



**ÆGIS** e-journal

***Addressing threats that affect your bottom line***

Volume 7 Number 3, March 2004

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 — Why we may not be able to talk to you after you hire us**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Camera phones as a tool of information theft**
- 3. Executive Protection — Dealing with threats that you can't envision**
- 4. Technical Issues — How AT&T Wireless and Cingular caught the handset manufacturing world with their pants down**
- 5. Real Stories from the Field — Checking ID**
- 6. Book and Product Reviews — Phone Manager II (for Nokia handsets)  
The Sourcebook to Public Record Information, 5<sup>th</sup> Edition**
- 7. Free-Subscription/Unsubscription/Copyright Information**

## **1. Due Diligence — Why we may not be able to talk to you after you hire us**

In many cases involving the recovery of missing assets, whether because of fraud, theft, or divorce, the proceedings tend to become quite adversarial. This should come as no surprise, because people steal money in order to keep it for themselves, not with the intention of giving it back. And in divorces, animosity often runs so high as to preclude any rational sense of fair play.

The process of recovery is made more difficult by the fact that the adversary more often than not has a lot of money, while you may have relatively little. This happens in the case of fraud and theft if the bad guy has stolen most of your disposable income. It happens in the case of divorce when your spouse works and has control of the assets, and you don't. This last is all too frequently complicated by the fact that attorneys tend to start looking for assets much too late in the game, by which time they have already spent much of the money that should have been available for the investigation.

The problem has two components.

First, if you don't have money to pursue your missing assets, the bad guy will be able to keep them with impunity.

If they have a LOT of assets and yours are more modest, they still have a lot of options. As an example, in one case on which we worked, a father had left his estate with the family attorney in trust for the children. The attorney, being no fool, realized that he had \$750 million dollars in his control and the children had only what he gave them, which went from very little to nothing. When the children tried to get outside help they were met with threats, attempted homicides, and all sorts of legal roadblocks. (You can buy an awful lot of judges and cops when you have three quarters of a billion dollars at your disposal.) Rumor had it that the attorney realized it was just as effective to have us killed as to kill the children. In this case, although we felt we were approaching a point where the case could be turned over to the Feds, the children chose to drop the case rather than continue to tempt fate.

Second, even in cases where the participants don't consider homicide to be a reasonable option, merely delaying things can be a worthwhile investment. If, for example, a husband has \$20 million hidden away, and can spend \$100 thousand to delay action for a year, he will still be \$900,000 ahead even if he only makes five percent on his money. This delay and the cost to the relatively impoverished wife may be enough to make her settle for a pittance.

A common technique that we see is for the adversary to file complaints against the investigators (that would be us!) in order to deplete resources from the plaintiff as a means to avoid having to defend against this legal attack. Since there is no such thing as investigator-client privilege, we can be forced into court and made to reveal all our information, which would be very helpful to the bad guy and very detrimental to our client.

Because of this, in cases where there is even the tiniest hint that this might be an issue, we work directly for the attorney, and have no contact with the client other than through the attorney. What we do is thus work product for the attorney – and is labeled as such – and is protected by attorney-client privilege. Since we do nothing for the client we have nothing that can be disclosed, and, thus, nothing that can be revealed in court. Anything the opposition wants they must try to get from the attorney, not from us, and that is protected by attorney-client privilege.

While this represents a significant protection for the client, it can also be a minor frustration that we may not be able to directly speak each with the other. In this case, however, it has been clearly demonstrated, time and again, that the benefit far and away outweighs the annoyance.

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — Camera phones as a tool of information theft**

Those who read *Inside the Tornado: Marketing Strategies from Silicon Valley's Cutting Edge* (AEGIS November 2002) know that Geoffrey A. Moore posits that the management of a company during a period of rapid growth may not be the management that is appropriate when the industry stabilizes into the provider of a commodity.

We are seeing this played out today in the mobile telecommunications industry, which has evolved into a commodity industry rate of growth of new subscribers, just as the average revenue per user has declined. This change in growth and revenue is not surprising given that, according to John Barrett's *Disconnected: Consumers and the Mobile Phone Industry* (<http://www.totaltele.com/ttdocuments/PDFs/mobile%20industry%20white%20paper.pdf>) from Parks Associates (<http://www.parksassociates.com/>), half of all Americans – 60% of all Americans over 10 – now have mobile devices. The landline industry surely now needs to be run with the approach needed for any commodity industry.

