



ÆGIS journal

Addressing threats that affect your bottom line

Volume 10 Number 2, February 2007

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: Critical Information and IP Conference**
- 1. **Asset Location and Due Diligence — Records retention policy**
- 2. **OPSEC, Economic Espionage, and Competitive Intelligence — CALL for PAPERS and PRESENTATIONS**
- 3. **Executive Protection — Straight from the cat's mouth**
- 4. **Technical Issues — EFT reversals and ACH fraud**
- 5. **Real Stories from the Field — BOP FOLP**
- 6. **Book and Product Reviews — ChoiceMail**
- 7. **Subscription/Unsubscription/Copyright Information**

ÆGIS journal, in conjunction with
The Center for the Study of Law, Science, and Technology,
Sandra Day O'Connor College of Law at Arizona State University
and
The OPSEC Professionals Society
will be hosting its two-day **Critical Information and IP Conference:**
Identification, Valuation, and Protection of Critical Information and Intellectual Property
For Directors, Finance Officers, and Counsel
At Arizona State University in Tempe, Arizona, **2-3 October 2007**
For information, contact us at conference@aegisjournal.com

1. Asset Location and Due Diligence — Records retention policy

The issue of records retention is one that has concerned us for quite some time. We would suggest you re-read our initial article (December 1998) on records retention policies, and integrate that information with this new update on Electronically Stored Information, or ESI as it is called.

Note upfront that we are not lawyers, and that what we are presenting here is not legal advice. Rather, these are some issues and suggestions that you should take to counsel for discussion.

In many cases it appears to us that ESI is discoverable. Failure to preserve ESI according to a written policy might allow judges and juries to draw the conclusion that the business had something to hide. You might be tainted with guilt and non-compliance for not having something they *assume* you should have. Crazy as it seems, by failing to have a written records retention policy that deals with ESI, you are then presumed to have whatever the other side alleges you should have. When you can't find the records they ask for, you may end up in a battle to show how their allegations of malfeasance or misfeasance are unfounded. In theory it sounds bad. In practice it is worse!

Here are some suggestions on what you should discuss with counsel.

A. Identification of all of those things you have floating around that may have ESI implications. Sure, we know about computers. But do not forget PDAs, cell phone records (including calls dialed, received, text messages, and photos), digital images and sounds on cameras computer CDs and DVDs, video recorders, offsite records backup, Web-based e-mail, flash drives, programmable calculators.... Now, this may be a daunting list for the average service business; however, if you are a technical business

with lab and field equipment, you have to deal with *all* of the ESI that may be contained within your equipment.

- B. Once you have catalogued *where* all of your ESI may be resident, choices need to be made. You need to discuss what stays and what goes and why. There are all sorts of rules and regulations about how long to keep things depending upon what they might be and to what they may relate. Your counsel should have concrete ideas about the law on those areas that apply to you. Don't guess. Your written policy should carry these statutory requirements, plus establishing a policy for retention or destruction of data for which there is no statutory retention requirement. We recommend a policy of getting rid of as much as possible as soon as possible within the provisions of statute, accompanied by the actual practice of getting rid of data as specified by this policy.
- C. All electronic devices require maintenance so they function at an optimal level. Maintenance often means shuffling data, archiving old data, and erasing caches of data and unused material. We all know that much erased data may remain resident on our machines. Is that erased data now part of a discoverable records? We believe so, but you should verify this with counsel for your specific circumstances. So your records retention policy may additionally need to address the consequences of t of maintenance on devices containing records.
- D. Getting it right can only be verified by testing. Our suggestion is to put together a team to test your system, with the team consisting minimally of an attorney and a technical person. The attorney can read over the policy, and the technical person can make sure the technical stuff works.

2. OPSEC, Economic Espionage, and Competitive Intelligence — IP/CI Conference CALL for PAPERS and PRESENTATIONS

Conference Mission:

The mission of this conference is to provide senior managers and counsel with the most current strategic and tactical knowledge base on the identification, valuation, and protection of intellectual property and critical information

The objective is for the papers and presenters to be informative, as well as to give readers/attendees no option but to think and plan.

