



**ÆGIS** e-journal

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

Volume 7 Number 5, May 2004

From the case files of

**The LUBRINCO Group**

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

and

**Financial Examinations and Evaluations, Inc.**

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

**Business in Bogotá or other high-threat areas? Call us!**

### **This month's features:**

- **Special Announcement**

1. **Due Diligence** — New regulations regarding internal controls
2. **OPSEC, Economic Espionage, and Competitive Intelligence** —  
**The National OPSEC Conference and Exhibition**
3. **Executive Protection** — Piracy update
4. **Technical Issues** — Communications in a suspicious society
5. **Real Stories from the Field** — But the numbers looked good...
6. **Book and Product Reviews** — *Glitter & Greed : The Secret World of the Diamond Cartel* || *Guns, Germs, and Steel: The Fates of Human Societies* || *World on Fire: How Exporting Free Market Democracy Breeds Ethnic Hatred and Global Instability* || *All You Need Is Love, and Other Lies about Marriage*
7. **Free-Subscription/Unsubscription/Copyright Information**

**Read *How Not to Tell All* by Richard Isaacs in the May 2004 issue of *Security Management***

**L. Burke Files will be speaking at the  
2nd Annual International-Caribbean Offshore Business Convention  
10 June 2004, Dominica**

<http://www.samuelgroup.com/cprmg/offshore-convention.html>

## **1. Due Diligence — New regulations regarding internal controls**

The SEC is in the process of adopting further rules on accounting and the role accounting firms will be required to play in the near future. The most significant of these rules is that auditing firms must conduct an in-depth review of the firm's internal controls. This is a significant change, and no doubt reflects the consequences of the sins of Enron.

It is estimated that this new requirement will drive auditing costs up another 25 to 35 percent. This is over and above the Sarbanes Oxley reforms which more-than-doubled auditing cost. These reforms will not only require a review of all of the corporate controls on both booking assets and recognizing revenue and expenses, but also on related "significant" matters.

These related matters can only mean a further step toward the European listing requirement of full risk disclosure. (This should not be a surprise, as the U.S. and the EU have been working towards a "harmonized" accounting standard for many years.) The process of full risk disclosure is one whereby the risks – system, market, internal, obsolescence, litigation, intellectual property, et cetera – are thoroughly reviewed, discussed, and addressed in a detailed narrative fashion for disclosure.

It is also likely that the new disclosure and review forced on U.S. companies will likely be internally governed by a new board of directors committee on risks and controls that will be independent of the audit committee. The outside members of this committee will need to come to the committee with real risk assessment and management experience. Specific business knowledge will come from the company members of the committee.

Increasing regulation on *all* firms is a knee jerk reaction to the unconscionable behavior of a few major firms. An anticipated consequence of the increased regulation and supervision requirements on accounting firms is a further reduction in the number of firms that conduct public company audits. According to industry insiders, the number of firms qualifying for public company audits has been reduced by 67% through recent legislation. Increased regulation has simultaneously increased the cost of compliance, and reduced those able and willing to perform the required services.

Another effect of increased regulation of *all* firms will be that many smaller public companies will see the cost of being a public company rise exponentially. What had been an expense of ten to twenty thousand dollars may now cost fifty to sixty thousand dollars. That is if they can find a firm that will take them on. In consequence, many smaller companies will be looking to reduce, defer, or share this expense. This is an environment that is ripe for fraudsters plucking up a few public companies here or there and fleecing them. Expected methods of fleecing will be mergers, “privatization” deals, and “international listing.”

Another consequence is that while a company may be eligible for public trading, it will choose to de-list, that is remove itself voluntarily from having its shares publicly traded. This is the worst of both worlds for the shareholder. The value of the shares decreases dramatically since there is less transparency in the company’s matters. There is no liquidity in the shares, since they are no longer traded and many shareholders will end up as minority shareholders in an illiquid investment in a company that no longer has any reporting requirements. We have seen this many times, and the companies most often get fleeced by the senior management, and the shareholders get a worthless piece of pretty paper.

In judging any policy or measure, five questions must be asked:

1. What problem is the policy or measure trying to solve?
2. How can it fail in practice?
3. Given the failure modes, how well does it solve the problem?
4. What are the costs, both financial and social, associated with it, and flowing from its unintended consequences?
5. Given the effectiveness and costs, is the policy or measure worth it?

