



ÆGIS journal

Addressing threats that affect your bottom line

Volume 10 Number 10, October 2007

From the case files of

LUBRINCO

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

1-212-695-1759

and



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

1-480-838-1728

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

This month's features:

- 1. Asset Location and Due Diligence — Watching TJX**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — OPSEC for profit**
- 3. Executive Protection — Jack of all trades?**
- 4. Technical Issues — Global warming and the little ice age**
- 5. Real Stories from the Field — Move it *and* lose it**
- 6. Book and Product Reviews — SpamArrest**
- 7. Subscription/Unsubscription/Copyright Information**

1. Asset Location and Due Diligence — Watching TJX

The interesting thing about the TJX caper is not that TJX lost the credit card data of 96 million consumers (about 29 million MasterCard victims and 65 million Visa victims). The cost, after all, will be picked up by the issuers of the credit cards. The interesting thing is that, from a business perspective, it appears not to have adversely affected TJX. It might matter to customers who become the victims of identity fraud and the banks who have to cover the fraudulent use of credit card numbers, but it has not affected TJX.

Indeed, unless TJX loses lawsuits by banks, it appears to confirm the oft-held (albeit unethical) belief that protective measures are window dressing, and that the minimal amount should be spent on them.

This same less than ethical logic springs up everywhere. We all remember cases where a manufacturer would balance the cost of reimbursing for customers who died as a result of a defective part against the cost of recalling the product. In many cases they opt for the less expensive option of buying off the families of the dead. From a business perspective, this makes sense: If it cost \$100 million to do a recall, and the statistical anticipation is that 3 people might die, then paying \$20 million each to buy a new wife, husband, or child to replace the one that died makes business sense.

Now, sometimes there is justification for bad things happening, particularly in the case of changing technology. It would not be beyond imagination that TJX was, in fact, in compliance with all current standards for protecting customer information, and believed in good faith that they were doing everything they could to protect customer information. If this were the case (though their claim appears reported to be more that everyone else was doing it, too), one would be hard pressed to find fault. To find an equivalent to this, think of cars. If a loved one dies in an accident today because the seat belt design was defective, you would doubtless blame the manufacturer. But the Sports Car Club of America didn't require competing drivers to wear lap belts until 1954, and Ford and Chrysler didn't offer lap belts in front at an option on some models until 1956. Nils Bohlin's lap-and-shoulder belt was introduced by Volvo in 1959, so if the car was your beltless restoration from the '40s or early '50s you shouldn't expect them to have original seat belts.

That said, it is clear that in many cases the letter of the law is not quite the same as the spirit of the law. Some companies have formal ethical standards in place (LUBRINCO does) that take precedence over profit. Some run by

the what-would-your-mother-think-if-she-read-this in-the-paper standard. Others simply opt for profit over principle.

Because of lack of ethics we are saddled with too many onerous laws. We can legislate compliance but not ethics. For example, Sarbanes-Oxley exists not because of poor record keeping, but because of dishonesty, theft, and fraud. When unethical behavior reaches a level too obvious to be ignored, we look for remedy either to the courts or to more onerous legislation.

2. OPSEC, Economic Espionage, and Competitive Intelligence — The economic impact of implementing an OPSEC program

It is a mistake to look at OPSEC as reducing losses. Rather, OPSEC should be looked at as increasing revenues. How does this work?

