

# **ÆGIS**



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

Volume 8 Number 10, October 2005

From the case files of

**LUBRINCO**

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

and



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

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

**This month's features:**

- **Special Announcement**

1. **Asset Location and Due Diligence — Be Prepared....**
2. **OPSEC, Economic Espionage, and Competitive Intelligence — Coming soon to your company: A class action lawsuit**
3. **Executive Protection — Do you know your roads?**
4. **Technical Issues — Pretty Good Privacy**
5. **Real Stories from the Field — Unintended consequences: How Sony and Universal will force you to make bootleg DVD movies**
6. **Book and Product Reviews — SpyFinder**
7. **Subscription/Unsubscription/Copyright Information**

L. Burke Files will be presenting a two day seminar on *Employee Fraud* Queretaro, Qro. Mexico October 6&7 for IPACITEFO <http://www.ipacitefo.com/>

L. Burke Files will be presenting a one day workshop on *Fraud Prevention for Corporate Treasury Professionals* at the Association for Financial Professionals annual conference in San Antonio, Texas, on October 9th. [http://www.afponline.org/pub/conf/annual\\_conference.html](http://www.afponline.org/pub/conf/annual_conference.html)

## 1. Asset Location and Due Diligence — Be Prepared

We have often said in these pages that if you are prepared for natural disaster you will be prepared for almost any other threat to your corporate existence. The corollary, of course, is that if you are not prepared for natural disaster you will not be prepared for anything else, either. We are personally relieved and pleased – and as a country fortunate – that the loss of human life in hurricane Katrina was significantly lower than had been forecast by some experts (<http://americanradioworks.publicradio.org/features/wetlands/hurricane1.html>), although ashamed that such a large number of the dead were the elderly, un-evacuated from nursing homes, where they waited, vainly, to be rescued.

The affect on businesses, however, has been right on target.

It had been estimated that there was a 1 in 6 chance of a Category 5 hurricane hitting New Orleans in this 1995 to 2015/25 high-intensity hurricane cycle. While 1 in 6 is high enough that businesses needed to give it very serious consideration, the implications were largely ignored, in spite of the LSU *Hurricane Pam* study of the potential for New Orleans of a category 3 hurricane ([http://hurricane.lsu.edu/floodprediction/PAM\\_Exercise04/](http://hurricane.lsu.edu/floodprediction/PAM_Exercise04/)). A small number of corporations learned the lessons of the World Trade Center, recognized that New Orleans had serious potential hurricane problems, and made appropriate backup plans. Most others did not. For those companies that were prepared, the hurricane was a survivable corporate disruptive event, although still a major trauma in terms of personal tragedy. For those that were not prepared, Katrina put them out of business, in many cases forever.

In some cases plans were doubtless made, and failed. Whenever a plan fails, it is important to go back and find out whether the problem was a flaw in the plan itself, or whether there was a systemic problem.

Systemic problems are interesting, because they generally bring us back to our mantra for evaluating policies and measures by asking five questions:

1. What problem is the policy or measure trying to solve?
2. How can it fail in practice?
3. Given the failure modes, how well does it solve the problem?

4. What are the costs, both financial and social, associated with it, and flowing from its unintended consequences?
5. Given the effectiveness and costs, is the policy or measure worth it?

In our experience, systemic problems come with the first question: The problem being addressed is not the problem we *think* is being addressed.

Often, both in private industry and in government, policies and measures that should address some specific issue in reality address the problem of building headcount and budget. We recall proposing a more efficient solution to a problem and being told that if our advice were followed, rather than having 600 people in his group, making him a senior member of the management team, our prospect would have 40 people doing the same work and be a division leader. You should not, for much the same reason, expect anyone at TSA to suggest letting America's 663,535 sworn officers carry their weapons on planes as a substitute for the Air Marshals program.

In other cases, a measure may be put in place because it will reduce insurance costs, or because it will reduce liability, or because it will give the perception of activity (i.e., it is being done largely for PR purposes). Since in all these cases the measures are designed to give the appearance of addressing a problem, rather than to actually address the problem, don't count on them being effective. This is especially true if the problems being addressed are statistically unlikely events, where the incidents planned-against will virtually never happen.

