



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 7 Number 11, November 2004

From the case files of

The LUBRINCO Group
<http://www.lubrinco.com/>

and

Financial Examinations and Evaluations, Inc.
<http://www.feeinc.com/>

Due diligence outside North America and Western Europe? Call us!

This month's features:

• **Special Announcement**

1. **Due Diligence — Do Christians suffer more from leprosy than do Muslims and Jews?**
2. **OPSEC, Economic Espionage, and Competitive Intelligence — Sarbanes-Oxley and corporate OPSEC programs**
3. **Executive Protection — Flu!**
4. **Technical Issues — Agnitum Outpost Firewall Pro**
5. **Real Stories from the Field — Pepper Sprays: Fourth Amendment to Eighth...**
6. **Book and Product Reviews — *Taking Sex Differences Seriously***
7. **Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Do Christians suffer more from leprosy than do Muslims and Jews?

We in the business world can gain a lot from the study of religion. For example, we all know that Muslims don't eat pork. The question is, why? The answer is that Muslims don't eat pork because Jews don't eat pork. We know – as much as we can know anything about religious figures of undocumentable historicity like Moses and Jesus and Mohammad – that Mohammad's first wife was Jewish, and some have posited that, like Jesus, the Prophet himself was Jewish, which may explain, for some, why Mohammad originally prayed toward Jerusalem, not Mecca.

The next logical question to ask is, of course, why Jews don't eat pork? The answer is that prior to the Exodus the biblical Jews came from Egypt, where the Pharonic priests believed that pigs carried leprosy. Because of this, Egypt got rid of both swine and swineherds (they attempted to replace pigs with the domestication of hyenas, which didn't work out, but that is a different story....). As it happens, while armadillos carry Hansen's disease, pigs don't. This means that about a third of the world doesn't eat pork, for reasons may have been reasonable to people who believed the world was flat, but that don't really stand up to the light of contemporary science.

As an interesting historical side note, Christianity, more influenced in the time of Constantine by the Mediterranean than the Mid-East, suffered from no such misconception, and did not disallow the consumption of pork. Even so, Mediterranean Christians used olive oil rather than butter because they thought butter carried leprosy. Although the Church did not see fit to institutionalize this as part of the religion itself, you should, germ theory or no, still expect to get a dish of olive oil, rather than butter, when you go to many Italian and Greek restaurants.

What can we bring to business from this? Mostly we should learn not to confuse faith, conviction, tradition, and sincerity with correctness. Knowledge evolves, and, short term or long term, when exercising due diligence we should constantly question our every belief and assumption, in case they turn out to be wrong.

An obvious corollary is that appropriate exercise of due diligence means that we should always actively seek dissenting views, in case our underlying

assumptions are wrong. The fact is that if our understanding of the causes of a problem is wrong, our solution will also be wrong, and the measures we take to solve the problem may well make things worse. As H. L. Mencken put it, “For every complex problem, there is a solution that is simple, neat, and wrong.”

Closely related to faith is trust. Faith exist absent facts, trust exist absent proof, thus we should learn that the exercise of due diligence should not be cut short just because of our assumptions of trust. As an example, theft of critical information is almost always done by people you trust. There is a natural tendency to want to avoid investigating those we trust, and a suspicion of those who are willing to do so. This explains why members of internal affairs departments in law enforcement agencies, and those who look for moles in intelligence agencies, are often despised by the rest of their professional community.

Finally, we should not assume that problems we encounter are unique problems, rather than systemic problems. It was a systemic problem that led to the series of failures and bad decisions that allowed the shortage of flu vaccine this year. Not that unique problems don't occasionally occur. As an example, some time ago a supermarket chain had a number of fires in its warehouses. It was prudently assumed that there was some sort of systemic problem with fire safety, and appropriate measures were taken throughout the warehouses. As it turned out, organized crime was trying to shake down the company, but the extortion requests were not making it to senior management.

Oh, and no, we checked, and it appears that Christians *don't* suffer more from leprosy than do Muslims or Jews.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Sarbanes-Oxley and corporate OPSEC programs

The SEC, in a letter dated 5 August 2004, said “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.” This view was not anticipated by most companies, and has produced confusion as to what is required.

It appears clear from this letter that companies, independent of their size, now have a *requirement* under Sarbanes-Oxley to have a system in place – the “existing standards” which we rarely encounter in any company – to deal

with competitive intelligence and economic espionage, two primary sources of loss of critical information!