Clearly, nobody wants a repeat of an Enron or a Tyco or a WorldCom. And those of us not actually making hundreds of millions of dollars would like to see some restraint of greed. Nonetheless, we leave it to the reader to evaluate the prudence or imprudence of the new legislation according to the above five questions. Meanwhile, we suggest you be very careful when purchasing shares in a small-company. You may own them forever

## 2. OPSEC, Economic Espionage, and Competitive Intelligence — The National OPSEC Conference and Exhibition

The annual national OPSEC security conference and exhibition, sponsored by the Interagency OPSEC Support Staff (IOSS) in association with the OPSEC Professionals Society (OPS) is being held this year in Baltimore, Maryland from June 6<sup>th</sup> through June 11<sup>th</sup>.

The OPSEC conference is the premier gathering of those whose expertise is the identification and protection of critical information. If you are concerned about the protection of your proprietary information, or protection from economic espionage, you ought to go (or send someone) to this conference. We have attached the provisional schedule, and urge you go: At \$385 – and including a few lunches – it is the informational bargain of the year. The conference registration information is to be found at <https://www.iaevents.com/NatOpsec04/newinfo.cfm>. For those who wish to become members of the OPSEC Professionals Society, an application can be found at <http://www.opsec.org/memberapp.html>.

### Conference and Exhibition Schedule

*(subject to change)*

Sunday, 6 June 2004						
1500-1900	Registration and Social					
Monday, 7 June 2004						
0700	Registration Open					
0700-1700	Exhibits open					
0800-0930	D*I*C*E “Now More Than Ever”					
0930-0945	Exhibits Break					
0930-1130	Hidden Universes of Information on the Internet	OPSE 1300 for DHS	OPSE 1300 for DOD	Overview of CI Threat in the U.S.	Protecting Tomorrow's Warfighting Systems Today	No Session
1130-1230	Luncheon Speaker – “Violence in the Workplace Protecting Our People in Changing Times”					

1230-1300	Exhibits Break					
1300-1700	Hidden Universes of Information on the Internet <i>continues</i>	OPSE 1300 for DHS <i>continues</i>	OPSE 1300 for DOD <i>continues</i>	Overview of CI Threat in the U.S. <i>continues</i>	Protecting Tomorrow's Warfighting Systems Today <i>continues</i>	Designing Awareness Training Workshop

<b>Tuesday, 8 June 2004</b>						
0700-1700	Registration & Exhibits Open					
0800-0815	Opening Remarks					
0815-0900	Opening Keynote Speaker					
0915-1015	How Legislators Contribute to the War on Terrorism	OSD Vision for OPSEC	Homeland Security	History of OPSEC		
1030-1130	Defense Cyber Crime Center	DOD OPSEC Support Elements	DHS OPSEC Program	Teaching Security to the Scientific Community		
11:45-1330	National OPSEC Awards Presentation and Luncheon					
1345-1515	Hierarchy of OPSEC	Homeland Security	Through the Eyes of OPSEC	Army Approach to Research Protection	OPSEC Award Program Panel Discussion	
1530-1700	Homeland Security	Commercial OPSEC	Navy and Marines	Army	Air Force	Joint Commands

**Wednesday, 9 June 2004**  
Breakout Sessions

0800-0900	Keynote Presentation: "Dawn Over Baghdad"					
	Threat	DoD	Public Safety	Homeland Security	Shared	IA
0915-1045	In Harm's Way	1 <sup>st</sup> IO	Applying OPSEC to Fire and Police Special Operations	DHS Speaker (TBD)	Legacy Speakers	Guerillas in the Net
1100-1200	Catching al-Qaida: Operational Methodology Assessment & Security Implications	Air Force Efforts in OPSEC Lessons Learned	Applying OPSEC to Criminal Investigations	(Intentionally left blank)	Information Operations	Solutions to Analytical Risk Management
1200-1330	<b>LUNCH:</b> <i>Special Keynote Speaker</i>					
1345-1445	Threat to U.S. Information Systems	Applying OPSEC to Force Protection	Domestic Terrorism: A National Overview	(Intentionally left blank)	OPSEC Planning for Military Operations	Have We Bugged Our Own Offices?
1500-1600	Understanding the Holy War Mentality: Perspectives from Within	Do You Feel Lucky? Open source, the wild card of the modern battlefield	Spies Vs. The U.S.	Infrastructure Vulnerabilities	Freedom of Information Act: Curse or Cure for OPSEC?	Have We Bugged Our Own Offices?

