who didn't recognize it. Or, even worse, you can be taken for a knave who deliberately chose to overlook it. Frankly, you really want people to think of you as a hero, and don't want people trying to decide whether you are, as the only two choices, a fool or a knave.

Abu Ghraib is an excellent example of this kind of issue. As we understand the chronology, the International Red Cross reported problems in October of 1993. The issue reached the attention of senior staff in January 2004. The Army ordered an investigation (you can read the report of Major General Antonio M. Taguba at <http://www.agonist.org/annex/taguba.htm>), mention of which was included in two public press briefings. This led to the current set of ongoing investigative and disciplinary actions. The process worked, and the military was cleaning its own house.

The process, however, did not take into account the emotional, social, or public relations implications of the problem, apparently because it was simply not recognized. Thus, when asked in Senate hearings if he had briefed the President on the issue, Defense Secretary Rumsfeld said he briefed the President on many things, and didn't remember. We have no reason to disbelieve him, but it shows that he hadn't recognized that this was an important issue. Certainly not important enough to be remembered.

Can we, in the commercial world, do a better job of taking ownership of a potential scandal than did the government? Sure! Just look at the way Johnson & Johnson handled the discovery of tainted Tylenol. They took ownership of the problem, and emerged with full customer confidence, and an unsullied reputation. Then compare that with the Firestone Tire scandal.

As Americans, we of course wish that no abuses ever happened under the color of our flag, but recognize that abuses can always happen, even when we are vigilant. And we are proud that the military addressed the problem, and of its own volition.

But we also wish that someone – anyone! – senior within the administration had recognized the serious nature of abuse in the most infamous Iraqi prison, and made a timely and independent (i.e., not mixed with other announcements), public, and condemnatory announcement regarding Abu Ghraib. Something like, “We have discovered this. It is not the American way. We are stopping it, and seeing that it never happens again.” Had the administration taken ownership of the problem, we believe they would have been thought heroes.

Practice, practice, practice...

Hopefully, you will be alert and sensitive enough to recognize and deal with problems of social import, allowing you to emerge a hero. But the likelihood of your reacting appropriately without having pre-thought similar problems is sadly low. As in most things, in a time of crisis you will react the way you trained. If you have never practiced to deal with significant issues, you will do nothing contributory.

How do you practice? Well, your crisis management team should regularly run dynamic simulations. Some of these should include strange crises, with the participants including management, corporate communications, and the outside PR firm. Keep in mind that these simulations must be run by someone outside the system. Anything you can think of should go into the crisis list. Abusing spouses holding an employee captive. Senior managers, committing fraud. Senior managers being arrested for bizarre and embarrassing crimes. Seepage of industrial waste into the water table. In one case we staged what eventually turned out to be the homicide of the president of the company by his head of corporate communications. Go out of your way to think of issues that go beyond the mere problem itself.

By including this kind of training, you will find yourself better positioned to identify and deal with critical problems that have a life of their own. You will have a chance to be a hero, and not a fool or a knave.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Offshore outsourcing as an information radiator

In the 60s American programmers earned around \$40 an hour. In the 70s they made around \$60 an hour. In the 80s they made around \$80 an hour. In the 90s, a time of much technical innovation, they made under \$90 an hour. Now, in this fourth year of the new millennium, we are given to understand that clock has been reset and that a good Java programmer is earning around \$40 an hour once again.

Forty dollars an hour – almost eight times the minimum wage – is a lot of money for someone sitting in a cubical all day. More to the point, it is four times as much as the twice-minimum-wage that one can pay for a good programmer overseas! Because of this price differential, not only in programming, but in a widening variety of areas, a lot of work that used to be done here – programming, review of your federal income taxes, management of your health care records, customer care, interpretation of x-ray, manufacturing and assembly, and accounting – can be outsourced

internationally. If it involves a bunch of people, and doesn't require someone physically here, it can probably be outsourced.

But there is a potential downside to outsourcing, particularly when it involves intellectual property: You are giving your intellectual property to someone who might not have the same standards regarding protection of intellectual property that exists in the United States. In fact, we are given to understand that a lot of Y2K work was outsourced overseas, and that the core processes within the programs were generously spread to competitors throughout the world.

A case can be made that while it is one thing to give away your core processes, the processes themselves don't do all that much good without the data that goes with it. This is may not be entirely true, as your competitors have their own numbers, and your processes might be of as great value with their numbers as they are with yours.

