



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 6 Number 9, September 2003

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 September's features:

• **Special Announcement**

1. **Due Diligence — Picking up the pieces**
2. **OPSEC, Economic Espionage, and Competitive Intelligence —
The economics of economic espionage**
3. **Executive Protection — Increased police use of Tasers™**
4. **Technical Issues — Stealing your secrets: Cheap and easy...**
5. **Real Stories from the Field — Without trust there can be no betrayal**
6. **Book and Product Reviews — *Beyond Fear*
*Firetrust Benign***
7. **Free-Subscription/Unsubscription/Copyright Information**

**L. Burke Files will be speaking at the
OffshoreAlert 2nd Due Diligence & Asset Recovery Symposium
3-4 November 2003, The Biltmore Hotel, Coral Gables, Florida
<http://www.offshorebusiness.com/03intro.htm>**

1. Due Diligence — Picking up the pieces

In an excellent article in *Chief Executive Magazine* (<http://www.chiefexecutive.net/depts/management/190.htm>) entitled *Picking Up the Pieces: It takes a special breed of CEO to repair the damage caused by corporate implosion*, Erik Sherman discusses the issue of how a new CEO should deal with the problems of taking over a company whose former management appeared to be guilty of, er, creative accounting.

Mr. Sherman noted “Rather than try to ferret out the problems directly, the best approach according to L. Burke Files, vice-president of New York risk management consulting firm The LUBRINCO Group and an expert in forensic accounting and asset recovery, is to develop a standard for critically evaluating the past. “You have to take a baseline assumption of what should have been going on and then test it against what was going on,” he says.”

While this is true as far as it goes, we would like to expand on this and say that the job of the new CEO is in reality tri-fold.

The first is to run the company, to make sure it survives and is profitable. In this respect, the job of the new CEO is not unlike that of any other CEO.

The second is to assure that whatever went wrong under the former administration is discovered. However, discovering what went wrong is not the job of the new CEO, largely because the *office*, and not just its former occupant, is under a cloud, and it is never appropriate for suspects – even retrospective suspects – to officially investigate their own potential crimes. While the new CEO has to ensure that it gets done, and must stay involved to ensure that what was wrong is eliminated and has no lingering effects, the job of figuring out what went wrong (and who done it) should be handed over to some *independent* group. He, not the independent group, will of course be the conduit to the outside world for the information discovered.

The third is to be the decision maker – or at least the one who makes the recommendations to the board – about what should be done with the information that is uncovered. The first instinct is to try to go after the bad guys once they are identified, but remember that the money may be, in fact, gone. If the Feds are pursuing a criminal case and there is money that can be

recovered, then it is wise to engage asset location specialists as early as possible to ensure that any leads are followed up on promptly. The Feds are interested only in prosecution, not in recovery of assets and the longer the time between the crime and the initiation of a search, the less the chances of recovery. However, if there is no money to be recovered, then the case should be carefully explained to the board, the shareholders, the employees, and the analysts, and a decision should be made to move forward to a profitable future, and leave the past to the Feds.

It is important to keep in mind that while theft on the part of those in charge is hard to stop if they have the inclination to steal and the cooperation of those in charge (including, in some cases we have seen, the active failure of legislators in restricting auditing abuses), it is still rare that the losses will bankrupt a major company. (One estimate is that in a successful company run by a greedy CEO, the figure approaches 10% of the operating budget.) Nonetheless, it is important for boards of directors to decide how much greed they will tolerate, and then to put into place and enforce audit measures designed to detect and put a stop to actions that might constitute a betrayal of the shareholders and employees.

2. OPSEC, Economic Espionage, and Competitive Intelligence — The economics of economic espionage

Imagine for a moment that your company is developing a new product, and that the development effort will cost fifty million dollars. Then imagine that you have competitors overseas who would have to pay a similar sum to develop a similar product.

Now imagine that these competitors are disinclined to spend fifty million dollars on the development effort, but they *are* willing to spend a million dollars to steal the information you developed, plus another million to implement it and beat you to market.