**Thursday, 10 June 2004**

Breakout Sessions

0800-0900	Keynote Presentation: “The <i>Other</i> Force Protection”					
	Threat	DoD	Public Safety	Homeland Security	Shared	IA
0915-1030	Threat to U.S. Information Systems	Do You Feel Lucky? Open source, the wild card of the modern battlefield	Domestic Terrorism: A National Overview	Infrastructure Vulnerabilities	Freedom of Information Act: Curse or Cure for OPSEC?	Have We Bugged Our Own Offices?
1030-1130	Understanding the American Holy War Mentality: Perspectives from Within	Applying OPSEC to Force Protection	Spies Vs. The U.S.	(Intentionally left blank)	OPSEC Planning for Military Operations	
1130-1300	<b>Lunch</b> “ <i>Was God on Vacation? – Memoir of a Holocaust Survivor</i> ”					
1315-1415	Catching al-Qaida: Operational Methodology Assessment & Security Implications	Air Force Efforts in OPSEC Lessons Learned	Applying OPSEC to Criminal Investigations	(Intentionally left blank)	Information Operations	Solutions to Analytical Risk Management
1430-1600	In Harm’s Way	1 <sup>st</sup> IO	Applying OPSEC to Fire and Police Special Operations	DHS Speaker (TBD)	Legacy Speakers	Guerillas in the Net

Friday, 11 June 2004 Workshops					
0800-1000	Designing Awareness Training	Identity Theft	Personal Computer OPSEC	OPSEC Applied to Program Protection Planning	Motivation Through Communication
1015-1200		Personal Opsec			

### 3. Executive Protection — Piracy update

It is coming up on vacation time, so let's talk about the mix of executive protection and sailing. For those who missed it, you might want to go back and look at the April 1999 issue of *ÆGIS*, and our article on piracy, before looking at this update.

In December of 2001, sailing champion Peter Blake was shot and killed by pirates near the mouth of the Amazon. In the summer of 2002 a group of clients exploring the Caribbean just barely averted being boarded (and ???) just north of Isla Margarita, and west of Grenada. In late fall of 2003, a dear friend was robbed while sailing from Chicago to Mackinac Island. Because of all of this activity, we have spoken with several seasoned sail- and pleasure-boat captains who have designed their cruises to be prepared for pirates. This is a distillation of the questions asked and answers received.

#### ***When do pirates attack?***

When you are vulnerable. They attack when you are at anchor and asleep, or when you are underway at night, and almost always approach from the rear when underway. They prefer the stealth of night, quiet rows out to boats at anchor, or muffled high-speed boats to approach in your wake and out of your running-lights area of illumination.

#### ***Should you have weapons?***

Yes, but it gets dicey when you come into port. The rules on weapons vary from place to place. In some places you have to declare the weapons, others disable them, and others still require them to be surrendered until departure,

or are banned completely. Check before you go. Some carry one weapon to be declared and have others well hidden. Some just don't come into harbor on the boat with the weapons: They use a dingy, or hire a local tender, to take them to and fro.

### ***What can the small craft owner do about pirates?***

These suggestions are for small boats targeted by local criminals engaging in crimes of opportunity. They are not meant for large ships that might be victimized by organized criminals who have pre-planned their attack, nor against, say, heavily-armed drug dealers intending to capture a small boat.

- Listen to the local radio channels and talk to the local provisioners and sailors about reports of piracy. They are the best source of information. In some countries, the police themselves are sources of information about you to the criminals.
- Make your boat a harder target. When at anchor, position a watch and have lights that are activated by motion above a certain height. Motion detectors are not always effective, especially in rough weather conditions, but when they do work they can help.
- Some innovators run electrical fence wire around the perimeter of the boat and charge it when they go to sleep. It draws little or no current until someone completes the circuit. The operation we saw ran two small dual strands, and we can attest to the sound potential boarders make when they touch it. Oh, yeah, turn it off when you're hosting the cocktail party!
- Another idea was to prepare a matt of tacks that can be laid on the deck at night and rolled up in the morning. Many locals go barefoot.
- When running at night keep an aft light to illuminate your wake.
- If you can, invest in a small water cannon for the rear of the ship. A strong stream of water can keep pirates from boarding, and does not often draw retaliation from small arms.

But most of all, think about what you are going to do, and be prepared. The world, including our seas, our oceans, and our lakes are getting a bit rougher.

### **4. Technical Issues — Communications in a suspicious society**

Security of communications is a concern in protective services, as in many other areas. As your information become more open to the government, this can be an area that is fraught with risk.

