



**ÆGIS** e-journal

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

Volume 5 Number 5, May 2002

From the case files of

The LUBRINCO Group

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

and

Financial Examinations and Evaluations, Inc.

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

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

**This month's features:**

- 1. Due Diligence — Could Enron have been prevented?**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Who are the bad guys?**
- 3. Executive Protection — Who are the bad guys?**
- 4. Technical Issues — Killing magnetic media**
- 5. Real Stories from the Field — Who are the bad guys?**
- 6. Book and Product Reviews — 2002 Local Court and County Record Retrievers**
- 7. Free-Subscription/Unsubscription/Copyright Information**

## **1. Due Diligence — Could Enron have been prevented?**

As risk managers we deal with problems that run the gamut from access control to the complex mathematics of financial risk management, and, inevitably, someone had to ask us whether the collapse of Enron could have been prevented. The answer is no.

The reason for this is embarrassingly straightforward. There were three possible groups who could have prevented this. The first was management, which could have adopted better accounting practices. Unfortunately, once management has bought into the belief that the function of a corporation is to reward upper management, rather than to maximize the profit of the company's owners (i.e., the shareholders), it is unlikely that they will behave with total propriety. This is made worse by the group dynamic of peer pressure, where otherwise honest people will do things that in retrospect should not have been done.

The second group that might have stepped in was the independent auditors. However, the independent auditors made much more money from consulting than they did from the audit, and we suspect there was a great deal of internal pressure to preserve the revenue stream, rather than endanger it through petty propriety. In a word, they were not independent. While we like to think that these actions were atypical (other partners in the firm seem astonished that those involved would have done what they did), it remains to be seen whether the innocent will be punished along with the guilty.

The third group was Congress, in its role as regulator. In 2000, Arthur Levitt, then chairman of the Securities and Exchange Commission, proposed an SEC rule that would bar accountants from also acting as consultants, because he felt it created a conflict of interest. That proposal was rejected after 46 members of Congress called or wrote personal letters to Levitt questioning the proposed rule and some lawmakers reportedly threatened to withdraw funding from the SEC.

Why would they do this? We hate to appear cynical, but if you look at the contributions by the accounting industry to senators and representatives (see [http://www.opensecrets.org/news/accountants/accountants\\_senate.asp](http://www.opensecrets.org/news/accountants/accountants_senate.asp) and [http://www.opensecrets.org/news/accountants/accountants\\_house.asp](http://www.opensecrets.org/news/accountants/accountants_house.asp)), it is a lot of money. It doesn't take a big stretch of the imagination to think that a senator or representative who accepts no money from the accounting industry might have fewer issues in this area than a senator who has received \$482,453, or a representative who has received \$286,593.

Now, the question of influence is a tricky one. Some feel that contributions allow the political process to continue, and that they, the receivers of this contributed largesse, are not, in fact, obligated to the contributors. Not unlike the way some believe that violence on television and the movies has no effect on violence among viewers, while others believe that advertising inclines people to buy the things they see advertised.

No matter what your views of these issues, if you had any money sunk into Enron stock you probably wish that either management, or the auditors, or your elected representatives had behaved better / more prudently with your money.

Is Enron relatively unique? Clearly no. Arthur Anderson had the same problems with the Baptist Foundation of Arizona several years earlier when 750 million in assets was more like 125 million in assets because most of the assets booked by the Baptist Foundation were found to be substantially overvalued. Other companies to look at: Cendant, RiteAid, and Sunbeam.

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — Who are the bad guys?**

An increasingly significant part of our casework is in the area of OPSEC within the private sector. Left to their own devices, our clients tend to neglect and particularly misunderstand the area of operations security known as threat analysis, and, more specifically within it, the identification of specific adversaries. Clearly, in the government, where there are real spies, knowing who your enemy is of key importance, but how important is this to those of us in industry? Very, in fact, and for many of the same reasons!