Confusion regarding this area is not surprising when one considers how completely this area has been neglected by the business community. Anti-espionage is not considered a mainstream business activity. You would be hard-pressed to find a corporation where a senior executive is tasked with the identification and protection of critical information from competitive intelligence and economic espionage. You would be hard-pressed to find any business school that deals with the issue. You would be equally hard-pressed to find a major consulting company with any anti-espionage experience. Very few people in academia, business, or consulting have ever heard of OPSEC.

Equally astonishing, even though there is an entire government agency (the Interagency OPSEC Support Staff, <http://www.iooss.gov/>), whose sole charge includes promulgating OPSEC, many former FBI and Secret Service folk hired as directors of security for major corporations are generally unaware of its this discipline. This is due to a combination of cultural approaches and considerations, not the least of which is that OPSRC includes systems analysis and planning, two traits rarely understood in the physical security community.

Based on the SEC letter, it appears that companies need to establish their own protocols to apply OPSEC analysis and planning within their companies. When your company finally takes the plunge into OPSEC, what should you expect? For a start, the disruption and cost of implementing an OPSEC program will be trivial compared with any other area of Sarbanes-Oxley compliance. In addition, an OPSEC program goes well beyond protecting the shareholder: It reduces the likelihood, costs, and repercussions of losses from competitive intelligence and economic espionage, so you can create an economic gain, rather than with a mere compliance cost.

Another benefit is that implementation of an effective OPSEC program can be done in stages. Although the process is not trivial – our custom-developed checklist is over 50 pages long – the concept is simple. A lot of what needs to be done comes with education, awareness, and making smarter decisions and small changes. Compare this to the costly technical investments needed to implement network security and information security programs.

Management buyin and executive training

First we start with training senior management and their staff, so that they understand the risks, the OPSEC process, and benefits. Once senior

management has bought into the process – and it will not otherwise work – we can work with your people to implement a program on the corporate level. This is usually quite straightforward, as the exposure here is less than lower down the corporate food chain.

Procedural and educational training

Once there is management buy-in, we work to help the company develop an in-house procedural and educational program, which comes in two parts. The first part is awareness training. If people are conscious of risks that can cost them their jobs, they tend to take things more personally, and will talk about the work with people who have some need to know, and be more restrained with those who don't really need to know. Nearly all areas of the company need this information. One of the most often overlooked communities in an organization is the administrative or secretarial staff. These people handle nearly every document and travel schedule. If you want to understand where the boss spends his time and what the relationships are between the company and external entities, check out the secretarial pool.

The second part is the development of procedures and forms to assure employees, subcontractors, partners, OEMs, and associates, formally sign off that they understand what they are allowed to do and not do. And that when they are no longer associated they sign off on this again as part of their exit from the organization or project. These procedures also affect subcontractors, joint-venture partners, suppliers, and everyone else with whom you have relationships.

OPSEC audit and implementation of vulnerability reduction

We then work together to audit the specific threats and vulnerabilities that exist within the various parts of the company, as well as the impact from possible losses. From these, the risk level can be calculated, and a management decision made as to what countermeasures should be put in place. This largely falls to middle management, who most intimately understand the processes, some of the real threats, and many of the vulnerabilities. With a little focused training, they can make a reasonable decision as to where scarce dollars should be spent to most effectively minimize risk.

Ongoing audit and change

Threats and vulnerabilities change as business changes, and it is important that regular reviews be done to make sure that countermeasures are still appropriate in our dynamic world. By doing so, we can maximize our scarce resources, and minimize our ongoing exposure and loss.

While some are irked by the fact that Sarbanes-Oxley has forced them to do many new things, OPSEC will turn out to be the least painful, the least costly to implement, and the most likely to increase your bottom line.

3. Executive Protection — Flu!

We spend a lot of time concerned with protecting from events so unlikely that we will read about them on the front page if they do occur. It is also necessary to prevent likely events, which explains our dogged concern with driving safety and health issues.

One issue that looms large in this season is the flu. This is because, in the United States alone, roughly 36,000 die of the flu in an average year, and roughly 200,000 will be hospitalized. This makes the flu a very real threat under the best of circumstances. This year, when vaccine will be scarce because of the unavailability of the vaccine from our major supplier's factory in the UK, it could be an even more serious threat. Those on the priority list include:

- All children aged 6-23 months.
- Adults aged 65 years and older.
- Persons aged 2-64 years with underlying chronic medical conditions.
- All women who will be pregnant during the influenza season.
- Residents of nursing homes and long-term care facilities.
- Children aged 6 months-18 years on chronic aspirin therapy.
- Health-care workers involved in direct patient care.
- Out-of-home caregivers with household contacts with children age of 6 months or under.