In a recent discussion of electronic sweeping devices in China, where we do a lot of work, there was a consensus opinion that your room will be bugged – possibly video as well as audio, your phone will be tapped, and your computer communications will be monitored. If you have private meetings, don't be surprised if you are joined by a Chinese official. If you bring in bug-sweeping equipment expect it to be confiscated, and consider the possibility of being arrested as a spy. We don't think that bringing in encryptors is a smart idea, as they will be detected as soon as the listener hears the hiss of the encrypted conversation. Bottom line? Expect that everything you say and do will be seen and heard.

How about a more-Western place, like France? Well, in France, encryption codes must be turned over to the government (thus explaining why sending encrypted messages there is sometimes less helpful than might be expected). While we are not sure about the legality of encryptors in France, we have never heard of any business person having a problem with their use. Bottom line? Expect that everything you say and do will be seen and heard.

The former Soviet Socialist Republics, in our experience (and confirmed by the good folk at L-3 Communications), are a suspicious lot, and will snap up encryption and bug-sweeping equipment. And don't think, when you meet some extremely attractive woman in Moscow, that you are suddenly any more attractive than you were in your hometown, and that the interest is merely in your attractive self. Bottom line? Expect that everything you say and do will be seen and heard.

How about the U.S.? Well, the good news is that encryptors are legal. The bad news is that reports on wiretapping seem to indicate that this doesn't bother those doing the taps. Overall, the Communications Assistance for Law Enforcement Act (CALEA), has made most types of telephonic communications accessible. But not all. New York State Attorney General Elliot Spitzer petitioned the Federal Communications Commission to require manufacturers to make devices that can be tapped by police, as he said they must do under the CALEA. This includes wireless phones with features such as "push to talk" and devices that offer picture and video messaging, as well as "voice over Internet" services, Spitzer said. How about the Internet? Well, a quick web search on Carnivore will tell you all you need to know. And as most of you know, some hotels now have video cameras in rooms to monitor employees. Bottom line? Expect that everything you say and do will be seen and heard.

## 5. Real Stories from the Field — But the numbers looked good...

A financial investor had interests in a number of restaurants that did very well. But obviously they weren't all like that if his story has made it here. This is the story of one of the bad ones.

The building was about a decade old and had been previously occupied by three different food establishments. The prior restaurants had gone out of business, and thus, there were *de facto* locational risks. But the demographics were great, and the access was great, and the rent was really good, so they took it.

The prior tenant had done minimal work and the interior was dated, but with only some heavy paint and a very few customized fixtures, they re-created the theme of their other restaurants: Kind of a warehouse feel with lots of space. The code and health inspections went well and they opened up 60 days after signing the lease.

On the first health inspection after opening they got several violations because of roach droppings and dead roaches. It was cleaned up and the place sprayed regularly, and the problem seemed to go away. Until the big storm.

A cool wave came through the area with a squall line that dropped the warm balmy summer temperatures of Southern Illinois to the cool of a late summer. The air temperature dropped, and the air pressure dropped, and an overpowering stench, along with a fine mist of roach droppings, began to spray from the cracks around the vents and doors. Roaches were dropping from the ceiling onto the staff and guests. People screamed, and ran from the restaurant. The owner / manager was in the parking lot scrambling to give everyone double their money back and a \$50 coupon for future use.

Only one person called the health department, and nobody called the local newspaper. Luckily, the health department got the call but didn't believe it. As soon as the last car pulled out of the lot, the manager closed the restaurant for "remodeling and updating," and called the other owners.

They ripped into the walls behind the wallboard and found a disgusting sea of roaches (we really hate roaches!) living on a thin film of fat and grease that lined the walls. Prior owners apparently dealt with the problem by sealing the walls as tightly as possible.

While this did confine the roaches, it is what led directly to the dramatic event. The extra effort of sealing accelerated the accumulation of droppings. It also created the condition that would cause the abrupt pressure change to suddenly exhaust the higher-pressure foul air trapped behind the sealed walls

– along with the droppings – through weak seams and cracks, and into the lower-pressure interior space.

Finding the source of the grease was not easy. They hunted high and low, and could only guess that it had something to do with the air handling and exhaust system. They were right. The kitchen exhaust-hood ductwork had a joint seam in it halfway between the roof and the wallboard ceiling, where there should be no joints. To add insult to injury, the joint was done incorrectly, causing a fine mist of grease and cooking fumes to be forced into the airspaces within the framing of the building.