The First Law of OPSEC (thanks to the DOE/NV) says that if you don't know the threat, how do you know what to protect? Although specific threats may vary from site to site or program to program, it is more important for employees to be aware of the universal actual and postulated threats . In any given situation, there is likely to be more than one adversary, and each may be interested in different information.

This is as true for industry as for government. You have many competitors and possible competitors. Each of them has a different interest in what you do. Each has different information they would like to have in order to further their goals. In addition, each of your competitors has a different corporate culture, and there are some that would not undertake illegal activities and some that would. In many industries you also have to be concerned about foreign governments that might be interested in stealing information about what you do, and have many fewer scruples than your industrial competitors.

Indeed, many governments will use all of their skills and technology to help acquire your technology for use by their domestic companies.

It is true that there are certain generic things that need to be done as part of the normal course of business. You need to be controlling access to your facilities. You need to be dealing with the kinds of disasters common to your industry and geography. You need to be protecting yourself from dishonest employees by doing pre-hiring background checks, and, in certain cases, continuing background checks. You need to be shredding documents that contain information of generic interest to your competitors. You need to be enforcing a policy of getting rid of old documents and information and data when it is no longer needed.

But these things primarily address what we might term generic incidents of opportunity, rather than specific threats. And, clearly, OPSEC will help you address these areas, which means that competitors who are serious about competitive intelligence, but not willing to cross the line to industrial espionage, will have been stopped.

But when it comes to specific threats from specific competitors, if you have not identified specific competitors who might – based on need, culture, and history – pose a specific threat, you are unlikely to be able to protect yourself from those who *are* willing to cross the line. Or at least to push it back a bit.

### **3. Executive Protection — Who are the bad guys?**

Most of our clients – indeed, most people, independent of their wealth, position, or celebrity – face relatively little risk in their lives other than that associated with normal living. By this we mean that all of us, rich and poor, famous and unknown, face the danger of accidents, traffic accidents, and health problems, but few of us face the danger of bad guys out to get us.

On the other hand, there are some clients – and some people – who indeed do face some generic special risk because of their wealth, position, or celebrity status. For these people, certain generic special precautions must be taken.

Within this group there is a smaller number of people who face a specific danger from a specific threat. These people require specific precautions to be put in place.

The big question is, how do you know when you have moved from the generic higher-risk group to the group where there is a specific threat? The answer is that you know through the gathering of intelligence regarding the

threat level you face. As we have noted in the past, this is important for two reasons. The first is that without a specific threat the IRS may consider precautions to be a taxable perk. The second, of course, is that without the appropriate intelligence you could end up dead or injured in some fashion.

Because of this, it is appropriate, when you reach a certain level of generic risk, to be paying someone to be your intelligence gathering department. This person (or persons) will be your intermediary with the police department, and any other appropriate source of information.

#### **4. Technical Issues — Killing magnetic media**

We are given to understand that the USPS is using devices to irradiate mail to destroy any pathogens that might be included in the mail. The high energy of these devices might erase magnetic media, expose film, and play havoc with flash memory as well as those devices that have any electronic circuitry.

The USPS and airport luggage screening companies are using MRI devices to look into packages and luggage. There is some indication that MRI will destroy all magnetic media, mess with flash memory such as EPROM, stick memory, and the like. It can also magnetize watches and other devices, altering their operation.

According the FAA and the Photographic and Image Manufacturing Association (PIMA) the CTXT and other high dose X-Ray systems will damage film of any speed. These devices are used to look into luggage and packages being checked or transported on aircraft.

In short, if this program is implemented, and these results hold true, you cannot ship via the post any magnetic media or flash memory items because of the high likelihood of damage. If you travel, all sensitive electronic gear must be carried on board and you must ask for a hand search if you have any questions about the devices your electronic gear may be passing through.

This also has implications for software sales of magnetic media delivered through the mail, and mail promotions using magnetic media, as well as the shipment of flash memory devices and similar EPROM devices.

