

# **ÆGIS**



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

Volume 9 Number 2, February 2006

From the case files of

**LUBRINCO**

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

and

**FE&E** CLARITY FROM COMPLEXITY  
Financial Examinations & Evaluations, Inc.

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

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

**This month's features:**

- 1. Asset Location and Due Diligence — Cashing in on the glass ceiling**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Internet losses**
- 3. Executive Protection — Carrying costs**
- 4. Technical Issues — Toner expiration games**
- 5. Real Stories from the Field — The case of the missing sniffles**
- 6. Book and Product Reviews — Spyware Doctor 3.5**
- 7. Subscription/Unsubscription/Copyright Information**

## **1. Asset Location and Due Diligence — Cashing in on the glass ceiling**

One of the nice things about holiday parties and bars is that in both one has the opportunity to eavesdrop on conversations, and learn things you would not be told directly. We recently overheard a conversation about a pending lawsuit by several women claiming that they were the victims of their company's glass ceiling.

The consensus opinion of the participants to whom we were listening was that the women involved had already risen to their level of incompetence, and that they would surely win the suit.

The reason for this was that while, in the view of those men and women discussing the case, the women suing did not deserve promotion (and possibly did not merit the jobs they currently held), the company had virtually no high-level female executives. This means that while the claimants themselves had not been hindered by a glass ceiling, other women, more competent than they, surely had been and would be.

Putting aside the women actually filing suit, and the women who *should* have been filing suit, the company will suffer in several ways.

First, the company will lose a substantial amount of money. The consensus was that if the plaintiffs hired a team of dancing monkeys as counsel, the monkeys would be able to win the suit just on the executive gender makeup of the company, and the virtual non-existence of women senior managers.

Second, some competent people, men and women, had already chosen other opportunities in other companies, rather at than the company being sued.

Third, it was likely that they would lose some customers over the allegations.

It is likely that the claimants will be bought off with either money or promotions. Since they were not particularly competent in their current positions, it is likely that they will make disastrous senior managers. And if they go somewhere else – though they will probably win enough so that they will never have to work again – some other company will be stuck with more bad managers.

While we can't vouch for the accuracy of what we overheard, the lesson to be learned is clear: You, as a senior manager, should be making sure that your management team is based on merit, rather than sex or color or religion, so that you can avoid needles lawsuits. Even more important, you will otherwise waste the talent of half the gene pool.

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — Internet losses**

A report released by the National Counterintelligence Center (NACIC) indicates that the Internet is the fastest growing method used by foreign entities to gather intelligence about U.S. companies. While the report was *largely* concerned with questions about defense-related technology, it was not *exclusively* concerned with defense-related areas. Plus, your CI group (we assume you have one), and the CI groups of your adversaries (some of whom *certainly* have them), largely uses the same techniques as are used by spies to gather 95 percent of the information they need, so you need to pay attention.

What does this mean to your company? It means that if you have an Internet presence you are adding to your potential risk. As always, there needs to be some balance between your ego and marketing needs, and the need to protect your information. It means that there is a need for someone in your corporate OPSEC program to be making sure that information being released is not doing more harm than good.

Since OPSEC is most widely used within the government, horror stories are generally most available from this venue. One of our favorites was a military base that had their own Web site. Now, there is always some question as to why the military needs a Web site. It is, after all, unlikely that someone might have a war, and would not know with whom to start it if they could not find a DOD Web site...

In this particular case there was a map of the base. As you moved the cursor over the map, the latitude and longitude would be displayed. This would, of course, be a great convenience for someone wanting to bomb the base. Fortunately, nobody seemed inclined to do so, and nothing bad happened before that feature was removed.

While this is an extreme case, the fact remains that if your corporate OPSEC practitioners are being excluded, the Internet – your Web site, and the information you give out in response to Internet queries – is probably needlessly costing you money in lost intellectual property.

The moral of this is to make sure that your OPSEC team is not being hindered from looking at your Internet presence. This will make sure that your SOX reporting will not disclose embarrassingly preventable losses.

### **3. Executive Protection — Carrying costs**

While we ourselves do not carry guns, the nature of that portion of our business that deals with protective services in high-threat environments means that some of the people who work for us must.

In truth, most people who carry guns at our behest will never need to use them to protect themselves or our clients, because their job – our job – is to try to make sure that we avoid situations where use of guns is necessary. But it is equally true that if we fail in preventing this from happening, and they are in a situation where they need to use a gun to defend themselves and our clients, there will be no other emergency safety tool that can be used in place of a gun.

While this is a necessity that cannot be avoided – our clients sometimes work in dangerous places, where very bad people want to do very bad things to them – one of the things of which we are always mindful is the balance between the risks of carrying a gun and the risks of not carrying a gun.