We see systemic problems when we do crisis management drills. We will be told that a company has, in fact, a crisis management plan. Nobody, however, has ever seen the plan, nobody knows where to find the plan, and the plan has never been exercised in training. In one case, we served on a committee to develop a plan for securing conferences of a law enforcement trade group. The committee provided a clean solution to that problem, but we failed to realize that the actual goal was to provide an adequate mechanism for placing blame. The plan was rejected, so a new plan was developed, oriented more toward post-incident finger-pointing, which was significantly less clear but was accepted. It has never been implemented.

The result of systemic problems is that the system tends to force good people out, and substitute them with incompetent people, or people who serve a bureaucratic need rather than a purposeful functional need.

So, let us assume that Katrina has attracted your attention, and you want to give some thought to an emergency plan that might actually allow your company to survive, rather than to merely placate shareholders or insurers.

The easiest way to begin thinking about the problem is with the assumption that you will wake up one morning and discover that your entire plant at one geographical location has disappeared. At this point don't even give much consideration to how it disappears. It doesn't matter whether you are in a hurricane area, an earthquake area, a tornado area, or an area at risk for faith-based initiatives: Just start with the basic assumption that everything is gone.

What would you need to get back in business, or to stay in business?

- You need information – seventy percent of the value of the average American company lies in its intellectual property – so safe backup of and subsequent access to information is critical. And safe backup means comprehensive and geographically safe. Just as the several holders of the Coca Cola formula are reputedly never allowed on the same continent, your information should be backed up in some geographically safe area or areas. The good news is that in this computer era backup can be anywhere.
- You will also need people. Either you need to have a backup operation elsewhere, or you need to be able to move people and their families from one place to another, probably under difficult circumstances, and re-start in a timely manner.
- Finally, you will need capital, so your flight and recovery needs to be pre-planned with your bankers.

With these three points understood, you should be in good shape to start thinking about dealing with disaster, natural or un-, and to speak intelligently to the experts you bring in for consultation. Folks in the disaster recovery business will know from experience what can be implemented, and what sounds good on paper, but won't work in real life.

In trying to avoid the kinds of system problems seen in New Orleans, note that our colleagues in the international disaster recovery arena have expressed the opinion that one of the problems faced on the federal level (we will spare you their comments on issues of state and local incompetence exacerbating the legitimate – and highly desirable – local/state/federal disconnections imposed by 18 USC 1385) was that it was being handled by a security department. While security is an important component in disaster recovery, security is not the core discipline. Nonetheless, one of the downsides of centralization into a security organization is that staff, independent of specialization, eventually will either be forced into the current security-culture mindset, or be forced to leave. So be aware of the corporate culture of the group where operational responsibility is placed.

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — Coming soon to your company: A class action lawsuit**

We have recently had conversations with attorneys interested in class action lawsuits against corporations that suffered losses through competitive intelligence, espionage, and theft, and have not disclosed lack of an OPSEC program in their financials. This may indicate that the issue of dealing with information loss is about to become mainstream and front-page.

We are neither attorneys nor accountants, nor do we play them on television, but their theory seems sound: The SEC now requires internal controls in this area, and FASB would seem to indicate that their lack needs to be disclosed. So if a corporation suffers a loss and has neither an OPSEC program nor a disclosure of the risk this causes for shareholders, the directors and senior management – certainly anyone who has Sarbanes-Oxley responsibility – are now fair game for securities litigators.

Dancing away from this is a trifle more difficult now than it was before Sarbanes-Oxley. In the old days you could make the claim that intellectual assets developed in-house have no book value, and that the loss of un-booked assets is not a matter of public record or concern. However, loss of assets that have no book value, but underlie current profits and future earnings, can lead to significant financial losses. Even if you believe that the loss of \$50 million or \$100 million is not material to your \$35 billion dollar company – a claim that we have heard made – this probably won't hold up in the post-Sarbanes-Oxley world. And, as a manager, it may end up being personally painful to take that approach, because insurance companies seem to be indicating that failure to comply with SEC requirements in this area would be an uncovered deliberate action, not a covered negligent action.