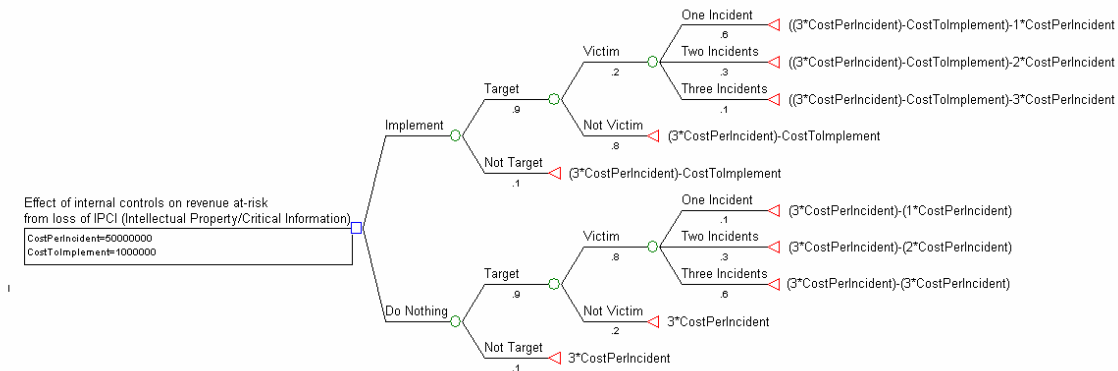
Due to the magnitude of the figures involved, it is a safe assumption that your company is an unknowing contributor to the \$300 billion lost each year to competitive intelligence, economic espionage, and theft. Let's model what this means for a manufacturing company. Keep in mind that the model will apply to each independent division of a multi-national. That is to say that if one division makes automobiles and a second makes electronic goods, each will face losses independent of the other.

Working backwards, we know that the cost of the average loss in a manufacturing environment is \$50 million. We also know that if we encounter one incident we more often than not encounter another two. This puts the theoretical potential loss of revenues at \$150 million. Let us also assume a cost for a fully functional OPSEC program to be \$1 million. This figure is high, but a nice round sum.

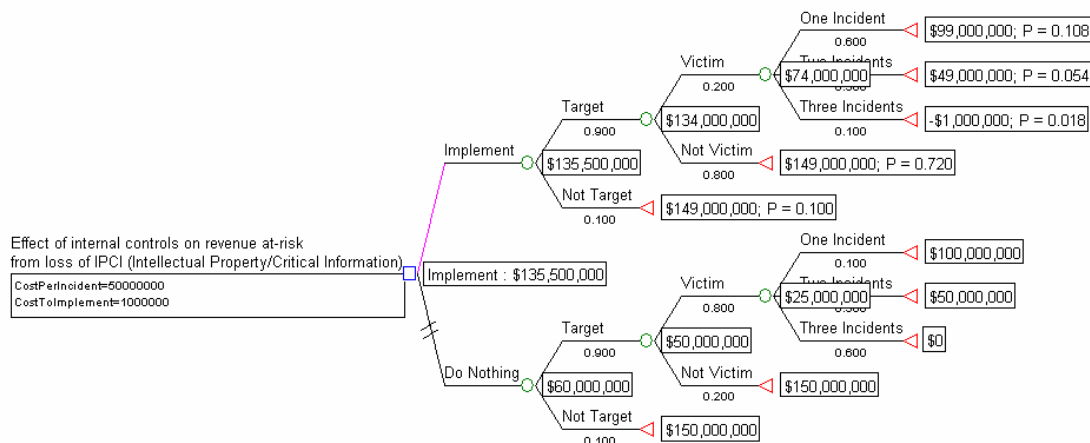
We also assume that a company that has implemented an OPSEC program has a much lower probability of being a victim, and that, if they are a victim, that there will more often than not be only one incident that slips through.

Finally we assume that a company has the choice to implement internal controls or not implement internal controls. Note that the likelihood of being a target is not affected by the presence or absence of an OPSEC program, but that the likelihood of becoming a victim decreases when there are adequate internal controls in place.

Our model might thus look like this:



If we run the model we get the following:



What this shows is that if you have not implemented an OPSEC program your revenues for that operating unit are likely to be \$90 million below where they should be. And that if you have implemented an OPSEC program they are likely to be \$15 million below where they should be.

Looked at from the perspective of revenue, if you implement an OPSEC program your revenues are likely to be, after the cost of the program, \$75.5 million dollars higher than if you chose not to implement.

This model does not account for three factors.

First, it deals with one operating unit. If you have more than one operating unit, each faces the same exposure.

Second, as with most programs, the cost of implementing OPSEC across operating units is not linear. That is to say if you spent X dollars to implement the first program, you now have a lot of expertise and infrastructure in-house, so the second implementation will cost less. This is

as true of implementing an OPSEC program as it is implementing a new accounting system.