If you, or those under your care, fall into any of these categories, you, and they, should definitely get a flu shot.

And, flu shot or not, it is certainly the season to stop shaking hands; stop touching your face (especially your nose); and to frequently wash your

hands throughout the day with lots of soap and friction, paying especial attention to the tips of the fingers and the cuticles. These three simple measures can cut the probability of your contacting the flu by half!

4. Technical Issues — Agnitum Outpost Firewall Pro

We have mentioned on many occasions the necessity of having a firewall, particularly if you have a broadband connection to the Internet. We recently got a recommendation from Nick Bolton, creator of the highly recommended MailWasher (<http://www.lubrinco.com/ejournal/ej200206.pdf>, <http://www.lubrinco.com/ejournal/ej200305.pdf>) and Benign (<http://www.lubrinco.com/ejournal/ej200309.pdf>), for Outpost Firewall Pro from Agnitum (<http://www.agnitum.com/products/outpost/>).

Outpost has all three of the qualities that *we* think make for a good firewall.

- It is effective. Agnitum notes that “Outpost filters all the network activity on your system and makes sure no dangerous data enters or leaves your PC.”
- When installed by the naïve user it is simple to use. It can pre-configure itself for many applications – and this should be your choice unless you are a sophisticated user – and when new applications try to access the Internet it gives you simple guidance. Agnitum notes that Outpost automatically blocks spyware, cookies, and referrers that trace your surfing habits, as well as online advertisements, and that it repels all known types of hacker attacks, and protects from mail worms and viruses and blocks Trojans. There is a quick-start manual for the beginner at [http://www.agnitum.com/download/Outpost_Pro_Getting_Started_\(ENG\).pdf](http://www.agnitum.com/download/Outpost_Pro_Getting_Started_(ENG).pdf).
- For the sophisticated user, Outpost allows significant control and oversight, and includes a host of useful features that can be implemented, or not, depending on your needs. There is an in-depth, detailed manual at [http://www.agnitum.com/download/Outpost_Pro_User_Guide_\(ENG\).pdf](http://www.agnitum.com/download/Outpost_Pro_User_Guide_(ENG).pdf). There is a support forum at <http://www.outpostfirewall.com/forum/>. And a guide to producing a secure configuration for Outpost, written and maintained by one of the forum moderators, at <http://www.outpostfirewall.com/forum/attachment.php?attachmentid=2404>

The one oversight we noticed was that in Version 2.5 we couldn't make Benign work. The problem was fixed at the advice of the Firetrust folks: To get Benign working with Outpost 2.5, under default policy setting of 'Rules Wizard' mode click Options >> System >> LAN Settings >> add '127.98.9.*' as a trusted IP. This will make sense if you need it...

The price for a single home user is a modest \$39.95, and there are various family and small-business plans, with a 25-user license going for \$800. We assume there are appropriate corporate discounts. If you already have a firewall, they will give you a fifty percent discount to migrate!

If you are looking for a firewall, Outpost merits your serious consideration.

5. Real Stories from the Field — Pepper Sprays: Fourth Amendment to Eighth...

Recently we were asked if we might consider being an expert witness in a trial involving police officers swabbing liquid from a pepper-based personal defense spray into the eyes of protesters. It appears the protesters had illegally chained themselves in inconvenient places, and were blocking legal entry and exit.

In some jurisdictions the police would reroute traffic, block off the protesters so they couldn't get hurt, and leave them until they wanted to leave, something that often starts to happen when it gets cold, or when the protesters need to pee.

In other jurisdictions the police would simply cut the chains or pipes (the chains are often put in pipes to make access to the locks difficult).

In this jurisdiction officers apparently gave the protesters the opportunity to leave, then, in this case, clinically put the inflammatory liquid in their eyes in order to cause enough pain to induce them to leave. While we have not read the depositions – the judge apparently decided not to allow the expert testimony – it is our impression that the feeling was that the protesters had been given several warnings, and that the time for diplomacy had ended, and that action needed to be taken.

While nobody can doubt that the action taken was certainly better than wiring their genitals to a battery, or sticking a plunger up their butts, there was still some feeling – at least on the part of those whose eyes participated in this experiment – that this set of actions was not *reasonable* under the Fourth Amendment.