Commercial Climate:

Loss of critical information and intellectual property from competitive intelligence, economic espionage, and theft is a serious and burgeoning problem. The cost of an average incident in a manufacturing environment is \$50 million. The cost of an average incident in a non-manufacturing environment is \$500,000. If one incident is uncovered, a second – and often third – incident is usually discovered to be taking place concurrently. Losses of \$100 million or more can have a significant effect on a company's financials, producing a reduction in earnings of a dollar per share if the company has 100 million shares outstanding!

The federal government estimates total annual cost of competitive intelligence, economic espionage, and theft to be \$300 billion. This is 2.25% of America's GDP, and translates into 7,500,000 American jobs lost annually.

Because of the economic and social significance of these losses, the SEC has mandated that, under Sarbanes Oxley, companies must implement internal controls to track these losses. That pre-supposes the ability to identify, value, and protect intellectual property and critical information.

There are three problems that can arise from not having a program for the identification, valuation, and protection of critical information and intellectual property, each of which can affect senior managers and directors:

1. They will have to deal with the consequences of being in non-compliance with Sarbanes-Oxley, which can involve both civil and criminal exposure.
2. If the theft ends up being prosecuted under the Economic Espionage Act of 1996, a compelling case can be made that by not having an OPSEC program as required by Sarbanes-Oxley to identify, value, and protect information from competitive intelligence, economic espionage, and theft, they failed to take the required "reasonable measures to keep such information secret." This means that they have, through negligence or deliberate indifference, abandoned the trade secret status of the stolen information, which was therefore not a trade secret as defined under the Economic Espionage Act of 1996 and the Uniform Trade Secrets Act.
3. They face the possibility of shareholders bringing a negligent action lawsuit because the company knew (or should have known) that with annual domestic losses of \$300 billion, there was a high-probability

threat that should have been addressed. PLUS they both abandoned the trade secret status of their information under the Economic Espionage Act AND were non-compliant with Sarbanes-Oxley, which were at least partly designed to force them to protect shareholders from just this type of loss. Since ignoring Sarbanes-Oxley requirements indicates negligence or deliberate indifference, there is a probability that their liability will not be covered by their Directors and Officers Insurance because they did not exercise due care. It becomes personal liability.

Topics

We are looking for presenters and papers addressing strategic and tactical (but not operational) issues on:

Identification

- The intangible economy
- Management objectives and the information that adversaries and business competitors would find helpful or critical in defeating those objectives
- Identification, cataloguing, and tracking IPCI
- IPCI audits
- IPCI banks and funds
- IPCI, public companies, SOX, and the SEC

Valuation

- Valuation of IPCI
- The effect on the organization of lost or compromised IPCI
- IPCI value impairment through failure to implement an OPSEC program
- Items that relate to the topics of IPCI, valuation, the future of IPCI
- Litigation / OPSEC / IPCI valuation / M&A
- Recovery after a loss

Protection

- OPSEC: The government-developed process for identification, valuation, and protection of critical information
- Identifying adversaries and competitors
- Tracking IPCI that has left its company

Implementation

- Creating a system-wide OPSEC program
- Location of IPCI, geographic and legal environment
- Dealing with the publicity of IPCI losses
- What an ideal IPCI jurisdiction would look like
- Re-domiciling IPCI
- IPCI and SOX reporting

Please note that while we are focused on addressing the Conference Mission, we will consider *all* submissions. After all, you may have a great topic we have not thought of, so send it in!

Submission Requirements:

The paper or presentation (if completed), or an abstract of the paper or summary of your presentation.

Include title, author's profile, affiliations, and contact information (address, e-mail and phone number).

Submission of a paper grants AEGIS unlimited use of the material if accepted for publication or presentation, with copyright retained by the author.

Submission deadline: Postmarked by 10 April 2007.

Send submissions to papers@aegisjournal.com

or

AEGIS journal
440 W 41st ST
New York, N.Y. 10036-6816

CLE Credits

CLE credits may be available (depending on state requirements).

Conference Registration:

Registration is \$450.00 for participants registered before April 1, 2007 and \$550.00 dollars for those registered after 1 May 2007.

Presenters will receive complementary registration.

