ÆGIS journal

Addressing threats that affect your bottom line

Volume 13 Number 6, November 2010

From the case files of

LUBRINCO

http://www.lubrinco.com/

1-212-695-1759and

FE&E Clarity From Complexity
Financial Examinations & Evaluations, Inc.

http://www.feeinc.com/

1-480-838-1728

Announcements:

Due Diligence for The Financial Professional – by L. Burke Files
Now available at Aegis Journal and Amazon.

http://www.amazon.com/Diligence-Financial-Professional-Burke-Files/dp/0982372337/ref=sr_1_1?s=gateway&ie=UTF8&qid=1285712297&sr=8-1

1. Asset Location and Due Diligence - The Cold Case

The fraud was many years ago. Fraudsters, victims and witnesses have moved on and have become difficult to locate. Clues are sparse. The statute of limitations is about to toll. Yet, a client wants you to investigate to determine if party X, Y or Z maybe liable. What is the approach?

The first is to hire investigative firms that are specialists in the subject matter. Hire A Financial Investigator if you are dealing with finance, or Aircraft Accident Investigator if you are dealing with aircraft accidents. Retain a specialist with a specialized knowledge so your expert will have the knowledge and tradecraft to uncover information that others will no doubt overlook.

Go for the low hanging fruit. Recover what legal filings are available, as well as exhibits, to find the names of witnesses and victims -- then locate them. Consider sending notices to all parties to preserve what records they have. This is dual edged sword. Some will do as instructed, and some will ensure everything is destroyed. It's a decision the team should consider.

Recover pubic records where possible. Not all records will be available via the Internet. More often than not you will need to physically retrieve records, and you need to be prepared for this. If the records sought are no longer available, check for municipal archivists. While a department may indicate that records were destroyed, more than half of the time we can find "destroyed" records with the city, county, or state archivist. Look for ancillary records. For example, with property records if you can't find the title information you're looking for, look for those records generated by property owners. If ABC Co-op owned the property of interest, go to the city and look for construction or renovation permits, check with the notary on the recorded documents, check with the trash department to see who was paying the bills, talk to neighbors, check with the police and fire departments to see if there were any calls for service during the time in question. You have to wear out some shoe leather -- this is not a desk problem.

Cold cases are not elegant forty-five minute solutions as seen on TV. They require patience and a thoughtfully designed investigative process which assesses what can be done and what should be done given the resources of time and funds available. The first objective is to assemble facts. Once some of the facts begin dribbling in, the assembled team should develop several different hypothesis of how the facts fit into

a congruent narrative, and then test and retest the hypothesis as new facts are discovered.

You will have one of three outcomes; you will have assembled enough information to initiate a cause of action, your facts rule out any cause of action, or you will run out of time and money.

All investigations are time and treasury sensitive, cold cases are just more sensitive. Cold case investigations are initiated when one or more of the victims or their representatives has an unresolved issues, aka a nagging question itching to be answered. They are willing to invest in the pursuit of an answer, but how much? If you find facts that support a cause of action they will, most likely, invest more money for a recovery. Thus, the facts need to be solid and presented as evidence worthy in as short a period of time as possible. If you find no cause of action or run out of time, they may be ridiculed for throwing good money after bad – they know that. Their hope is for a recovery -- their fear is another loss and ridicule. The investigator needs to be authentic in the retention process and let the potential client know that they, the investigator, is aware of the conundrum; crafting an effort with an insufficient budget or time will result in the worst of all outcomes. It assures that no recovery will be made and there will be no resolution to their nagging feeling that something was left on the table.

2. OPSEC, Economic Espionage, and Competitive Intelligence - Get out of Jail Free. (Thank You Howard Fisher)

One of your editors was speaking at the Offshore Investment Conference in San Juan Puerto Rico in November, and enjoyed a presentation by Howard Fisher. Part of his comments revolved around what he called “Get Out Of Jail Free” cards. The presentation was an overview of offshore financial fraudsters and some of the companies who have perpetrated financial frauds. The gist was that many owners or employees of a company who were dealing with very bad people – mob guys and drug dealers -- used records they had obtained through their workplace to trade for stuff. The stuff included their freedom when they traded it with prosecutors who were after them. It also included cash, as they sold financial records on tax cheats to governments where the tax cheats resided.