There are three ways for a manager to deal with this issue. The easiest is to do nothing and hope that you will neither have a problem nor get caught.

The second easiest is to make a disclosure of risk in your financials, though you may be opening yourself up to additional problems.

The third easiest is to simply implement an OPSEC program. An OPSEC program is the least expensive SOX internal control you implement, and will not only remove the liability, but will go far in eliminating your share of the country's \$300 billion annual loss to competitive intelligence, economic espionage, and theft.

Prudence suggests that an OPSEC program should be implemented – and disclosed – before a loss, and before you are hit with a class action suit.

### **3. Executive Protection — Do you know your roads?**

Contributed by Basilio 'Bob' Reyes Jr., Executive Protection Officer, ConocoPhillips, Inc. (basilio-bob-jr.reyes@conocophillips.com). Contributed articles do not necessarily reflect the viewpoint of AEGIS.

As a Personal Protection Officer for my employer, the primary responsibility for my office is the daily safe and expedient transportation of our principal. While driving in and around this busy city where I live, work, and play, the question that comes to my mind on a constant basis is “WHAT/WHEN?”

As professionals, we have been trained by EP driving instructors that an attack on our principal is most likely to happen while the principal is being transported. Our vehicle, be it a sedan or SUV, armored or unarmored, is an office on wheels, and this is where the bad guys will try to snatch, harass, or kill our principal. We as professionals are already aware of this fact....I now ask you this: “Do You Know Your Roads?”

You may ask yourself, “what does he mean by “Do I know my roads?” I drive these same roads everyday. I know the exact number of miles from my principal’s residence to the office and back again. I could drive my primary route with my eyes closed, and my second and third routes with no problem. I can tell you where all the safe havens and choke points are. I’m on top of things. I arrive at the principal’s residence 15 minutes prior to pick-up and park down the street and watch for any unusual activity in the area. I’m on top of it. I’ve got it covered.”

No doubt you do because you take your job seriously and you want to continue to work in an industry that pays well and has outstanding benefits. Well then...what is this officer talking about when he asks “Do You Know Your Roads?”

As a professional, what do you do when you are confronted with a situation – carjacking, attempted kidnapping – while in your vehicle with your principal, your family, or even while you are alone? We all know that to hesitate or to do nothing will probably mean the bad guys will accomplish their mission. We are trained that we must keep the car moving. We may have to bang-up the vehicle some, or, worse, get shot at, but the most important thing to do as a driver is to MOVE! MOVE! MOVE! Get your principal out of the kill zone as quickly as possible.

As professionals we must conduct advances of not only the destinations where our principal will be in the future, but also of the various roads along the route(s) we take to these destinations. We must ask ourselves the WHAT/WHEN question continuously. It may not seem important to

investigate possible surface contacts along your route but keep in mind the vehicle is heavy, and you may have 3 or 4 passengers in the car, plus luggage. It may have rained that night or earlier in the day. The ground that was hard is now soft. Weather conditions definitely come into play....rain, drought, spills, construction, missing manhole covers, or accidents can change an area quickly.

This means that you must get out of the vehicle to look, feel, and investigate areas where you may have to drive one day: grassy areas, medians, hilly areas, construction areas, and ditches. Yes, it may mean breaking a sweat or getting those nice shoes a little dirty, but it is necessary, because the bad guys are looking at these areas in order to better trap you.

This is where KNOWING YOUR ROADS comes into play. When this EP professional is driving along the route, be it the primary or secondary or tertiary route, I drive past grassy areas, construction areas, ditches, hills, mountain ranges, deserts, and I am always asking *what* will I do *when*...

Let's say that out of the corner of your eye you see the bad guys coming, or maybe your principal or spouse or kid alerts you that trouble is brewing. You advise them to "GET DOWN" while at the same time you execute your move to get them out of the kill zone. You drive on, or drive through, or drive over whatever may be in your way. Let's say you're successful, but end up in the grassy area between the express way and feeder road, and your vehicle gets bogged down. Guess what? That's right, chances are that the bad guys may be able to recover and come after you. Chances are that your goose, or that of your principal or your family, will soon be cooked.