Those who have had papers selected for the conference publication, but not for presentation, will receive the conference publication free of charge and may attend for a registration fee of \$50.00.

Those interested in attending can call us at 1-917-545-9428, e-mail us at conference@aegisjournal.com, or mail us at

AEGIS journal

440 W 41st ST

New York, N.Y. 10036-6816

3. Executive Protection — Straight from the cat's mouth

In our line of work we occasionally get to spend time at seminars with some very accomplished criminals. Counterfeiters, embezzlers, and cat burglars, oh my! At a recent convention we had a chance to meet a cat burglar of some renown. And while never actually caught, he was very well known by the insurance and high-end jewelry industry. In our wide-ranging discussions we learned a great deal about how these burglars work.

As a jewel thief, the first thing you need is a target. The best targets were in Orange County, California, along the Dallas / Austin corridor, and on the east coast of southern Florida. Every so often he would drive through these different locations. He would visit high-end jewelry store parking lots and write down the plate numbers of the fancier cars, then work to trace those cars back to a residence. He would also pick up society magazines and see who was wearing what jewelry in the vanity photos. He also kept a very good calendar on for the different charity and social events, with a list of who would be in attendance at which events.

This detailed process of lead generation and record keeping allowed for the efficient vetting of potential targets. It also allowed for the assemblage, over the years, of an inventory of different pieces of jewelry for each of the socialites culled from the vanity photos in the society magazines.

Appearance at high-end jewelry stores prior to an event was a clue that a

new bauble was being added to the collection, and that the previous baubles would be left at home during the event. It also allowed for the assessment of “lower events” where the target maybe present but not likely to wear any of the good stuff.

Additional vetting was done in person. He would crash society events as a well dressed, convivial, member. He actually became fairly well-known and even, much to the chagrin of all involved, ended up with no small number of photos in society publications.

The objective was to determine the value of the target, and what was to be expected at the residence while they were away at an event, including how much time the target would be gone. Finding the residences of the socialites was not difficult. County records were usually all that was needed.

Alarms at the home were always a problem, but since alarm companies love to put up signs and stickers, they knew what company was running and monitoring the alarms. Most alarm installers don't bother to remove the factory default codes for the alarms, and he knew which firms were sloppy.

For those alarm installers known to do their job correctly, and where it was a target of high desirability, he would trigger the alarm several times in the preceding weeks leading up to the event, and sometimes even as the target was leaving. Most of the time he would place powerful magnets by several of the window alarms just prior to the society event so the alarm would either go off or be unable to be set. The target always gave up on the alarm and left the residence un-alarmed.

Once the target was selected and calendared, the target would be studied as laboratory animals (or potential subjects for kidnapping) would be studied. All of the regular places, habits, friends, et cetera, would be cataloged. He would know more about the target than possibly even their spouse, so when the night came, nothing would happen by accident.

His selected entrance to a target home would be the most secluded, most expeditious, and closest to where the target's jewelry might be hidden. He frequently would discover that most of the jewelry was kept unlocked in a jewelry box on a dresser, or in a locked drawer in a closet. Some was kept in safes, which were not secure since he would have several hours open it.

All good things come to an end. The pictures in the vanity publications were not only his shopping list, but also nearly lead to a rap sheet. An insurance investigator began to tie his appearance in town to the daring thefts. The first hint of danger was when he opened a locked drawer in a closet of one of his

targets in Austin. It contained only a note. “Sorry, Hank, we are on to you.” That sent a cold shiver down his spine, and he ran and never went back to Austin. Then, four months later in South Florida, he found the same note in the safe of a target. “Sorry, Hank, we are on to you.” That was his last night of work.

He later learned that an insurance carrier had contacted all of the big clients tied to these society events and had instructed them to move all of their jewelry to a bank vault, and leave the note in place of the jewelry. The fact that the insurance company had his alias was a great shock.

So what were Hank’s suggestions to keep stuff safe? Simple, read the story and see what everyone was doing wrong. They had cut-rate security systems, if they had any at all. In most cases, if they were above the 10th floor and lived in a “secure building,” targets usually failed to lock their verandah doors or condo windows.