The risks involved in carrying a gun do not relate to gun accidents: They are so rare that they do not constitute a major concern in the trade. Rather, the risks are legal and financial.

One of our people recently attended a training course in Massachusetts on carrying a gun in that state. Since what happens in Boston is not dissimilar to what happens in New York or Phoenix or Los Angeles, it was interesting to note that the presenter felt if you shot someone, and the shooting was justified, your legal defense is likely to cost you hundreds of thousands of dollars. This is in line with the general industry belief that the legal costs in a completely justified shooting will be a minimum of \$40,000, and could be up to half a million dollars.

We can't vouch for the accuracy of these figures, but we do accept that if you are forced shoot and kill someone you are likely to end up impoverished by the legal system. Even assuming you are not jailed, you are also likely to end up divorced, jobless, and suffering a variety of psychological ills.

The bottom line is that if you keep or carry a gun for protection, you should be as mindful as we are of the potential costs involved. While we have heard people casually say things like “Better to be judged by twelve than carried by six,” if there is any reasonable alternative to taking the life of another person, you should exercise that alternative, and avoid the whole issue.

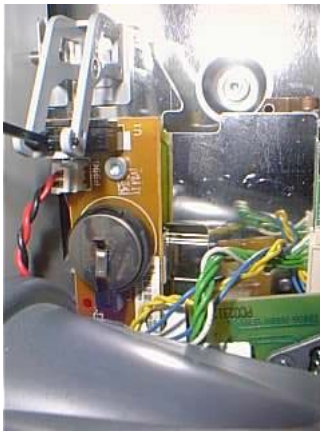
#### 4. Technical Issues — Toner expiration games

We recently got a call from an irate friend who had bought a case of toner cartridges for the HP OfficeJet printer that he used in his home office. At the time, this seemed like a good idea, because it saved him a substantial amount on each cartridge. Unfortunately, this evening he had tried to make a print, and the printer gave him a message that the toner cartridge had expired.

At first he thought this meant he was out of toner, which seemed unlikely, but possible, so he changed the cartridge. That gave the same message, and a little searching on the Internet revealed that cartridges for this printer had an imbedded chip to track their age, and to not let them be used when, like a bottle of milk, they had expired. This meant that he was now sitting on what was, for him, a very expensive case of unusable cartridges.

A further search indicated a general consensus that there was nothing that could be done, other than buy a new cartridge. Only one, of course, because it was the desire to save money by buying many, rather than pay single unit price, that had gotten him in trouble in the first place.

Fortunately, further investigation turned up a helpful article at <http://www.land.netonecom.net/tlp/ref/letters/hpPrinters.php> (on a Web site called The Lawful Path, with which we were not familiar) which said that one merely had to remove the battery that kept the CMOS alive in the d125xi printer, let it sit for about an hour (presumably to let the CMOS capacitor drain), then put back the battery.



If you look at the attached picture, you can see the battery. It is, according to the article, difficult to find and reach, but worth the effort if the alternative is to have to replace perfectly good toner.

Now, it may well be that this kill-on-expiration feature has a benefit, in that it prevents you from using ink which will clog the print heads, either because the ink has curdled, or because you are using refills that are not assembled in clean rooms, and have greater potential to clog the print heads.

Nonetheless, it appears that a lot of people would prefer to regularly spend less on toner, and risk having to occasionally replace the print heads.

## **5. Real Stories from the Field — The case of the missing sniffles**

One of our editors tends to get sick in the winter, and yet, this winter, he has not had so much as the sniffles. We asked what he thought was responsible, and whether he is doing anything differently this year.

Most of what he is doing is the same as what he has done in the past. He washes his hands frequently (a trick any school teacher knows), uses a protective agent, Dermashield (<http://www.dermashieldusa.com/>), and tries to avoid being around sick people. He has also, at the recommendation of a friend, been taking colostrum (<http://www.symbiotics.com/>, and bought at <http://www.vitacost.com/SymbioticsNewLifeColostrumPLUS/>). Colostrum, better known as mothers' milk, has a positive effect of the immune system of babies. Indeed, the colostrum FAQ from La Leche League at <http://www.lalecheleague.org/FAQ/colostrum.html> says:

“Colostrum actually works as a natural and 100% safe vaccine. It contains large quantities of an antibody called secretory immunoglobulin A (IgA) which is a new substance to the newborn. Before your baby was born, he received the benefit of another antibody, called IgG, through your placenta. IgG worked through the baby's circulatory system, but IgA protects the baby in the places most likely to come under attack from germs, namely the mucous membranes in the throat, lungs, and intestines.