Third, since the SEC has said that “the Sarbanes-Oxley Act of 2002 and the Commission’s rules promulgated under the Act seek to strengthen pre-existing standards for internal controls, thereby potentially improving the ability of companies to track the costs and impact of economic espionage and theft of intellectual property,” senior managers face a higher risk if there is a shareholder lawsuit over lost revenues, plus potential SEC follow-up action for noncompliance with SOX if there is a lawsuit. The liability largely disappears if you in fact have the internal controls in place, and this reduction in liability is not reflected in the model.

3. Executive Protection — Jack of all trades?

In the world of protective services there are a wide variety of skill sets available. Some operators are really good at advance work, but you probably don’t want to hand them an MP5 and drop them into a high-threat situation. Others may be equipped to handle a high-threat environment but wouldn’t fit into a social situation. We generally look for a team of specialists that give us a balance of the skills we need.

The exception to this is situations where we have reason to believe the threat to be relatively low, and where the team, for cost (and believed threat) reasons is likely to consist of a single person. In this case the operator will have to fit discreetly into social situations, and the emphasis is likely to be on the ability to do advance work, with medical knowledge being the second consideration. In other somewhat-higher threat situations we still need someone who excels in advance work.

Advance work is where someone actually goes and lays out the groundwork for what needs to be done. If the advance work is done properly, use of time, convenience, and safety will all be maximized. In the best of all possible worlds, advance work will eliminate all variables from the trip – or at least make them known in advance. The cost for advance work seems high to the inexperienced, because you have to send an operator to wherever you will be going, so that they can check things out, and make arrangement in advance.

What is not accounted for by a good advance team? Relatively little, with the amount depending on how well they know the client. Thus, the advance team may know everything about airport construction and street congestion due to maintenance, know where every hospital and police station is, pre-arrange every meeting and meal and shopping trip, have back-up plans in

case of natural disaster or civil disorder. If the client has a sudden whim not in the plans, there may be some detail not examined.

Sometimes clients balk at sending someone overseas to do the advance work at the final destination. When this happens, the advance work relies on past experience and second-hand advice. The smoothness of the operation can be diminished unless you are very lucky. And the function of advance work is to minimize, as much as possible, the effect of luck.

4. Technical Issues — Global warming and the little ice age

By any standard global warming is a serious issue, particularly if you are a polar bear – the harbinger of things to come – whose habitat is rapidly disappearing. There is no doubt in our mind that man’s activities have influenced what is happening.

That said, it is often hard to figure out what happens in nature, and why. As an example, we might look at the little ice age that struck the Earth in the 13th century. While there is disagreement as to when it started, in about 1250 the Atlantic ice pack started to grow, as did glaciers in the formerly-appropriately-named Greenland. In 1300 summers in Europe stopped being predictably warm. This global cooling lasted until the mid 19th century.

Why did the climate cool? If you have a high level of whimsy, a reasonable guess might be man’s intervention, in the form of the invention of the longbow in the 13th century. The less inventive suggest a decrease in solar activity and an increase in volcanic activity.

Others posit a 1500 year climatic cycle, but records going back in 1500 year increments are hard to come by. Indeed even shorter cycles seem to surprise people. Our article on the multi-decadal signals of hurricanes (in the September 2005 issue of *ÆGIS*) seemed to leave many astonished by the fact that hurricanes were at a predicted level of violence.

Does the fact that nature may have a significant hand in what is going on with the climate— perhaps in the form of increased solar activity and decreased volcanic activity – mean we don’t need to do anything? Clearly not. We are doing our share in this, and need to get our house in better ecological order.

5. Real Stories from the Field — Move it *and* lose it

We have seen two cases of late where people were acting stupid in the smart zone while moving from one residence to another.

In the first case someone who was moving left a gun unattended in an unlocked bag. He went in and out many times during the day, and finally noticed that the bag had apparently been inadvertently packed with everything else. Since there were an awful lot of cartons in the moving van, he chose to ignore the missing bag, assuming he would find it when he finally unpacked at this new home.