Next, keep good fakes in the jewelry box and safe. Secure the good stuff someplace other than in the bedroom, or the closet, or behind a painting.

When traveling, bring one set of good jewelry to wear out. If you want more for day use, buy some good paste. Good enough to fool friends, but not so good that an expert could not spot it 20 feet away.

He also suggested quit showing up in society vanity papers – essentially advertising what they owned – but some things are just too much to ask.

4. Technical Issues — EFT reversals and ACH fraud

Many Thanks to Bob Leahy at moi@bobleahy.com for allowing us to pirate and paraphrase his questions and answers on EFT reversals and ACH fraud. A client called him with a question. “We inadvertently sent an EFT payment to the wrong vendor and have been unable to retrieve the funds from the vendor. Do we have any recourse from the banking system?”

The NACHA (National Automated Clearing House Association) will allow the recall of a *file*. A file is not an individual transaction but the whole group of transactions initiated at the same time. However, if the EFT was the only transaction initiated at that time you can reverse that transaction through an EFT Debit. To do this you must request a reversal from the receiving bank. The receiving bank will request permission from the account holder whose account the funds went into. If the consent is granted, the EFT reversal will be granted and the receiving bank will return the funds. If the receiving account holder refuses permission you get to go to court.

Another question came from a reader on how to prevent fraudulent check and ACH transaction hitting their accounts. The answer is that you cannot prevent them from hitting your accounts. You can, however, prevent those accounts from paying out. What needs to be done is for you to set up an account that is for deposits only. All of the credit cards, cash, checks, ACH, et cetera, all go into that account. That account is a check- and ACH-blocked account. The funds are then transferred into other accounts used for payments, purchasing, payroll, et cetera. On those other accounts you use positive pay to monitor the activity and stop unauthorized debits.

If you are large enough, you can use one account and negotiate with the bank to see if you can add some MICR lines at the bottom of the check. Those MICR lines will contain coding that automatically assigns that amount to a cost account. But you need to be big company or have a really accommodating bank if you are smaller.

5. Real Stories from the Field — BOP FOLP

The scam is a straightforward pitch to help people get out of debt and put money in their pockets. It was made through BOP FOLP advertisements in local papers and signs nailed to street posts. BOP FOLP – Back of paper/front of lamp post – are two of our favorite credentials for financial services.

When you came to a meeting there were real people standing up and extolling the benefits of how Mr. X had helped them with their debt problem, and how he was able to help them refinance their house to put \$10,000, \$20,000, or even \$30,000 cash into their hands.

There was a \$200 dollar sign up fee, plus 30% of any new cash Mr. X put into your pocket. He promised that for this \$200 he would help you get out of debt. A few people there did sign with Mr. X, and we asked to see the contract. It looked all nice and pretty, but did contain a paragraph about disclosure. If the client were to disclose the methods used, he could be subject to a contractual debt for this disclosure of \$5,000 or 70% of the newly acquired cash-in-hand.

Over the next three weeks we followed two couples through the process that Mr. X proposed. The first thing he instructed them to do was to file notice of lien satisfaction with the appropriate courts for all of the outstanding judgments they may have had, and to file the same notices with the county recorder's office. Concurrently, a number of fictitious loans and repayments were reported to various credit bureaus through Mr. X's companies, so the

client looked as if they had borrowed and repaid large sums of money. Thus, they have appeared to have repaired all of their debts (when they had not), and now appeared to be a good credit risk (which they were not).

Mr. X was then able to get many of them new loans on their homes and collect 30% of that new cash. If they did not have enough equity in the home, no problem: He helped them file papers showing their lien was paid off, and got them new loans.

Mr. X was not doing anything illegal. Well of course not! All of the people were filing the fictitious releases, not him. He was just helping people pay their bills and find new money. In the end, Mr. X turned out to be a convicted felon, and now all of the people he was helping also face the real prospect of becoming felons too.

By the way, Mr. X immediately filed suit in federal court against those good folks who ratted on him, claiming breach of contract. He obtained a number of 5K judgments against these people (you can't make this stuff up). Since Mr. X already knew where they banked, he was able to garnish what little these poor saps had left, even as they were trying to deal with the county accusing them of fraud and their creditors coming after them.