But let us say that it is true. As it happens, most companies do not examine all that carefully code that is written in-house, unless it fails, in which case someone looks at it. We can tell you from painful experience that relatively few organizations have coding standards, and that fewer still have people on staff to review code to make sure it adheres to those standards. And the likelihood of review diminishes when you have outsourced your coding.

You should therefore consider the possibility that, when you outsource programming, you are sharing your code with others, and that it is not impossible that backdoors will be built into the code to allow access to your data, as well as to the handling of that data.

While outsourcing is often the appropriate thing to do, be sure to throw the cost of lost intellectual property into your calculations.

3. Executive Protection — Arrival identification

When you were a kid your mother told you not to get into cars with strangers. This advice is still pretty good, particularly in areas when kidnapping is a growth business.

This has been particularly in our minds because of several incidents that have taken place in the last while. One involved a protective team (not ours) in Thailand that escorted the person in their trust into a car that turned out not to be theirs, as they discovered a few minutes later when their car, driven by their driver, arrived.

In Colombia, we once arrived at the airport to discover a driver holding up a placard with our name. We didn't know the person, so before approaching him we called our office to find out why someone we knew wasn't there to pick us up, and to get a description of the person sent.

In Buenos Aires and Mexico City, both cities in which one does not prudently get into a taxi these days, it is wise to arrange for a car and driver, and made sure that pictures go back and forth so each party can recognize the other without the need for names being held up for all the world to see.

The bottom line is that while there are many places in the world where it is safe to get into a taxi, there are a lot of places where this is not the case. In these places you should not be getting into cars with people you don't know.

How do you tell which places are dangerous and which aren't? If your company has a travel department, or a group that provides protective services for senior management, at least one of these should be subscribing to a service such as that offered by Specialized Consulting Services (<http://www.speconsult.com/>), which we discussed in our article "We are going *where*?" in the March 2003 issue of AEGIS. They should therefore be able to give you a very accurate picture of the level and type of threat you are likely to face.

If the level of risk is not sufficiently great as to require an actual protective team, it may be still appropriate to arrange for a **known** car and driver. If you do this, and are using someone you know and trust, it is better to exchange pictures of the traveler and the driver, so each knows what the other looks like. If that is not practical, you should arrange a name to be put on the placard, and some sort of verbal identification.

While this may seem a little to secret agent-ish, it is still better than being kidnapped, and having to send us to liberate you.

4. Technical Issues — Bluejacking and bluesnarfing

One of the exciting new additions to the world of cellular devices is Bluetooth. Bluetooth-enabled devices allow all sorts of interesting communications, including connections to laptops, to wireless headsets, to car hands-free kits, to local devices which will send you sales messages, and even to devices to allow you to make purchases.

The less exciting news is that in November 2003, Adam Laurie of A.L. Digital Ltd. discovered flaws in the authentication / data transfer mechanisms on some Bluetooth-enabled devices. At the moment some

Nokia and Sony Ericsson devices have the theoretical potential to cause you some problems. (We are given to understand that Sony Ericsson has made an effort to fix the problem, and that Nokia said the problem is not serious enough to warrant repairing.)

Bluejacking (originally a way to send messages to another handset based on “discovering” their Bluetooth device, including messages which will re-set certain devices) and bluesnarfing allow hackers to download text messages, phone lists. Bluesnarfing also allows remotely tampering with handsets to enable them to be used as listening devices. This means that someone could, without your knowledge, download all the information on your handset. And they could in essence make a silent call to them, and listen in on whatever is being said.

In addition, there are companies that offer services which allow you to track specific handsets. This is generally done to track sales people, and for other similar, legitimate reasons. But with some handsets, an unscrupulous hacker can use Bluetooth to surreptitiously insert the activation code, and be able to track the handset 24 hours a day, without the owner of the handset being aware it is being tracked.

How serious is this? Well, if you don’t care about sharing your information, it isn’t serious at all. If sharing your information, or being listened-in on, or being tracked would present a problem, then it is at least a concern.

How do you deal with this? If you have a Bluetooth device, keep it in hidden (not visible or discoverable) mode. Even better, turn off Bluetooth if you don’t actually use the feature.