It appears however, that most service providers are still run by management that is locked into the good old days where even a small service provider's

stock might soar to a ludicrous \$100 per share or more. Thus, when we look at the \$60 billion spent over the last three years by the six major providers (AT&T Wireless, Cingular, Nextel, Sprint, T-Mobile, and Verizon) it would appear that much of it was spent on expanding data capabilities (\$50 billion) and data-capable devices (\$10 billion). Yes, as with the landline industry, data will be an increasingly important piece of the pie, but there still needs to be a base level of coverage, which we don't think yet exists.

Thus, when you get on a train anywhere, it is fairly sure that every few miles you will lose signal, for lack of coverage, but will be able to take a picture with your camera phone to send when back in a coverage area. We would suggest, however, that as camera phones become more common, you should give serious thought to banning them in your facilities, and, in some cases, summarily firing anyone found on your premises with a camera phone.

In what sort of circumstances would a camera phone be inappropriate? Well, we have already seen that many health clubs with locker rooms and retail stores with dressing rooms have banned them. We vaguely recall that that some courts have banned them. Some schools have banned them after a few camera-phone pictures of high school girls in the shower after gym class made it onto the Internet.

Some corporations and government areas that have sensitive areas where photography is prohibited, so for them banning camera phones is not even necessary: They are pre-banned. Other corporations that have concerns about physical safety or protection of information should also consider banning camera phones. According to one person who works for one of the mobile telecom service providers, because of an incident they are considering banning camera phones anywhere you can have access to a computer.

The bottom line is that your kids will undoubtedly want a camera phone, which will be fine until their schools crack down on them. For those who work in a business environment, however, buying a camera phone with no expectation of having it confiscated or vouchered at some point is unrealistic. This means that if not having a mobile device at your disposal during the business day would be a problem for you, you are probably better off simply getting a mobile device that allows you to make calls, but not to take pictures.

And for those of you who set policy regarding information loss, you ought to be thinking now about what you want to do to manage the vulnerability created by this very real threat. If there is a ban it should be clear to all and posted both as the property border for a facility and at all entrance points along with the consequences for employee and visitor alike.

### **3. Executive Protection — Dealing with threats that you can't envision**

What do natural disasters, anarchists and terrorists, fraudsters and thieves, and religion have in common? They all present potential threats (of generally low individual probability) for which generic preparation can offer a significant degree of solution. Our goal is to manage vulnerability, to transfer risk, or to reduce risk to a level with which we can comfortably live.

In order to do this, we must stop thinking of causes, and deal with effects. The reason we need to do this is that we know that under the best of circumstances we can't affect threats, and we certainly can't affect threats of which we haven't thought. We also can't deal much with vulnerabilities, that portion of the risk formula over which we do have control. If we don't know the threat we can't identify the associated vulnerabilities. What we have left is worst-case scenarios.

As an example, we once looked at a company that had its computer room next to the parking lot. If a large truck lost its brakes and backed through the wall they would lose their computers. This was a threat (brake failure or bad driver) coupled with a vulnerability. But what if some unknown threat knocked out a computer room that had been protected from every threat of which they could think? It would still be gone.

What actions could they take if they asked what would happen if the whole computer system disappeared, independent of the cause? Well, for a start, they could have one or more backup sites, geographically separated so that if one disappeared, for whatever reason, they still preserved their options. While this would not address the immediate vulnerability (which did need to be addressed), it would still be a better choice.

The good news is that with some small amount of effort, you are likely to be able to identify critical resources without which your organization has a serious problem, and may simply disappear. If you can protect these resources, you don't really care from whence the threat comes.

The bad news is that few organizations bother to do this. We recently asked a senior official in a major metropolitan law enforcement agency whether his department had anyone who sat around thinking about how bad people could do bad things, and how to prevent these bad things from happening. The answer was no, he knew of no such group.

We strongly urge you to delegate a team to identify critical resources. Work out the most cost-effective way to ensure the organization's survival in the face of threats to these resources that you cannot even begin to imagine.

#### **4. Technical Issues — How AT&T Wireless and Cingular caught the handset manufacturing world with their pants down**

For those mobile phone users who have been international travelers the landscape has changed of late. Originally, if you wanted to use one GSM handset both in the United States and abroad, you needed a dual-band handset, which used 900 MHz GSM in the country of your choice abroad and 1900 MHz (on Sprint here in the United States, followed by other GSM providers). Most early adopters started with the 900/1900 MHz Bosch WorldPhone, which was, we believe, the first dual-band WorldPhone.