What happens when you get chased by the bad guys, or an accident in front of you develops and all you have time to do is swerve left or right to avoid an accident of your own? What do you now do? You deal with it as best you can, and do what is necessary to keep your principal safe while escaping and making your way to your nearest safe haven. We are trained to look where we want the vehicle to go, and know that eventually the car will respond. Now you find yourself headed straight toward the rather large grassy hill bordered by a small ditch with overgrown grass or weeds....

An executive protection *advance* of a location or building is very important; and not doing a proper advance can make or break an EP mission. But a well done advance of the destination doesn't matter when you're bogged down in a grassy area trying to escape the bad guys.

If we continue to do the best job possible there is no doubt but that we will be ready for the roads ahead.

#### 4. Technical Issues — Pretty Good Privacy

As our readers know, we at LUBRINCO are big believers in encryption. We encrypt our telephone calls using the Privatel™ 960V telephone encryptor (<http://www.lubrinco.com/ejournal/ej200104.pdf>) from L3 Communications, and encrypt e-mail and files with Pretty Good Privacy. Although we have reviewed the Privatel, we have never really discussed PGP® or OpenPGP (the publicly shared standard) programs. We will not here discuss every feature of Pretty Good Privacy programs, and we will discuss only Windows software: Our goal is to give you an overview of the main features of several programs in encrypting, decrypting, and signing files and e-mail messages: The specific features will be found on the vendors' Web sites.

PGP, developed by Phil Zimmerman, works on a public/private key principle. You have a private key you use to decrypt files and messages encrypted to you, and you have a public key that others use to encrypt files to you. Files and messages can be encrypted to multiple keys, and prudence says you should set the system to always add your key when you encrypt anything for others, so you can read it, too

Each version of PGP and OpenPGP has a mechanism for generating your key, and for getting keys of others from online *keyservers*. They give you choices in key length, with longer keys being theoretically more difficult to crack. We suggest choosing the custom option, and then choosing the largest number allowed. The reason for this is that in the old days, when we were running 6 MHz processors on our PCs, it took a long time to generate a long key. Today, with fast processors, the longest keys possible generate very quickly, so don't skimp. If you lose your key you are completely out of luck, and will not be able to read encrypted messages, nor restore encrypted files, so be sure to back up your personal key, and keep it somewhere recoverable after the flood. Alternatively, make the key valid for only a short period of time – say six months – so if you lose it, or forget your passphrase, people won't think it is still valid.

Once you have your public key made you can send it to others, and once you have the public keys of others you can send them encrypted messages. You can also *sign* messages with PGP, which allows the receiver to know that the message, encrypted or unencrypted, has not been tampered-with.

Since the functioning of most versions is very similar, we will spend a good deal of time discussing the features in the first product we discuss, and avoid a repetition of the same discussion in following products. Please do not consider this lack of re-discuss the features to mean we didn't like the

product. It merely means that we have already discussed that specific feature or feature set.

### **PGP 6.5.8**

PGP 6.5.8 is an older freeware version of PGP. It is in-theory obsolete, but can still be found on the Internet in a number of places (<http://www.pgpi.org/products/pgp/versions/freeware/win32/6.5.8/> is a good place to start, and you can find a good tutorial on its use at <http://www.neiu.edu/~ncaftori/PGP.htm>).

While in theory PGP 6.5.8 is *not* supported under Windows XP, XP is nonetheless the platform on which we happily ran it. Note also that the freeware version is not for commercial use. We don't encourage theft of services, so if you wanted to use it in your business, you should buy a license from PGP Corporation. Since this product is no longer supported, you will likely end up buying the license for their current product (which we will discuss below), and use it to cover the freeware version.

6.5.8 installs easily using standard installation software, and integrates nicely into your system, with an icon – PGPtray on the bottom of your screen in the system tray, and some choices added to the right click of the mouse in Windows Explorer. If you want to encrypt a file, you merely select it using Windows Explorer, click with the right button, choose PGP/Encrypt, choose to whom you want it encrypted (always set PGP to add your key to anything it encrypts), enter your passphrase, and you will have a second copy, encrypted, with the same name, but a new extension of *pgp*.