#### **5. Real Stories from the Field — Who are the bad guys?**

It is always a good idea to check documentation, and birth certificates are a generally accepted form of documentation, especially for things like a passport, first driver's license and a few other key documents that follow us throughout our lives.

To make life interesting for all of us who rely on such documents for proof of identity, on April 9, 2002 someone stole 2,306 sheets of security paper, that can be used to create birth and death certificates, from the City and County of Denver Vital Records Office. In addition, they stole an electronic seal machine that produces an embossed seal of the City and County of Denver.

Two sizes of paper were stolen, one (9 3/4 inches by 7 inches) for birth certificates, preprinted with State of Colorado, Colorado Department of Public Health and Environment, Certified Abstract of Birth, and the name of Ronald S. Hyman, State Registrar. The control numbers (1851001-1853000) are printed in red ink in the seal on the left front side of the paper.

The other (8 by 11 inches), normally used for death certificates but also usable for birth certificates, is preprinted with the name of Franklin Judson, M.D., Local Registrar. The City and County of Denver seal is in the left front corner, and the control numbers (309695-310000) are printed in red ink above the seal.

The presence of these should cause some interesting problems over the next few years, unless they happen to be found before they go into circulation.

## **6. Book and Product Reviews**

### *2002 Local Court and County Record Retrievers*

BRB Publications, Inc., ISBN#: 1-879792-67-2 600 pages \$39.95

<http://www.brbpub.com/> 1-800-929-3811

BRB Publication is a long-standing publisher of good books on how find records and where to look for people and records. The 2002 edition is no different. If you are an investigator and you actually do work or may do work in areas other than your own little suburb, this book is a must.

How many times have you found yourself looking for a record on a person or a company that is literally in the middle of nowhere? Need documents from Bethel, Alaska? There is someone there ready to help you. Need someone for those records from Jim Hogg county Texas? There is someone there ready to help you. Need someone in Windsor County in Vermont to pull land ownership records and send you a photo of a house? There is someone there to help you. We have used the old book for all of these purposes in the last year.

Why is the book so important? For \$39.95 you aren't wasting hours looking for someone to help you in far away places. And you are finding local people who know the local rules and how to get the local rules to work in

their favor for you. After all, according to the locals in South Texas, a Texan is a neighbor, a Northerner is anyone north of a line between San Antonio and Houston, and a foreigner is anyone from outside Texas! Many don't like foreigners and won't answer their questions. But they'll help a fellow Texan.

## **7. Free-Subscription/Unsubscription/Copyright Information**

•• AEGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2002 by The LUBRINCO Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com) and L. Burke Files (LBFiles@lubrinco.com).

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

- **Protection of trade secrets and intellectual assets.**
  - Anti-economic espionage.
  - OPSEC: The identification and protection of information that would give your competitors and adversaries an advantage.
- **International financial investigations and due diligence consulting.**
  - Location and recovery of missing and hidden assets.
  - Establishing business relationships and strategic partnerships in Central and Eastern Europe, the offshore financial centers, Beijing and Shanghai, Central Asia, and Latin America and the Caribbean.
  - Anti-money laundering and financial fraud requirements under the *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2002* and the *EU Revised Money Laundering Directive of 2002*.
- **Protection of management, staff, and families.**
  - In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.
  - When traveling and living overseas.
  - When transporting items of substantial value.

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

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

To sign up for a **complimentary subscription** to *ÆGIS* e-journal or the *ÆGIS* e-journal PDF notification list, go to <http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to [ejournal@lubrinco.com](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 May 2002 *ÆGIS* e-journal (© 2002 LUBRINCO & FEE), to be found at <http://www.lubrinco.com/>.

*ÆGIS* e-journal is a forum for the exchange of information, ideas, operating styles, theories, and related topics for corporate managers who make

decisions about threats typically outside the expertise available in-house, yet which have the potential to affect their company's domestic and international bottom lines. Nothing appearing in *ÆGIS* e-journal should be construed as legal advice. The information provided is "general information," not "specific advice."

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

Please be safe, and be smart.