As the 900 MHz spectrum became overloaded, 1800 MHz was paired with it. Since there were no tri-band (900/1800/1900 MHz) handsets, most international travelers had a 1900 MHz handset for use with the increasing number of GSM service providers in the United States, and a 900/1800 MHz handset for use in Europe and Asia. Eventually it was recognized that some international travelers wanted a single handset, and we believe the 900/1800/1900 MHz Motorola Timeport became the first of the tri-band WorldPhones, leaving dual-band handsets obsolete.

It looked as if this was the way thing would stay, save for the oddity of Latin America, with Panama using GSM 850. Then AT&T Wireless and Cingular made the business decision to add GSM to their AMPS/TDMA base. This created something of a problem, as both companies owned a lot of 800 MHz spectrum. And so they started implementing GSM 850. It appeared to many of us that this would not be a significant factor for users in most areas of the U.S. until the last quarter of 2004, or perhaps the first quarter of 2005. It apparently caught some manufacturers by surprise, too. As late as last year Nokia said that no country outside of the United States had implemented GSM 850, and that only Cingular had implemented or expressed any intention to implement in North America.

We were all wrong. We know AT&T Wireless customers in Boston who get no reception in their offices with 1900 MHz handsets, but excellent reception with 850/1900 MHz handsets. And GSM 850 has been implemented in a number of countries in Latin America and the Caribbean. In fact, if you travel widely in Latin America you need all four bands: 850, 900, 1800, and 1900 MHz.

This means that, in the period of a year, tri-band international handsets became as obsolete as dual-band international handsets. Unfortunately, the development time for a terminal is some years. Since the manufacturers of handsets appear to have been unaware of this technical shift, and caught by

surprise, a flow of obsolete-before-release tri-band handsets is still coming off the assembly lines.

What does this mean to you, the business traveler who uses GSM? Well, you still need 900/1800 in Europe and Asia, and you now need 850/1900 MHz in the United States, and you need all four in Latin America. You have three possible solutions for widest GSM coverage.

1. You can have two dual-band devices: A 900/1800 MHz device for Europe, Asia, and parts of Latin America, and an 850/1900 MHz device for North America and parts of Latin America.
2. You can follow Nokia's advice and have two tri-band devices: A 900/1800/1900 MHz device for Europe, Asia, and parts of Latin America, and an 850/1900/1800 MHz device for North America and other parts of Latin America.
3. You can have a quad-band WorldPhone to give you coverage everywhere you go. The selection is rather slim at the moment: Two devices from NEC, three devices from Motorola, and one device from Palm/Handspring. If you assume you need a device that won't be confiscated because it contains a camera, you have one choice at present: The NEC 515.

Until there is a larger selection of camera-free quad-band devices, it seems to us that choice one is the most reasonable, followed by choice two. Choice two seems less reasonable in theory because you have redundant circuitry on each handset that will most likely never be used. In practice it may be more reasonable if those handsets have features you want, which are not available in the dual-band devices. In this case you simply pretend that the never-to-be-used frequency simply isn't there.

The important thing, however, is not what you need as a user, but the fact that the handset manufacturers – and the service providers – were caught so unawares by this transition. It is inexcusable that anyone would make a handset that might be used in Europe or Asia that does not contain both 900 MHz and 1800 MHz. It is inexcusable that anyone would make a handset that might be used in North America that does not contain both 850 MHz and 1900 MHz. We know of a lot of people who are holding out for a better selection of camera-free quad-band handsets, which means that sales that could and would be made now, when economic times are tough, are being deferred until the industry catches up to the reality of the quad-band GSM world created by AT&T Wireless and Cingular.

## 5. Real Stories from the Field — Checking ID

It is always difficult to convince people that protective measures need to be taken seriously. This can be an issue if no bad things happen for a very long time, and it can be an issue if the measures are not uniformly applied. If measures are applied to lower level employees, but not higher-level employees, it is a clear sign from management that the measures are for show, and not to be taken seriously.

Jack Sink of Payless Shoes wanted the people who checked ID at the doors to check everyone's ID but had a problem getting the guards to check the ID of those they knew. They would check the ID of strangers, but not that of executives or friends or those whom they recognized. Now, in most cases this is not really an issue, but there is some feeling in the trade that if protective measures are not taken seriously at the top, and are not applied evenly, it creates larger opportunities for bad things to happen.

The question, of course, is how do you convince those required to enforce policy that you are serious. It takes, after all, a brave guard to ask the chairman of the board for his ID each time he comes in.