To send encrypted e-mail you have many choices.

- You can put the text into a document, encrypt the document, and attach it to your e-mail message. We often send encrypted Word documents, or encrypted Acrobat files.
- Copy the text (it goes to the *clipboard*), click on PGPtray and select clipboard/encrypt (the encrypted text will be put into the clipboard), then do a paste into your e-mail.
- Click on the PGPtray, select Current Window/Encrypt. Whatever text is in the current window will be replaced with the encrypted text
- If there is a *plug-in* for your e-mail client (Eudora or Outlook or Outlook Express. The Bat!, the e-mail client we use, supplies their own) you can just tell your e-mail program to do the encryption. Plug-

ins have fallen into disfavor, as they are difficult to write, and to keep current as software changes.

Any of these options take mere seconds though having the e-mail client handle the work makes the process of encrypting (tell it to encrypt) and decrypting (tell it to decrypt) trivial.

Decrypting is equally simple. If you manually decrypt (as opposed to having the e-mail program do the work) you will either copy the encrypted text and do a *Clipboard/Decrypt & Verify* which will place the encrypted text in your clipboard, or a *Current Window/Decrypt & Verify* that will show you the decrypted text and give you the option to put it in the clipboard. You then paste the decrypted message in Notepad or Word, or whatever other program you choose.

You can attach an encrypted file to your encrypted e-mail. To do this you encrypt the file manually, as described earlier, and then attach it as you would any other file.

Finally, this version includes the ability to securely *wipe* files, which overwrites them so they cannot be read, and deletes the unreadable file.

### ***FileCrypt® Desktop***

This early version of FileCrypt Desktop is an open PGP variant that comes from Veridis SA (<http://www.veridis.com/pgp/products/filecrypt-desktop.html>) and costs \$49. In its current state, FileCrypt does not add a system tray, nor tamper with the right-button options. Instead, when you start the program it brings you to the key manager the File option includes choices to encrypt, to sign, or to encrypt and sign. The dialog box includes the option to choose a file, or to choose the clipboard. Encrypted files can be attached to e-mail, and the encrypted clipboard can be pasted into an e-mail (or anywhere else, for that matter).

To decrypt, you select File/Open, and either select an encrypted file (which will place a decrypted version in the specified location) or the clipboard (which will place the decrypted text in the clipboard).

We are told by the folks at Verdis that the next version of FileCrypt Desktop will integrate a system tray, a shell extension (the right-button stuff), and an Outlook plug-in, as well as other updates. This version should be available sometime in October.

The operation of the version of FileCrypt Desktop we tried was straightforward, swift, and trivial to use, and we expect the new version will be equally so.

### ***FileAssurity OpenPGP***

Another Open PGPentry comes from Artisoft ([http://www.artisoft.com/open\\_pgp\\_encryption.htm](http://www.artisoft.com/open_pgp_encryption.htm)) and costs \$65.

FAOPGP integrates with the system, adding an item to the system tray, and changing the behavior of the right mouse click in Windows Explorer to allow you to encrypt, decrypt, or wipe. But in order to do any of these things, you need to sign in to the application using a password you put in when you install the program. This **password** is not the same as the longer **passphrase** you use to encrypt and decrypt.

While much of the operation of FAOPGP is similar to that of the previously described programs, this program handles e-mail in an interesting fashion that avoids potential problems associated with plug-ins. To select files to encrypt and e-mail, you select the files in Windows Explorer, click on the selection with the right mouse button, and select *protect*. This brings up a panel that allows you to select to whom it will be encrypted, and the option to send as an e-mail. If you choose the e-mail option, you can also choose to add an encrypted message. This will open an editing panel, into which you can type your message. When you click on *protect*, it will open your e-mail program and present you with a message for sending.

FileAssurity OpenPGP is fast and easy to use, and a reasonable choice if you don't want to use plug-ins, but still want a fairly integrated manner of sending encrypted e-mail.