Eventually the cartons all arrived in his new home. Eventually plus a week or so he started unpacking the cartons. He did find the box in which the bag was packed. The gun, sadly, was not in the bag.

The good news is that the gun has not been reported as having been used in a crime. Yet.

In the second case, someone who was moving had taken money – about \$9,000 – out of the bank. He used a thousand of it to pay various debts, and left the rest in his briefcase. His unlocked briefcase. As with the previous case, he was in and out while movers were in and out, while cable guys were in and out, and while a host of others were in and out.

Eventually the packing was done, and all of his possessions – save his briefcase – were gone from the apartment. When he bothered to look inside the briefcase, he discovered that the remaining \$8,000 was missing.

Now, we would certainly not make a case that movers, or cable repair guys, or anyone else as a class are any more dishonest than, say, CEOs. Indeed, we might even suppose that the chance of your being robbed was not much greater than being struck by lightning while playing golf. That said, the prudent golfer does not walk across the fairway during a thunderstorm while holding his nine iron above his head.

Crimes of opportunity happen because there is opportunity. Just as CEOs rob because they have the opportunity, even so do petty thieves steal because they have the opportunity. If you make the minor effort to reduce the opportunity, you will reduce the likelihood of acting stupid in the smart zone.

6. Book and Product Reviews

SpamArrest

Spam Arrest LLC

\$5.95/month or \$24.95/6 months or 44.95/12 months or 74.95/24 months

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

In the February 2007 issue of *ÆGIS* we discussed ChoiceMail, a PC based e-mail challenge and response system. While ChoiceMail works quite well, it has one problem: Because ChoiceMail downloads your e-mail to the PC, you have no access to our e-mail while traveling. In theory this is no problem for us, because we hate traveling, and make every effort to avoid going anywhere. As often happens, practice doesn't work quite as well as theory, and in the month following the writing of the ChoiceMail review, this editor was on four different continents, traveling to countries as alphabetically and geographically far apart as Argentina and Uzbekistan.

This, and subsequent trips, made it clear that what was needed in our particular circumstances was a Web based challenge and response program. Because of this we have been using SpamArrest for several months now.

The transition was quite smooth. We exported the list of approved e-mail addresses from ChoiceMail and uploaded it to Spam Arrest, and were pretty much in business.

There are some differences between the two programs.

Spam Arrest reads your various e-mail servers (three in this editor's case) every few minutes, and brings the e-mail to its Web space. You can then download your mail to your e-mail client, or look at it on the Web mail portion of Spam Arrest. In our case we first run it through MailWasher (see the June 2002 and May 2003 issues of *ÆGIS*). Once we get rid of valid but unwanted e-mail, we then download it to our e-mail client. Since it all comes in one batch, independent of the e-mail address to which it was sent, we built filters in our e-mail client, The Bat! (see the January 2005 and July 2006 issue of *ÆGIS*), to direct it to the appropriate mailbox. The few on which we were BCCd stay in the Spam Arrest mailbox until we drag them to the appropriate mailbox.

Filtering on Spam Arrest is more simplistic than on ChoiceMail (or The Bat!, for that matter). Each filter handles one condition, rather than many. You get 20 filters thrown in for your monthly fee. Since you are really relying on the challenge and response system, this is interesting, but not really an issue.

We tend to look at the unverified e-mail periodically, just to make sure there is nothing we want. The best way to do this in SpamArrest seems to be to hide all messages with bounced verifications – surely spam – and scroll through page by page until the bold listings turn to un-bold listings, indicating they have been previously seen.

One of the nice features of ChoiceMail was that if you sent someone an e-mail, that address would automatically go into the approved list. This doesn't happen with Spam Arrest, so you have to remember to do this manually, or catch the response in the unverified list if the person does not respond to the challenge sent them by Spam Arrest.

We have been quite pleased with Spam Arrest. If a local system such as ChoiceMail does not serve your purposes, then Spam Arrest is a good choice.

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 Philips (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.**
 - American businesses lose \$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.
- **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, anti-money laundering, and anti-corruption program development and training.
- **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, 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, 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 October 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.