Because we were the ones who introduced pepper based sprays to the law enforcement community at the 1988 ASLET (American Society for Law Enforcement Trainers) conference, and are therefore indirectly responsible for its use in this – and every other – case, it seems appropriate for *us* to comment on the use of these products.

It was our intention, both with the introduction of the original product at the 1988 ASLET conference, and the introduction of training in use of personal

defense sprays for line officers at the 1989 ASLET conference, to extend the range of options available to officers under the Fourth Amendment. While teargas and riot gas had traditionally been used at the same level of force as impact weapons, Aerosol Subject Restraints – ASRs, as capsaicin-based sprays came to be known (the term was coined by William J. “Doc” McCarthy of Indianapolis) were accepted as being usable at below the level of hard empty-hand control. That is to say, officers could use them before they actually hit the person.

The reason for this is that tear gas and riot gas are *irritants* that work by causing pain. While this makes them good for crowd control (you want to have people move away from the discomfort) they are, by definition, not very effective for controlling pain-resistant subjects, who – again by definition – didn’t feel pain. Keep in mind that people can be pain resistant because they are drunk, or on drugs, or really angry, or crazy. These are the categories of people most likely to be fighting cops in the first place.

ASRs, on the other hand, are inflammatory agents. When the atomized liquid is inhaled, it inflames the capillaries of the mucous membranes in the throat, doubling the person over with uncontrollable coughing (which makes capsaicin-based products inappropriate for crowd control). It doesn’t matter whether the person is pain-sensitive or pain-resistant: Inflammation at a capillary level is not a voluntary action. The object of the game is to take a physically resistant, generally pain-resistant, subject and restrain them so that neither they, nor the officer, will get hurt.

As it happens, when an ASR is sprayed directly on the skin (as opposed to being breathed out of the air), rapid inflammation of tissues causes dermal discomfort in pain-sensitive people, but this discomfort is an unfortunate artifact of the inflammation, and not a control factor. Indeed, during training, the *ASR Instructors Council* recommends that trainees’ exposed skin be slathered with some protective agent, such as *Derma Shield* or *Derma Plus* (<http://www.dermashieldusa.com/>, <http://www.dermashield.co.uk/>), which will prevent any dermal discomfort, and thus simulate pain-resistance on the part of the officer being trained.

When protesters, expressing civil disobedience, chain themselves, they have some expectation that they will be arrested and, possibly, punished by the judicial system. However, they expect that this arrest and punishment will take place within the constraints of the Fourth Amendment, which mandates *reasonable* search and seizure.

The question, then, becomes one of whether taking protesters – who are exercising non-violent civil disobedience and who are arguably causing inconvenience, but no real danger – and dropping an inflammatory agent in their eyes to cause discomfort, rather than to restrain – they are already chained and self-restrained – remains in the realm of reasonable seizure, or does it now become cruel and unusual punishment, which is precluded by the Eighth Amendment. Having been sprayed in training and in testing more times than any sane person would willingly admit, we think it falls into the area of cruel and unusual punishment.

It is up to supervisors to make sure this doesn't happen. While it may have seemed a good idea a good idea to someone to save time by dropping an inflammatory liquid in the eyes of the protesters, a lot more time has been and will be spent in court than was saved.

Several thousand years of diplomatic experience indicates that hasty actions can save a little time up front, and be, short term, *extremely* emotionally satisfying, but are likely to cost a lot in time and money (and careers) on the back end. We therefore suggest that, given the choice, spending a *little* annoying time up front in diplomatic negotiation is almost always better than spending a *lot* of time and money at the back end.

This is as true for hasty business actions by representatives of the company as it is for government agencies acting under color of law.

6. Book and Product Reviews

Taking Sex Differences Seriously

Steven E. Rhoads

Encounter Books ISBN: 1-893554-93-7 240 pages \$25.95

<http://www.encounterbooks.com/> 1-415-538-1460

On very *very* rare occasion we come across a book such extraordinary contemporary social significance that we feel it must be read by virtually everyone we know. One such book was *Beyond Fear*, by Bruce Schneier (<http://www.lubrinco.com/ejournal/ej200309.pdf>), where we noted that, “If you could only read one book about security, the book you should read is *Beyond Fear*.”

Taking Sex Differences Seriously falls into this same category, and we believe it should be read by every policy maker.

Sex permeates all human existence, affecting social structure, religion, civil life, criminology, and the world of business. It is, for most, an area of much fascination and little knowledge.

As chance would have it, this editor's area of study, when getting his Masters, was sex, and therefore some of the researchers – and some of the research – discussed in the book are known personally.