If you think this is stolen information – you're right. The governments response to obtaining or buying stolen information is *tuff* stuffing (legal term of art). It comes under what Howard referred to as the silver platter doctrine. Whatever the origin of the information, as long as the government did not steal it -- it doesn't matter. Just as John the Baptists head was delivered by Herodias to Salome, the information was delivered to the government on a silver platter.

So what is the warning on CI and OPSEC? Secure your information. Though you may not be engaged in multinational criminal acts, your information is, nonetheless, still valuable. It can be sold to a competitor overtly as information stolen, excuse

me -- liberated, from your company. It can be sold to a competitor covertly through a consultant who just happened to posses your information. The information could be used by a former employee now working for a competitor. An executive recruiter could try to buy a copy of your employee directory to recruit your best employees. There are more ways to make use of information than you can imagine. Trust us on this.

There are also many ways to secure your information. It's not enough to be aware of this, you have to do it. Begin the process yourself and then hire an expert to coach you on what you may have missed – but do it! There are more cards in the Chance deck than just "Get of Jail Free" – some are good and some are damaging ; that's why it's called "Chance". Your unsecured information is like the evil twin to the lottery. Many will play, and most will lose, but every now and then someone, somewhere, will win the jackpot.

Collectively, whatever their motivation, people understand that there is value in information they possess. Whether it's internal records of a company, or information on the dealings of their clients -- all can go up for sale or barter in a legal action. Admittedly, multinational frauds are an extreme example of the recognition of information, but they do drive home a point.

(Howard Fisher – howardsfisher.com)

3. Executive Protection - TSA Body Scanner

"TSA Naked Body Scanner Images found on the internet"; "Backscatter radiation is harmful especially in cumulative doses"; "Backscatter poses *no* health risks".

The new TSA screening system is rolled out with promises made about privacy filters, limited retention of records, and whatever other statements are necessary to move it forward. It appears to be bull right out of the gate. Images posted on the Internet, the Indian movie star Khan having his naked image printed up and shared – all very disappointing. I know, it's not the system; it's just one or two untrained or poorly supervised bad actors. But aren't failures of complex systems always like that? The system is fine; the people who run the system are the problem. That logic is faulty on its face, since there would be no system without the people. It is the system.

Complex technology or processes married with complex human control systems (bureaucracy) are prone to failure. Why? They are not tested and retested before deployment, and generally lack a credible feedback loop if failure or clues to impending failures appear.

Yet the discipline of deploying new technology demands testing and retesting in a variety of circumstances. But testing is such a bother… The government says the Backscatter device is safe, and the manufacturers say the Backscatter device is safe. Hardly an unbiased opinion. So if the Backscatter device has been tested, really

tested, then -- where was the device tested? How was it tested? Who did the testing? Who funded the testing? Was the testing pushed until failures occurred? We looked for specific information – but did not find any. If any of our readers knows where it is, please forward a copy or link to us.

Absent specific studies, as the good little editors we are, we did a bit of research on submillimeter radiation. What we found is that there is not a coherent scientific conclusion that submillimeter is safe, but it is presumed to be safe based upon what is known. Conversely, there is a blanket medical community consensus that more radiation exposure is bad and less is better. The submillimeter radiation used in the body scanners appears not be harmful, and appears not to penetrate bodies of water, but can penetrate dry skin and some layers of fatty tissue. But we, as editors and frequent flyers, are still skeptical of the safety claim. Please read below what is lifted from the Wikipedia posting on submillimeter radiation / Backscatter.

The term typically applies to electromagnetic radiation with frequencies between high-frequency edge of the microwave band, 300 gigahertz (3×1011 Hz), and the long-wavelength edge of far-infrared light, 3000 GHz (3×1012 Hz or 3 THz). In wavelengths, this range corresponds to 0.1 mm (or 100 μm) infrared to 1.0 mm microwave. The THz band straddles the region where electromagnetic physics can best be described by its wave-like characteristics (microwave) and its particle-like characteristics (infrared). Terahertz waves lie at the far end of the infrared band, just before the start of the microwave band.