Colostrum has an especially important role to play in the baby's gastrointestinal tract. A newborn's intestines are very permeable. Colostrum seals the holes by “painting” the gastrointestinal tract with a barrier which mostly prevents foreign substances from penetrating and possibly sensitizing a baby to foods the mother has eaten.

Colostrum also contains high concentrations of leukocytes, protective white cells which can destroy disease-causing bacteria and viruses.”

Since most of us don't have a ready supply of lactating mothers, the colostrum used is from cows. According to <http://www.colostruminfo.com/>, “Bovine (cow) colostrum is nearly identical to human colostrum but research confirms it is four times richer in immune factors than human colostrum.”

While we can't vouch for the efficacy of mothers' milk with adults, nor that it is the mothers' milk that has been keeping him healthy, the idea has a certain charm to it, and might be worth your examination.

## 6. Book and Product Reviews

*Spyware Doctor 3.5*

PC Tools Software

\$29.95

<http://www.pctools.com/spyware-doctor/> 1-800-406-4966

In the January issue of *ÆGIS* we mentioned the malware that Sony-BMG installed on computers that played certain of their CDs. One of the interesting things about it was that anti-spyware and anti-virus software did not seem to address this issue.

However, when we recently did an update of our anti-spyware software, *Spyware Doctor*, we noticed that the description said. “\* New! Real-time protection against rootkits, using kernel technology the updated Process Guard protects your system from hidden processes attempting to monitor or compromise your PC.”

The Sony-BMG malware used a rootkit that changed the computer (Sony-BMG is a large corporation, and can afford to write state of the art malware), so we wrote asking if *Spyware Doctor* would prevent the installation of this rootkit? PC Tools responded, “To answer your question - yes *Spyware Doctor* does remove the Sony BMG malware.”

Good anti-spyware such as *Spyware Doctor* works in three ways. It immunizes your system against certain hacks (like Active-X exploits) that can be prevented in advance. It runs in background to detect certain kinds of real-time exploits, and block them. It allows a scan to detect any known malware, and remove whatever is found.

*Spyware Doctor* has extremely frequent updates, and allows you to schedule automatic updates and automatic scans. We do an automatic update every morning at 0255, and automatically run a full scan at 0300.

Malware is no longer merely the destructive activity of misguided kids. It has become a big business. In the Sony-BMG case it was supposed to prevent copyright violation, with the inclusion of exploitable vulnerabilities merely an unfortunate side effect. In other cases it is built to be sold or leased to others for some specific business purpose.

With the proliferation of malware, and the entry of criminal organizations and sophisticated corporations into the malware business, *Spyware Doctor* is well worth your consideration.

## 7. Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2006 by The **LUBRINCO** Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com) and L. Burke Files (LBFiles@feeinc.com).

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

- **Corporate counterintelligence.**

1. American businesses lose \$300 billion annually to competitive intelligence, economic espionage, and information theft.
2. Sarbanes-Oxley requires internal controls tracking the costs, and impact on valuation, of competitive intelligence, economic espionage, and information theft.
  - LUBRINCO provides private sector access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information from competitive intelligence, economic espionage, and information theft.

- **International asset location and due diligence.**

- Location of concealed assets in fraud, theft, and divorce.
- Due diligence to prevent fraud and loss in China, Central and Eastern Europe, Central Asia, the offshore financial centers, Latin America, the Caribbean.
- Financial fraud and anti-money laundering program development and training for compliance with the US *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001* and the EU *Revised Money Laundering Directive of 2001*.

- **Protection of management, staff, and families.**

- In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.
- When traveling and living overseas.
- When transporting items of substantial value.

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

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

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

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

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

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

If there is a topic that you would like to know more about, send it to [aegis@lubrinco.com](mailto:aegis@lubrinco.com) and the editors will consider it as the topic for an article in an upcoming issue.

If you would like to submit an article for publication in **ÆGIS**, send it as an attachment to an e-mail to [aegis@lubrinco.com](mailto:aegis@lubrinco.com). Submission of an article certifies that (a) all information in the article is in the public record, or (b) that you are authorized to release any personal or corporate proprietary information contained in the article, and (c) that none of the article has previously been copyrighted. The submission of materials for publication in **ÆGIS** constitutes a license to **LUBRINCO**, and/or Financial Examinations and Evaluations, Inc, their assigns, associates, or affiliates, to abridge and/or edit said submission, and to copyright and publish/republish any submitted materials in whatever written and/or electronic form they may choose.

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

*Article Title*, from the February 2006 **ÆGIS** (© 2006 **LUBRINCO** & FEE), to be found at <http://www.lubrinco.com/>.

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

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

Please be safe, and be smart.