How can a million bucks be enough to get development information worth fifty million? Through a relatively low-cost espionage operation that begins with determining which of their potential victims is likely to be doing development in their field of choice. They can then find out who is working on the precise project that includes that information. At that point, how they get the information is immaterial as long as they get the information they need.

What are the possibilities? Multiple, unfortunately for you:

- They can hack your computer system.

- Even better, they can suborn someone on your computer staff, or get someone to get a job on your computer staff, and have them steal the information for them.
- If you have telecommuters working for you with access to sensitive information, or employees who take their work home with them, they can monitor them, get into their homes and steal the information from their laptops.
- They can use bribery. Oddly, most people who betray their employers – or their countries, for that matter – sometimes do it for surprisingly small amounts. You may think that millions of dollars of stolen information might cost them millions of dollars, or at least hundreds of thousands of dollars, but it will more likely only cost them in the tens of thousands.
- They can use blackmail.
- They can use deception operations (E.G. Have an employee meet a beautiful woman or handsome man, and, over a period of time fall in love and persuade the new love to steal the information, or steal information from them without their knowledge.)
- They can move someone in next door, have them become trusted friends, then they can steal the information.
- They can put someone on the cleaning staff that can bug offices, steal information, and put key loggers on computers to send out information of interest.
- They can get someone hired on the staff of the facility that stores your emergency backup system and steal the backup information.
- They can put someone on the staff of a supplier who has access to your information, but is less rigorously checked or monitored, and whose systems are less secure.
- They can rob your people at gunpoint.

Some of the above scenarios are, we admit, less likely than others. Depending on the value of the development, however, in some cases murder might not be far-fetched. Clearly, not everyone can be corrupted. (We can't, but the consensus opinion among the single men in the company is that if you want to try, you should please try it via seduction.) But almost anyone can be robbed. And absolutely *everyone* lets their guard down or makes a mistake

from time to time. If someone is spending a lot of time and money to be there to take advantage of that mistake, you may – you will! – have a problem.

The good news is that proper preparation can help you can avoid many of the risks of economic espionage (much of our work is helping companies do just that). And if you can't avoid it entirely, you can anticipate the possibility (and try to detect it) and take some damage-limiting steps.

Being a victim of economic espionage is partly a matter of choice. The bad news is that many companies choose not to spend the time and money needed to protect themselves.

We like to think the regular readers of the *ÆGIS* e-journal are a cut above average, and that you have chosen – or will choose – the path of prudence, and will let some other less-than-prudent company be the victim of economic espionage.

3. Executive Protection — Increased police use of Tasers™

We read an article an article entitled *Police seek ways to avoid firing guns* in a recent issue of the Mercury News. The article discussed increased use of – and need for – Tasers™ and other alternative emergency safety tools. This is of interest to those responsible for your protection, as neither you nor they want to shoot anybody. The Taser™ is an excellent tool, but not generally available within the private sector, so we note with relief that much of the interest in new police emergency safety tools has come about as a result of the increasing failure-to-control rates associated with use of pepper-sprays, or ASRs (Aerosol Subject Restraints), as they are more technically termed.

When we first introduced ASRs at the 1988 conference of the American Society of Law Enforcement Trainers, the spray was an alcohol-based misting product that contained one tenth of one percent capsaicin, and had a near-zero failure-to-control rate in the hands of trained users. (We introduced the first official training program for line officers at the 1989 ASLET conference.) The FBI subsequently recommended upping the percentage to one half of one percent capsaicin, noting that this seemed to eliminate some of the rare failures without increasing the recovery time, and that anything more powerful than that caused needless pain. (I recall the term used in conversation was “cruel and unusual punishment.”)