The terahertz band, covering the wavelength range between 0.1 and 1 mm, is identical to the submillimeter wavelength band. However, typically, the term "terahertz" is used more often in marketing in relation to generation and detection with pulsed lasers, as in terahertz time domain spectroscopy, while the term "submillimeter" is used for generation and detection with microwave technology, such as harmonic multiplication.

Safety

The terahertz region is between the radio frequency region and the optical region generally associated with lasers. Both the IEEE RF safety standard [8] and the ANSI Laser safety standard [9] have limits into the terahertz region, but both safety limits are based on extrapolation. It is expected that effects on tissues are thermal in nature and, therefore, predictable by conventional thermal models. Research is underway to collect data to populate this region of the spectrum and validate safety limits.

In October 2009, a possible mechanism of DNA damage from terahertz radiation was proposed, according to which resonant effects allow THz waves to unzip double-stranded DNA, creating bubbles in the double strand that could significantly interfere with processes such as gene expression and DNA replication. However, the predicted DNA unzipping has not been verified experimentally and DNA bubbles have been reported to naturally occur due to temperature effects. Researchers claim.

The evidence that terahertz radiation damages biological systems is mixed. "Some

studies reported significant genetic damage while others, although similar, showed none," say Boian Alexandrov at the Center for Nonlinear Studies at Los Alamos National Laboratory in New Mexico...

So the mixed research has not resolved the issue of safety. It is simply deemed to be safe by the interested parties.

For security reasons I get why these devices are being deployed. Death mongering third world zealots want all of us to live in a world of their design. To influence us, the western world, to pull out, go away, devolve, convert, or whatever, they sell their points of view by causing terror events such as blowing things up with people in or near them. They have been successful a few times and, thankfully, failed many more times. They have tried the exploding shoe - so now we take our shoes off. They tried binary liquid chemical (very scary stuff) - so now it's 3 ounces or less (more than enough, by the way). And let's not forget the Christmas Crotch bomber - who we can thank for the opportunity to be submillimeter radiated.

My intuition on new things is to avoid them. I have a wait and see attitude. I would feel much better if the scanners had gone through something similar to a testing procedure that a new medical device would go through, or an LD-50 test used to test the toxicity of a substance. With the many decision makers caught between the complications of technology and the bureaucratic demands for immediate deployment, I can foresee small cumulative failures reinforcing one another into an unintended consequence. Homeland Security and TSA may be working well on this issue, but are they working wisely?

Just think of other technology marvels, such as Windows OS. Rushed into service version after version, without sufficient testing. What passes for quality with Windows OS are field installed program patches. Imagine if these Backscatter devices have the same percentage of issues requiring “patches". It causes one to think of all of the imponderables, which always get resolved in the negative.

I am not concerned for the casual flyer. If there are unintended consequences, I am concerned for those most likely to bear the brunt of the of the radiation emitted by these devices. Think of the airport workers and the airline crews who don’t just go through them once a day, but often several times a day. I'm extremely concerned for the TSA employees who will be standing next to these devices that are going off all day long.

So the editors educated skeptical read on these devices, until educated otherwise, is if you are an occasional flyer, it's probably not a health issue. A frequent flyer, someone who flies more than once per month, it may matter. For the Executive traveler, airport workers and airline crews -- you may want to consider a manual pat down and expect a few less than dignified moments.

For the TSA screener who will do the pat down, be kind to them and wear some cologne with a bikini or Speedo.

4. Technical Issues - The Edges of Technology

A few stories from the headlines have attracted my attention these last few weeks. “New Trojan viruses that reside on computers and send the computers information of to an unknown server - excellent tools for spying on businesses.” “Government web traffic hijacked to Chinese servers.” And an endless parade of vehicles recalled because of *software* issues.