Rhoad's book "argues that sex differences are large, deeply rooted and consequential. Men and women still have different natures, and, generally speaking, different preferences, talents and interests. The book presents evidence that these differences can be explained in part by hormones and other physiological and chemical distinctions between men and women. Thus they won't disappear unless we tinker with our fundamental biological natures."

Now, the idea that men and women are inherently different may not seem too outlandish to anyone who has seen a member of the opposite sex close up. Until you remember that much feminist theory, and much social policy, is based on the assumption that the differences between men and women are largely caused by socialization rather than biology. The author makes a compelling contrary case to for this former worker in the field.

Assuming you accept his premise, the next question you ask should reasonably be "so what?"

The "so what" comes when you consider any interaction whatsoever between men and women.

- If you have a daughter, and would like her to grow up to be as happy and contributive as possible, this book will give you some insights that will help you guide her through the contemporary world.
- If you have a son, and would like him to grow up to be as happy and contributive as possible, this book will give you some insights that will help you guide him through the contemporary world.
- If you were a coach, and trying to produce a set of competitive Title IX teams for your school, this book will help you understand the different playing styles and approaches to sports with which you will have to deal.
- If you are a principal trying to put together a zero-tolerance policy against violence, this book will help you understand the problems you will encounter.

- If you are considering divorce, this book will help you understand some of the foreseeable implications for your children if you do, and your future level of happiness if you don't.
- If you are interested in crime, this book will give you the most reliable demographic predictor for youth violence.
- If you are concerned with inner city pregnancy, this book will give you an insight into some of the problems that are faced.
- If you run a company, and want to develop the most appropriate child-care policies, this book will give you an idea of the complexities of the issues, which are still not clear in the research.
- If you run a company, and want to provide gender-neutral advancement, this book will help you see the landmines ahead.
- If you run a police department or an army, and want to have equal representation by women, you will gain insights from this book.
- If you are a boy and want to maximize your dating success – or your ultimate happiness in life – this book will help you achieve your goal.
- If you are a girl, overwhelmed by predatory sexual pressures, this book will give you social strategies and goals.
- If you are trying to understand the role of women in other cultures, this book will give you cross-cultural insights.
- If you don't understand how members of the opposite sex think, this book will help a little.
- If you want to have a long and happy marriage, this book may well give you some clues.

The bottom line is that men and women appear to have some fundamental differences. While these differences range along a spectrum (due more, we suspect, to *in utero* testosterone levels than to socialization), rather than being sharply defined, they are nonetheless there. Behaving as if women are merely men who can give birth and lactate, and men are merely women who can't, may create a good gender feminist (as opposed to equity feminist) but a bad social policy maker and planner.

Because of its wide range of application, as well as its break from the more-commonly held approach to the role of socialization in *gender* differences, we consider this book to be critically important, and a must-read for any policy maker.

7. Free-Subscription/Unsubscription/Copyright Information

•• AEGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2004 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@lubrinco.com).

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

- **OPSEC: The identification and protection of information that would give your competitors and adversaries an advantage.**
 - Sarbanes-Oxley compliance.
 - Protection of trade secrets and intellectual assets.
 - ◆ Anti-competitive intelligence.
 - ◆ Anti-economic espionage.
- **International financial investigations and due diligence consulting.**
 - Location and recovery of missing and hidden assets.
 - Establishing business relationships and strategic partnerships in Central and Eastern Europe, the offshore financial centers, Beijing and Shanghai, Central Asia, and Latin America and the Caribbean.
 - Anti-money laundering and financial fraud requirements under the *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 **The LUBRINCO Group** and its services, or for the archive of all past issues of *ÆGIS* e-journal in PDF format, please go to <http://www.lubrinco.com/>.

To sign up for a **complimentary subscription** to *ÆGIS* e-journal or the *ÆGIS* e-journal PDF notification list, go to <http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to ejournal@lubrinco.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 ejournal@lubrinco.com.

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

If there is a topic that you would like to know more about, send it to ejournal@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* e-journal, send it as an attachment to an e-mail to ejournal@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* e-journal constitutes a license to The LUBRINCO Group Ltd, Inc., 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* e-journal, you may do so freely as long as appropriate source, copyright, accreditation, and link to the LUBRINCO website is included. This should be in the form

Article Title, from the November 2004 *ÆGIS* e-journal (© 2004 LUBRINCO & FEE), to be found at <http://www.lubrinco.com/>.

ÆGIS e-journal 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* e-journal 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* e-journal.

Please be safe, and be smart.