ASRs had a number of advantages over teargas. First, they worked by inflaming the mucosa of the trachea when the mist was inhaled, rather than by causing pain, so they would work on pain-resistant subjects. Second, they would work at very close distances, which was important because most

police confrontations start at about four feet (field interrogation distance) and then move closer. Third, because they were dispensed as a mist, it was much easier to hit the target than with the narrow stream typically associated with teargas, and the mist avoided the theoretical potential for eye injuries from the stream.

Although we have not been involved with the sale of ASRs for over a decade, and have had no financial interest in any of them, we have kept a paternal eye on ASRs. Several things have happened. First, manufacturers introduced burst and stream units so that they could be used at greater distances. While confrontations still begin at field interrogation distance and move closer, the dispensers no longer mist, and the products are no longer inhaled.

Since the majority of ASRs are now stream and burst units, there was a move away from alcohol (in which capsaicin is extremely soluble, which aerosols easily, and which converted the oleoresin capsicum to an ester, which some felt seemingly made it more effective) as a misting carrier compared to nonflammable (and non-misting) carriers such as water and methylene chloride. The increased failure-to-control rates associated with burst and stream units induced manufacturers to increase the concentration of capsaicin more and more, with products now commonly having moved (from the original range of one-tenth to one half of one percent) to between a full percent to a percent and a half!

We have therefore seen ASRs go from a near-zero failure-to-control rate to, in some reports, a failure-to-control rate approaching seventy percent! We are not surprised that agencies are looking at new alternatives.

4. Technical Issues — Stealing your secrets: Cheap and easy...

In many large companies roughly 70% of the value of the company lies in its intellectual property. (One of the reasons there is all this talk about “knowledge management!)) This is a *very* significant percentage, and makes a tempting target for the unscrupulous competitor. According to estimates in the *2002 Annual Report to Congress on Foreign Economic Collection and Industrial Espionage*, the cost to American companies of foreign and domestic economic espionage and theft of intellectual property is \$300 billion dollars a year and rising. The average cost per incident is \$500,000 in non-manufacturing companies, and a whopping \$50 million per incident for manufacturing companies!

Who threatens this intellectual property? About 80% of the time it is insiders. By insiders we mean employees, temporary staff, contractors,

vendors, suppliers, consultants, government agents, business partners, accountants, attorneys, security guards, OEM manufacturers, visitors, and a host of others, plus their associates, friends, and family.

How high is the threat? It depends on the company. Putting aside outside issues like competitors or foreign government interest, if your company is in any sort of crisis (in which we include mergers, real or rumored, layoffs or anticipated layoffs, large stock price fluctuations or any other financial situation that might endanger jobs), then the threat is high because all the insiders are not at their highest level of comfort and loyalty. This is particularly true in companies where the insecure insiders (or their friends, family, and associates) perceive that senior management has exceeded the traditional limit of 10% of the operating budget on themselves. Add the high mobility of employees today — no longer do we work at the same company for 25-30 years — and the risk is further multiplied.

What are you doing about reducing the risks? We will ignore the things you are probably not doing, i.e. an inventory of sensitive information (the average company has never done an inventory of sensitive information, and if they have, it is almost certainly not current). Nor will we make any mention of adequate document control, and a host of other simple procedures needed to assure the safety of their information. And we'll overlook the fact that most companies have never trained their employees on what sensitive data is, how to protect it, from whom to protect it, how to tell if someone is trying to steal it, and what to do if there is a suspicion of theft.

Rather than dwell on these negative aspects, we will merely note that 80% of your security budget is most probably spent on physical security and access control, which is to say keeping the 20% out, rather than dealing with the 80% who are already in. Since most of the risk arises from people you willingly let in, and since much of the illegal activity takes place outside the company walls, most security efforts are, in short, misdirected.

Thus theft of your sensitive information is easy and cheap because it is inadequately protected. We certainly do not advocate getting rid of your alarm systems and guard forces, but we do heartily recommend a reevaluation of your security priorities and expenditures. After all, at \$500,000 per non-manufacturing incident to \$50 million per manufacturing incident, it is a small step to take toward preserving your financial future.