### ***PGP® Desktop Home 9.0 and PGP® Desktop Professional 9.0***

Finally, we come to the versions for home and small business users from PGP Corporation. PGP Corporation offers their Home version for \$99 (<http://www1.pgpstore.com/product.html?productid=300023321>) and the Professional version for \$79 to \$199, depending on subscription (<http://www1.pgpstore.com/product.html?productid=300023322>). As best we can see, the primary difference between is that PGP Whole Disk Encryption and support for enterprise messaging (Lotus Notes and Microsoft Exchange) is not included in the home version. Both versions allow encryption of e-mail and, interestingly, instant messages.

This is a very complex program, and installation is likely to require some help. Unfortunately, we purchased licenses some months before we planned to install them to test. As it turned out, we should have read the small print. Free installation support is available only for 30 days after purchase, so by the time we did the install we had to rely on the kindness of strangers at the PGP support forum (<http://forums.pgpsupport.com/>) for help. It took about two months to get the program up and running, and, even with the advice we were able to give, based on our experience, to one of our associates co-opted for this exercise, he simply threw in the towel after a week of frustration.

Installing and using this program is like playing Go Fish with your five year old niece, with new rules appearing at each draw of the cards. As an example, we thought the program was working, but when we checked the message log we discovered that messages were being sent out unencrypted. We were told that the keys needed to be validated, and that if a key is not validated it will not be used, with the only notification being, *post facto*, the message log. How do you validate a key? According to the help file you do it by checking the key's fingerprint. In fact, you do it by *signing* the key, the details of which we will not go into here.

In addition, PGP Desktop 9 doesn't play well with others. The warning on the bottle, er, installation notes, says that if you run Norton AntiVirus 2005 (which we do) you have to disable scanning of incoming and outgoing e-mail. And if you use the VPN the FBI hands out for Infragard communications (which we do), you have a problem because it won't co-exist with PGP Desktop 9. And even with the helpful efforts of the programming staff at Firetrust we were never able to make it work with Benign (<http://www.lubrinco.com/ejournal/ej200309.pdf>), which we use.

But let us assume, for the sake of argument, that you work in a corporate environment with all your software compatible with PGP, and that you are able to get the program installed and running, i.e., that you have an experienced IT staff at your disposal, and don't have to do it yourself. In this case you end up with a pretty nifty product.

The integration with Windows Explorer is consistent with that previously described, and the Current Window and Clipboard features seen in other versions also are part of the PGPTray options. Handling of e-mail to those with known keys, however, is now totally automated, with PGP avoiding the plug-in issue by acting as an e-mail proxy server. Thus, when we send an e-mail with attachments (astonishingly, PGP Desktop 9 worked, sort of, with our e-mail client, The Bat!, for which it is not certified), the program

recognizes that there is a key, encrypts the text, encrypts the files, and sends the whole kit and caboodle, encrypting both the message and any attached files. Well, usually: Sometimes it doesn't seem to encrypt messages, and sometimes it doesn't encrypt attachments, but this could be the fault of our not-certified e-mail client, or operator error.

When you get encrypted e-mail, PGP Desktop will automatically decrypt both the messages and the attachments before they hit your e-mail client, so that you are never aware that anything has been encrypted at all. If you like to have encrypted documents stored encrypted, you can either copy the attachment somewhere and re-encrypt it, or make an encrypted directory on your hard drive and store this information there.

In any case, if you have a good IT staff that can actually get the program working (We have no reason to believe that this is not actually possible: The fact that we are not able to do something doesn't mean that others won't be able to do it.), and if you have users who should be using encryption but sometimes forget, this program will automate the process for them, taking the decision as to when to encrypt or not completely out of their hands.

### ***And the bottom line is...***

Encryption, whether of voice or documents, is very important. For voice, get a Privatel. For document and e-mail encryption, choose one of the PGP or OpenPGP programs available to you – and there are more available than we have discussed here, particularly for the large-scale corporate user. One will surely meet your needs. Find it and use it.