5. Real Stories from the Field — Competing with ourselves

We work largely in areas where we have relatively little competition. If you need financial investigations or due diligence in China, or Central and Eastern Europe, or Central Asia, there are not a lot of players. And if someone has stolen \$200 million from you, there are not a lot of people to call on to try to get it back. And you can count on very few fingers of your hand the number of service providers who have even heard the term OPSEC! We can generally tell that the field is small because other firms will occasionally sell a job in competition with us, and then subcontract the work to us.

However, we have never thought of ourselves as being totally unique in the small world of high-risk protective services. There are, in fact, a number of very good companies in this specialized field – though for certain tasks, like

bringing a few hundred million dollars worth of uncut diamonds out of Africa, we think we are the best in the business.

Because of this, we were surprised to find that we have now started competing with ourselves in providing protective services in Colombia. We are not sure why there is a sudden influx of protective service offerings in Colombia, but we are delighted that, even if we lose in our bid to provide you services while you're there, we are likely to still have the opportunity to get you safely in and out.

6. Book and Product Reviews

KEYController

KeySure

PO Box 362

Hudson NY 12534-0362

<http://www.keysure.net/> 1-518-828-5337

Some time ago we took responsibility for the protection of an apartment that contained several million dollars worth of art. The first thing we did was change the alarm codes, with re-keying of the locks scheduled for day two. At 3 a.m. the alarm went off, and the front door was discovered to be unlocked and open.



Upon re-keying the locks, one of our concerns became the keys that had to be, by law, left with the building.

Traditionally, in most apartment buildings, the super puts a label on each set of keys and tosses them all into a drawer. Since the super's office is generally less than fort-like, the keys are vulnerable, and it is easy for someone to take a key, rob an apartment, and then return the key.



One approach commonly used is to put the keys in an envelope, seal it, and sign the back. This allows you to see whether the envelope has been opened. Unfortunately, envelopes are relatively fragile, and over time keys sometimes poke their way through.

KEYController allows keys to be sealed in a small plastic box that can only be open by breaking, which removes all question as to whether the key has been accessed. Obviously, other things, like passwords, or access control

cards, could just as easily be stored. And if neighbors give you keys to hold – particularly sensitive keys, like gun-lock keys – sealing them this way should give everyone a higher level of comfort: The keys are either there and sealed, or missing, or broken-into.

KeySure’s recommendation for setting up a system for a building is:

1. **CODING:** The KEYSURE system is based on a consecutive numbering system. Example: Numbering 1 through 100 if it is a 100 unit building. These numbers then become the code number for each apartment unit.
2. **MASTER CODE LIST:** Since most buildings have a computer print out tenant list or rent roll, we suggest you use this already existing list and simply consecutively number it. Exercise caution, and do not keep the list with the keys.
3. **KEY TAGS:** Each key will be put on a numbered key tag corresponding to the apartment code established above. Key tags are an integral part of the system and serve to organize and identify individual keys. The last thing you want, is to be seen trying keys in tenants doors to identify random keys.
4. **APPLYING CODE NUMBER:** Number the outside of the KEYController container with the same number that is on the key tag.
5. **SIGNATURES:** The tenant signs a signature on both inside surfaces where indicated. The signatures must be applied before the container is closed. The signatures on the inside insure the tenants Anonymity
6. **CLOSING THE KEYController:** After the signatures are applied and the key with tag is placed inside. close the container with a squeezing action, until a snap is heard. Caution: Once closed, the KEYController will have to be broken to gain access to the key.
7. **MOTHER'S MAIDEN NAME:** Have the tenant sign mother’s maiden name on the outside of the container. This will allow a tenant to check up on a key without breaking the container. It also serves to confuse anyone with criminal intent. [NOTE: Since this is a common measure used by banks and others, a middle name, or a pet’s name, could be used instead.]
8. **STORAGE WALL CABINETS DRAWERS:** Carefully load the containers keeping them in numerical order. Good order will make it

that much easier to retrieve keys. Audit the key boxes on a scheduled basis to insure that they are all there and in order.

9. **SECURITY POLICY:** Security of any kind is only strengthened by having a well thought out written security policy. This written policy should be distributed to every tenant so that each tenant understands it and feels as though he or she is involved in the process of creating a more secure and safe environment.

We think the system is worth considering for your coop or condo, if you have concerns regarding the security of your keys. And for the storage of other items where you need to be able to confirm if they have been accessed.

7. Free-Subscription/Unsubscription/Copyright Information

•• AEGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2004 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 2004* and the *EU Revised Money Laundering Directive of 2004*.
- **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 June 2004 ÆGIS e-journal (© 2004 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.