When technology works right, it's great -- but when it goes bad, it's often worse than never having had that technology at all. The failures come from many areas, but all of the failures have common roots. Insufficient testing, and testing done in controlled environments. Testing anywhere outside of the real world environments where the equipment will be expected to perform is not proper testing. While these incidents all are software or computer related, the same failures occur in other systems -- and for the same reason.

As business and technical professionals, we need to think clearly about what we are creating, what it is supposed to be, and how it will be used. We also need to think about how our creations can be misused or improperly used.

As a note, antiviral and malware programs are only effective against 24% of attacks. So right now the game is to the hackers.

Nothing is ever foolproof. Bigger, better, and more sophisticated fools are minted each and every day.

5. Real Stories from the Field - Jury Instructions / The Digital Age

Judges routinely admonish jurors only to consider the evidence presented to them at trial, and not to consider outside information. Do not look at the TV or read the papers. So how is this working in digital age? Not well. There are numerous reports of jurors going online to research and comment on cases which they are hearing.

Surely these instructions were easier to follow in a simpler time. Checking expert testimony required a trip to the library, and viewing the crime scene required physically going there. Today, everything is at the juror’s fingertips -- including satellite and street images of locations where crimes may have occurred.

On the other hand ...

You could post an article or set up web sites that contain content unfavorable to your client, and then drive traffic to the site by buying Google AdWords so that your site will be at the top of any search. Next, you monitor all of the IP addresses of those who visit the site, trace those you can back to the jurors, and use the information to protest the verdict if it goes against you ...

6. Book and Product Reviews - Secretariat

The movie *Secretariat* chronicles the successes and failures of owner Penny Tweedy and "Big Red" (aka Secretariat). In the beginning of the movie Penny is happily ensconced as a suburban Denver housewife in the early 1970's . After her mothers death, Penny is brought back to the horse farm where she had grown up, to settle the affairs of the estate and take care of her father who was slipping into dementia. Penny ends up running the family horse farm and maintaining her fathers racing legacy. She had to fight convention and her family to keep it together, but in the end ... well, those of us over 45 know how it ends, and for those who don't -- I will not spoil the story. As one of the few who actually had the opportunity to see Secretariat run, I found it a very memorable movie. It is beautifully scripted, filmed, and edited.

7. Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2010 by The **LUBRINCO** Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by L. Burke Files (LBFiles@feeinc.com), Gregg Lowney (*Greg@feeinc.com*), and Shaun Hassett (SHassett@lubrinco.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.

- **International asset location and due diligence.**
- **Anti-money laundering, financial fraud, and anti-corruption program development and training.**
- **Risk Assessment and statutorily mandated AML independent examinations and program reviews for financial institutions and gatekeepers.**
- **Investigation and location of missing or concealed assets, related to fraud, theft, and divorce.**
- **Due Diligence to prevent fraud and loss, as well as validate potential business partners, counterparties or potential business acquisition or merger targets. LUBRINCO has significant expertise in performing Due Diligence in China, Central and Eastern Europe, Central and Southern Asia, the offshore financial centers, Latin America, and the Caribbean.**

- **Identification, valuation, and protection of intellectual assets and critical information.**
- **American businesses lose more than $300 billion in revenues annually to competitive intelligence, economic espionage, inappropriate disclosure, and information theft.**
- **LUBRINCO provides private sector consulting access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information.**
- **Implementing an OPSEC program is likely to increase revenues for an at-risk operating group by $75 million.**
- **Protection of executive management, staff, and families.**
- **In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.**
- **When traveling or 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 $25 per year outside of North America.

To sign up to receive a complimentary subscription to ***ÆGIS*** or the ***ÆGIS*** PDF notification list, send an email to subscribe@aegisjournal.com.

To be removed from the subscription list, 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, please send your request to editor@aegisjournal.com and the editors will consider it as the topic for an article in an upcoming issue.

We welcome readers who wish to submit a short article for publication in ÆGIS:

If you would like to submit an article for publication in ***ÆGIS***, please send it as an attachment to an e-mail to editor@aegisjournal.com.

Submission of an article for publishing consideration 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 April 2010 ***ÆGIS*** (© 2010 **LUBRINCO** and FE&E), 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.