5. Real Stories from the Field — Without trust there can be no betrayal

Some time ago we had the chance to speak with a man who for many years had shared an office with Robert Hanson, the FBI agent who gave secrets to the Russians. I asked him how he felt about having shared so much of his life with this man, and whether he felt, for lack of a better word, silly about not having realized Hanson was a spy.

He said that no, he didn't. From his perspective there were two Bob Hansons. There was the good Bob Hanson that he knew and liked, who would have never done such a thing, and there was the bad Bob Hanson that he didn't know, who did these things.

The point here is that for many in business there is a good chance that you will end up knowing, even if only in passing, someone who is stealing company secrets. An annual cost to American companies of \$300 billion is a clue that there is a lot of theft going on, and it would be more surprising if your company *weren't* a victim, and if you never met someone who was a thief. If you are a reader of this Journal you might well be the person who hired the thief. Should you feel betrayed when this happens? Obviously!

Should you feel foolish? If you have taken prudent measures to prevent information theft, then no. You have probably stopped others.

If the FBI and the CIA, who are way more paranoid than are you, can't completely stop theft of information, there is no reason to believe that you should be able to. However, you should be able to prevent much of it, and to detect most of the rest of it. But business – life – depends largely on trust. And while there can be no betrayal without trust, that is not reason to abandon trust, just as trust is not a reason to abandon prudence.

6. Book and Product Reviews

Beyond Fear

Bruce Schneier

Copernicus Books ISBN: 0-387-02620-7 295 pages \$25.00

<http://www.copernicusbooks.com/> 1-212-228-0175

The big frustration for security professionals when dealing with security issues is that most people – including those making security decisions at all levels of our society, starting with the President of the United States and working down – simply don't get it. What they mostly don't get is that all security policies and all security decisions involve tradeoffs, that all security

policies and all security decisions address agendas not problems, and that many security policies and measures are made for others by people whose agendas may differ radically from the agendas of the people on whose behalf they are making the decisions.

Bruce Schneier gets it, and this shows clearly in his new book. If you could only read one book about security, the book you should read is *Beyond Fear*.

On a pragmatic level, *Beyond Fear* gives you a set of tools to evaluate any given security policy or measure (actually, these can be used to judge any social policy of measure):

1. What assets are you trying to protect?
2. What are the risks to these assets?
3. How well does the security solution mitigate these risks?
4. What other risks does the security solution cause?
5. What tradeoffs does the security solution require?

As all of us have seen in the last few years, security decisions are rarely straightforward. As an example, many spend a good deal of time criticizing airport security measures, few of which address airport security issues. However, if you realize that the purpose – the agenda – was not to increase airport security, but to make you feel comfortable about flying so that the airline infrastructure didn't collapse, it all makes sense. It is security as theater, not security as protection. Is it worth it? That depends on your agenda, and Schneier deals with this issue.

The author emphasizes the importance agendas and tradeoffs. For example, which better – and for whom?

- a. To spend \$60 billion making us feel better about flying, the inconvenience of which will cause a large number of people to drive rather than fly, which in turn will mean that the actual number of travel deaths will go up because of the security measures.
- b. To spend \$60 billion on intelligence gathering to have information that might allow us to prevent terrorist attacks.
- c. To spend \$60 billion on finding a cure for cancer or malaria or some other disease.

The “better” decision depends very much on who you are.

Beyond Fear also considers the philosophical nuts and bolts of security. How do systems interact and fail? Are you better off having multiple levels

of systems? Should you protect against things that don't matter? How do detection, protection, and response all work together to increase security? What are the differences among the three distinct concepts (which seem to puzzle so many) of identification, authentication, and authorization?

If you are involved in making decisions about security policy (something which is rarely entrusted to security people), this book will help put you in a position to understand what is actually involved, and to make sure your decisions are designed to meet some determined need – hopefully actually addressing some risk in a reasonable manner – rather than throwing money blindly, with the feeling that security is a needless cost which adds nothing to the bottom line.