## **5. Real Stories from the Field — Unintended consequences: How Sony and Universal will force you to make bootleg DVD movies**

Like most of you, we have a lot of CDs, many of which replace the vinyl disks that preceded them. And we have a lot of DVDs, many of which were replacements for the VHS tapes that replaced our Betamax tapes. Storing and playing these has been made much easier with the advent of high-capacity CD/DVD players such as the Sony DVP-CX985V and Sony DVP-CX995V, each of which hold 400 disks. These devices are incredibly convenient. Once they are loaded you can put the player in some convenient yet inaccessible place, and still access every disk using the remote control, never having to touch the disks again. Until, however, you buy a DVD such as *Schindler's List* or the CITA DVDs (tango DVDs available for those who

love Argentine tango at <http://www.cosmotango.com/DVDs.htm>), which come not as two DVDs, but as a single double-sided DVD.

If you have your DVD carousel, as we do, conveniently located under a cabinet where it can be seen by the remote control, but not easily accessed, you are in for some annoyance. When you have finished playing the first side, you have to crawl under the cabinet, push the open button, eject the disk, put it back in, albeit now with side B facing left, push the close button, crawl out from under the cabinet, press the play button on the remote control, and watch the rest of the picture.

Of course, you could avoid this annoyance and buy two copies of the Schindler's List, and use one disk for side A and the second for side B.

Or you could buy some other movie that didn't use double-sided disks: There are lots of movies, and your life won't be ruined by not having one that is only available on double-sided DVDs.

Or you could make a copy of the second side, and take up two slots, as you would with any other double disk movie. The bad news, is that the movie folk have been cracking down on the people who published decryption software, and have forced them to remove their software from the Internet (though DVD Cloner II, at <http://www.dvd-cloner.com/>, appears to be still available). The good news is that your kids most likely already have copies of banned software, or have friends who do, so you can probably have them bootleg a side for you, and avoid crawling under cabinets or doing without.

## 6. Book and Product Reviews

*SpyFinder*® - Personal Hidden Camera Locator  
Apogen Technologies, Inc.  
\$114.99

<http://www.thespyfinder.com> 1-800-903-3479



SpyFinder is the civilian version of the \$2,500 laser-based camera detection system (<http://store.yahoo.com/shop-seatech/spyfinder.html>) developed by Apogen Technologies. The product is deceptively simple: You push a button which triggers a ring of six flashing LEDs, peer through the center of the ring and look for reflections. If you move your head slightly, reflections off shiny surfaces will move with you. Reflections from a lens system will not.

We took the SpyFinder with us to a trade show for folks in the alarm business, sure that there would be a lot of hidden cameras among the vendors' wares. There were, and we were able to find all of them.

That said, it is important to remember that this device requires a significant amount of operator experience. A camera may well be hidden in a clock, behind smoked Plexiglass. This means that the reflection will be small – pinhole cameras use very small lenses – and not terribly bright. Thus, while some advertisements optimistically say “You can instantly locate any hidden cameras, wired or wireless,” they are very wrong.

Just as with electronic bug sweeping, it takes a trained operator a surprisingly long time to do a sweep, and even then you will leave with some nagging doubts as to whether you have found everything.

The instruction manual suggests that you scan at the rate of a foot per second at a distance of three to ten feet, which seems about right to us, at least on something like a blank wall at ten feet, where there should be no reflections. It will be slower when there are a lot of false positives to eliminate, and you have to move to the three foot range.

This is assuming you know what you are looking for. How do you know what you are looking for? Get a pinhole camera and look at its reflection, so you know what a valid positive looks like. Then try hiding it behind various translucent barriers. Then go to one of the stores that sell James Bond-ish toys, and try to find the cameras they have hidden in clocks, teddy bears, and a host of other objects.

Once you have gotten proficient at finding lenses that you know are there, you can have someone else start hiding them for you, with you trying to find them. Eventually you will gain a feeling of confidence, and be able to do a sweep with only the normal minimal nagging doubts as to whether you have found them all.

This is a good device which has a very low price tag. With sufficient time, a diligent user with some experience should be able to do a good job of finding hidden cameras.

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

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2005 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.

- **Sarbanes-Oxley Section 404 OPSEC compliance.**
  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 October 2005 **ÆGIS** (© 2005 **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.