Sink's approach was both novel and successful. At random intervals – perhaps once every week or two – he would pick some person whom he thought was a good candidate for being let through because they were known to the guards. He would give them a twenty-dollar bill. If the guard asked for the ID, the person would give them the twenty bucks.

Eventually the appropriate Pavlovian response became ingrained, and everyone, including Sink himself, was asked for ID each time they entered the facility.

Even-handedness has the additional benefit of being easily applied in a wide variety of circumstances. As an example, this author was recently changing planes in Chicago, and decided to get something to eat. At the next table was a couple in their 80s. The man ordered a beer to go with his meal, and the waitress asked for his ID. The patron, who had probably not been carded for well over half a century, was endlessly amused. But since it was obvious to all that *everyone* was carded, nobody of any age could complain, or feel discriminated-against, when asked for their ID.

## 6. Book and Product Reviews

*Phone Manager II* (for Nokia handsets)

Oxygen Software

€39 (1 handset), €59 (3), €89 (5), €1599 (100), €6995 (500)

<http://www.oxygensoftware.com/> +7-095-713-9582

Modern mobile phones are becoming more and more feature laden, and often have a degree of flexibility that is rather astonishing. Unfortunately, in many cases the features are either difficult to access, or inconvenient to access. Thus, some who don't need or want to carry a PDA may want to use their handset to remind them of a meeting, or to send a text message, but don't want to laboriously type on the handset's keypad. Many manufacturers of handsets have software available to access some or all of the features. Some, like Motorola's *Mobile Phone Tools* cost money, and some, like Nokia's *PC Suite*, are free. Free or paid, however, most of this software is somewhat limited.

For those of you who use Nokia devices, an alternative to Nokia's free software is Phone Manager II. This software does everything, as best we can see. We originally wanted it for three functional areas that we needed because we don't quite need a PDA.

The first was manipulating the phonebook. OPM2 allows us to put in a multitude of names, phone numbers, e-mail addresses, and notes for each entry, and move them from phone to SIM and phone to phone and profile to profile. The facility provided by OPM2 is richer than that provided by the free software from Nokia.

The second was manipulating the calendar. This can be done directly, or through import and export, and allows you to set, from your computer, meetings, calls, memos, and birthdays, along with the alarms and reoccurrences associated with them.

The third was sending text messages. We send and receive a LOT of text messages, and typing them into the handset would be tedious to an extreme, even with predictive text. Using our computer to type them in, and to respond to incoming messages, makes life much easier. While this facility is adequately presented in Nokia's software, the Oxygen software does not crash with the regularity of Nokia's freeware.

We additionally used OPM2 to make sure the profiles in our various domestic and international handsets behave the same way. We had a

problem here in that Nokia has changed the base ringtones, and we were missing two tones (City Bird and Going Up) on some of the handsets. Originally Nokia said that they were available on their web site (they aren't), then from AT&T Wireless (they aren't), then suggested I mail a letter to Finland to ask them. We finally found a vague approximation of one of the tones on a British web site and installed that, leaving only one missing tone.

Functions we haven't used included WAP- MMS- and GPRS-related features, and features related to access to Java applications and games as well as to the Gallery.

If you have a Nokia handset or handsets, and want to make more use of their potential, we strongly urge you to look at Phone Manager II.

*The Sourcebook to Public Record Information, 5<sup>th</sup> Edition*

ISBN#: 1-879792-72-9 1840 pages \$84.00

BRB Publications, Inc. 1-800-929-3811 <http://www.brbpub.com/>

If your organization has people doing public record research, you will be a hero if you make them aware of the 5<sup>th</sup> edition of this book, particularly since its only competitor, *The Guide to Background Investigations*, is no longer being published. The first 63 pages tell the reader a great deal about public records, and the remainder tells where and how to access those public records. Over the years, as subsequent editions have appeared, readers of AEGIS have been told that each edition is better than the previous. This is once again true. The maps are clearer, the information more comprehensive, and more online website addresses are published for speedier recovery of information and documents. At a scant \$84.00 it is a waste of time and money not to have a copy in every research office, public library, and professional library.

## **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](mailto:ejournal@lubrinco.com).

To subscribe to our AvantGo channel, go to [http://avantgo.com/channels/\\_add\\_channel.pl?cha\\_id=1773](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](mailto: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](mailto:ejournal@lubrinco.com).

If there is a topic that you would like to know more about, send it to [ejournal@lubrinco.com](mailto: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](mailto: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 March 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.