The exterminator had no ideas how to handle this, so the owners and their finance team – ignorant as they were – decided to fix the problem themselves.

First they fixed the exhaust-hood ductwork. This took two hours and about \$120 of ductwork.

Next they drilled pairs of 6 inch holes in the walls from the *outside* of the building. One hole was drilled at the top of the building and one at the bottom, in between each set of framing/furring studs. They then vacuumed all of the droppings, along with no small amount of live roaches, out of the walls.

Next, they set off nicotine smoke bombs in the restaurant, and forced additional smoke into the walls through the holes. They repeated this process two times, at which point they saw no roaches, and no more roaches – dead or alive – were being vacuumed out. Then they did it one more time, just for good luck. After a lot of cleaning, and a lot of new paint and patching, the restaurant was re-opened. The entire process took two weeks.

How did this to happen in the first place? The finance guys didn't demand appropriate due diligence from the restaurant guys: The numbers looked good, after all. The restaurant guys saw a great opportunity, and figured they better get the place quick before someone else leased the prime location. So they didn't do their homework.

Had they checked the health department records, they would have seen that every month there was a report of a roach problem at this location. All of the locals and the neighbors in the complex knew of the problem, but the new restaurateurs didn't, and didn't wonder where the roaches had gone.

When they re-opened, the managers told the locals and neighbors that there was just a problem with how the building was sealed, and that it had taken care of. Now, two roach-free years later, the restaurant is doing well.

The good news is that the finance guys sat down with the restaurant guys, and they jointly devised a checklist for due diligence on each and every site that was to be considered in the future.

In addition, they went after the building owner who had failed to disclose the problem. They settled with the former owner on a reduced purchase price on the building.

The moral is that due diligence, whether on a \$100 million project or a \$100 thousand project is more hands-on than most people realize.

## **6. Book and Product Reviews**

Every once in a while we like to recommend some good books that may not always be on topic – but heck – live on the edge!

*Glitter & Greed: The Secret World of the Diamond Cartel*

Janine Roberts

The Disinformation Company ISBN: 0-9713942-9-6 384 pages \$22.95  
<http://www.disinfo.com/> 1-877-809-1659

This is a 15-year in the making treatise on the diamond industry and how effective the DeBeers Cartel has been at keeping the price of a common stone artificially high.

*Guns, Germs, and Steel: The Fates of Human Societies*

Jared Diamond

W. W. Norton & Company ISBN: 0-393-03891-2 480 pages \$27.50  
<http://www.wwnorton.com/> 1-800-233-4830

This Pulitzer Prize winning book is an exhaustive look at how people and societies came to be where they are, and what components and societal tendencies lead to their success or failure.

*World on Fire: How Exporting Free Market Democracy Breeds Ethnic Hatred and Global Instability*

Amy Chua

Doubleday ISBN: 0-385-50302-4 256 pages \$26.00  
<http://www.randomhouse.com/doubleday/>

Chua challenges the belief that exporting free markets and democracy to developing countries will increase worldwide peace and prosperity. Since wealth tends not to be spread evenly, “market-dominant minorities,” become targets of hatred, and ethnic violence and social instability follow. Individual

countries can be viewed as dominant minorities, thus explaining the view of much of the developing world toward the U.S.

*All You Need Is Love, and Other Lies about Marriage*

John W. Jacobs, M.D.

HarperCollins ISBN: 0060509309 272 pages \$24.95

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

Divorce can be one of the most traumatic – and costly – of life events, which makes it a concern for this journal, and for our readers. This book examines some of the stressors unique to marriage in our era.

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

•• ÆGIS 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.

- **Protection of trade secrets and intellectual assets.**
  - Anti-economic espionage.
  - OPSEC: The identification and protection of information that would give your competitors and adversaries an advantage.
- **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 2004* and the *EU Revised Money Laundering Directive of 2004*.
- **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](mailto:ejournal@lubrinco.com).

To subscribe to our AvantGo channel, go to [http://avantgo.com/channels/\\_add\\_channel.pl?cha\\_id=1773](http://avantgo.com/channels/_add_channel.pl?cha_id=1773)

To be removed from the subscription list, follow the instructions on the mailing you received, or send an e-mail to [ejournal@lubrinco.com](mailto: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](mailto:ejournal@lubrinco.com).

If there is a topic that you would like to know more about, send it to [ejournal@lubrinco.com](mailto: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](mailto: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 May 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.