6. Book and Product Reviews

ChoiceMail

DigiPortal

\$39.95

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

The other day we realized we were drowning in a sea of spam, with this editor alone receiving between eighteen to twenty thousand pieces of spam each month, and growing. MailWasher, the excellent tool we had used up to now was ideal when the flow of spam was more reasonable, but we had reached the point where, if we went on a trip, our mailbox was full, with bouncing messages, before we had checked into our hotel. We decided to look at challenge-and-response systems, and tried ChoiceMail, which had been recommended by a friend.

DigiPortal makes ChoiceMail in versions for in-house servers and third-party servers, as well as for single users, which is what we tried. They also have a free version if you have only a single POP3 account (ChoiceMail Free does not work with Yahoo, AOL, MSN and Hotmail Webmail accounts), and can live with some minor restriction of features.

After downloading the trial software from http://www.digiportal.com/redirect/try_cmo.htm, we installed it and configured it (we ignore here the internals of the system), which was quite straightforward. We were able to import our MailWasher friends list, which meant that the people with whom we were already in correspondence would not be subject to challenge. For them the change would be transparent.

For the rest, this is the way it works. You select a time-period for mail checks. The program downloads all your mail from all your accounts on that schedule. E-mail from people on your approved list (or who meet criteria you set up, such as accepting mail from listservs) go into the approved mail section of the program.

Everyone else gets sent a response asking them to take a few seconds to click on a link and verify themselves. When they do this, the system (as we have it configured) adds them to the approved list and moves their mail into the approved folder.

After a period of time that you specify (we chose three days), mail in the unknown senders list gets moved to the junk box, where it sits for another user-specified time (one day for us), at which point it is deleted. Over time ChoceMail stabilized at 92% of the incoming mail being spam.

For the first few days we checked the unknown users list regularly, but stopped bothering once we had confidence in the system. Now we check it only if we expect something unknown, like order confirmation from a new on-line vendor.

Keep in mind that unlike MailWasher, which allows you to delete e-mail on the server without ever downloading it, ChoiceMail will download all e-mail. This means you will be getting a lot of malware laden e-mail hitting your computer. The good news is that you don't care, because A) your anti-virus software will kill all of it and B) this mail will never receive a response to the challenge, so it will go from unknown to junk to gone without your ever having contact with it. The bad news is that if your anti-virus software makes a noise when it finds a virus, you will need to turn the noise feature off. Rest assured that this will not slip your mind for too long....

The only problem we foresee is travel. As an example, next month we will be away for several weeks in places as far apart, geographically, culturally, and alphabetically, as Argentina and Uzbekistan. During this period we won't, for a variety of reasons, be able to directly access our e-mail. While we can have someone check it regularly, we may just set up a temporary account on one of the Web providers, and send all legitimate users an away

message saying to either wait until we get back, or re-send to the temporary Web mail account.

The only oddity we experienced was that six months after we bought our copy they came out with a new version. You got a free upgrade if you bought it in the previous month, but those who bought it earlier in the calendar year had an upgrade charge of \$19.95, or half the original purchase price. We feel this high a percentage this soon after purchase is untoward. Since we could see no functional difference between the old version and the new, we chose to stick with what we had.

If you have small amounts of spam then MailWasher continues to be a useful tool. If you are overwhelmed with spam then ChoiceMail is definitely worth a look.

7. Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2007 by The **LUBRINCO** Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com), L. Burke Files (LBFiles@feeinc.com), and Terry Phillips (TPhillips@aegisjournal.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.

- **Identification, valuation, and protection of intellectual assets and critical information.**
 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 is the leading private sector provider of 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, and 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.aegisjournal.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 subscribe@aegisjournal.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 unsubscribe@aegisjournal.com.

If you know of anyone else who should be receiving **ÆGIS**, please send their e-mail address to subscribe@aegisjournal.com.

If there is a topic that you would like to know more about, send it to editor@aegisjournal.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 editor@aegisjournal.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 **ÆGIS** Web site is included. This should be in the form

Article Title, from the February 2007 **ÆGIS** (© 2007 **LUBRINCO** & FEEINC), to be found at <http://www.aegisjournal.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.