Benign

Firetrust \$34.95

<http://www.firetrust.com/products/benign/>

When we get e-mail we face a number of problems. One, of course, is spam, which we deal with using MailWasher from Firetrust. The other is people putting bad things into their e-mail messages, like viruses and worms, which we deal with by using anti-virus software, which we update regularly.

There is, however, a whole set of other objects, some dangerous and some not, that come wafting their way to us via e-mail, and of which many are unaware. These include web bugs, malicious html, scripts, and in some cases as-yet unknown viruses and worms. We deal with these threats and potential by using *Benign*, also from Firetrust, the MailWasher people.

Benign stands between your ISP's POP3 server and your e-mail client. More technically, according to the good folks at Firetrust, if *Benign* is the only incoming mail scanner then *Benign* will come first, then your e-mail client, and then your antivirus program. If *Benign* is not the only incoming mail scanner (i.e., your anti-virus software scans incoming e-mail) then normally the antivirus mail scanner will come first, then *Benign*, then a second scan by the anti-virus mail scanner (if the mail client is connecting to *Benign* using the default port 110), then the e-mail will arrive at the e-mail client.

Benign looks at the incoming e-mail and recognizes odd or undesirable HTML code and strips it out. It takes out 1x1 images, which are often web bugs that send back a message saying you are a valid e-mail address. It renames or blocks scripts and executable code. What you are left with is your e-mail, stripped of dangerous attachments and potential problems.

How many potentially bad things are you likely to have? Today we had 38 e-mails come to our machine, of which 22 were filtered. This filtering included renaming 14 attachments, removing 194 non-standard HTML tags, removing 102 scripting tags and attributes, and blocking 2 web bugs. Were all of these serious threats? No. Is there any reason for us to have received them? No.

Once installed, the operation of Benign is transparent to the user. Installation is trivial, and, if you are lucky, will be automatic. If you are less lucky, you will have to manually configure your e-mail client according to the simple instructions given for the listing of e-mail clients. For other issues, there is a Firetrust user group at <http://www.computercops.biz/forums.html>.

We had two other minor problems. The first is that the installation program writes to the Windows *hosts* file, which on our machine was marked read only by *Spybot* (discussed in the July 2003 e-Journal) to protect it from hijackers. To deal with this, you can temporarily unselect this option in *Spybot*, or you find the *hosts* file (on our machine it is in C:\WINNT\system32\drivers\etc), click on the file with the right (as opposed to left) mouse button, and un-check the read only box. Reset it after the installation. Problem solved!

The other problem was that the installation made port 110 visible to the outside world (you can test this by running a port scan using Steve Gibson's *Shields Up!* program at <https://grc.com/>). In theory this is not a big deal, as the port will reject any attempts to use it, but we personally feel more comfortable with the port simply being invisible, and thus not tempting hackers. Fortunately, this is just a matter of tweaking your firewall. (We say this very casually, but, *entre nous*, it took the helpful ZoneAlarm experts at their technical forum at <http://forums.zonelabs.com/zonelabs> to figure out how to do this.) In the case of ZoneAlarm Pro 4, the firewall we use, it *appears* that all you do is put in an *expert rule* for Benign by opening ZAP4, selecting Program Control, clicking on Firetrust Benign, selecting Options/Expert Rules, clicking on Add, then filling in the boxes with:

Name: POP3 server

Rank: 1

Action: Allow

Source: My Computer

Destination: The IP address of your POP3 server from your ISP

Protocol: POP3

Figuring out the mechanics of entering a program expert rule in ZoneAlarm – and entering it – takes about five minutes. This small effort makes

everything work, and, *milagro!*, port 110 is hidden! We are given to understand that the process is similarly trivial with other firewalls.

We strongly recommend Benign for your consideration.

7. Free-Subscription/Unsubscription/Copyright Information

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

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

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

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

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

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

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

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

Please be safe, and be smart.