



**ÆGIS** journal

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

Volume 10 Number 1, January 2007

From the case files of

**LUBRINCO**

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

and



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

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

**This month's features:**

- **Special Announcement: Critical Information and IP Conference**
- 1. **Asset Location and Due Diligence — Choosing electronic voting machines**
- 2. **OPSEC, Economic Espionage, and Competitive Intelligence — Do intangibles matter?**
- 3. **Executive Protection — Protecting inaccessible places**
- 4. **Technical Issues — Heart attack performance review**
- 5. **Real Stories from the Field — I once was lost, but now am found....**
- 6. **Book and Product Reviews — Motorola V195s / Palm Tungsten E2**
- 7. **Subscription/Unsubscription/Copyright Information**

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

### **1. Asset Location and Due Diligence — Choosing electronic voting machines**

In evaluating electronic voting machines we must look at two types of error. The first is system error, which is error induced by the machine. That is to say that you vote for choice A and choice B is recorded. System error can either be accidental or deliberately programmed. Since this editor spent much of his youth as a professional programmer, we can assure you that even the most trivial programs can have mysterious and unanticipated errors.

The second is user error, which is error that occurs because the voter does not understand how the device works and indicates the wrong choice. This might be caused by the design of the system, or by the voter simply making an honest mistake. To find out the potential scale of user error, we spoke with one of the original implementers of ATMs, and asked what user error rates were observed when ATMs were implemented. He noted that this was not entirely a fair question, because when ATMs were first introduced there was an attendant at each machine to help users understand how they were used. However, the rate of error in this somewhat artificial environment was roughly fifteen percent.

System error caused by mistakes in programming can either be random, giving roughly the same number of bad votes to the various candidates (this is the best case) or skewed so that one particular candidates gets more than their fair share of votes. System error that is deliberately programmed in – the goal of most efforts to hijack elections – would be designed to give the benefit to one candidate, or one party.

With system and user errors in mind, let us look at the three kinds of electronic voting machines.

The most desirable from the voters' perspective are those where a person marks a paper ballot, after which the ballot is put into the machine which first checks to make sure the ballot is completely legible (i.e., there are no hanging chads). If the ballot is completely readable, it records the vote (this is the electronic part), and the paper ballot is kept for later verification if needed. If the ballot is not completely readable, the ballot is corrected if possible, or marked as invalid and another ballot issued. While user error may still occur (a person marks the wrong spot by mistake), system errors are likely to be of minimal concern for two reasons. First, the technology for readers has been around since the pre-electronic era. Second, the ballot is the original, not the electronic entry, and tracking errors can be found in a straightforward manner if the ballots are manually examined. The main concern here is the design of the form, as this will determine much of the user error.

Less desirable are voting machines that operate in the manner of a cash register, with the primary vote being electronic, and the paper trail being a backup. Since the paper trail is an artifact, there is no reason to expect that the vote recorded electronically is the vote cast. But at least there *is* a paper trail.

The least desirable voting machines are completely electronic, where there is neither an actual paper trail, nor even the pretense of a paper trail. These machines have deservedly been the center of many jokes (“18-year-old Diebold programmer elected president of United States”), and the techniques for hacking these machines have been widely discussed.

An interesting question is how to nullify votes on completely electronic voting machines where it is anticipated that the vote will be unfavorable, but where either scrutiny will be so tight as to make rigging the machines difficult, or the expertise to do so is lacking. A solution we have heard discussed is to simply remove a particular machine from the voting pool after the votes have been cast. This would need to be done subtly, disabling a few critical machines in very close races, which likely means local races, rather than presidential races.

One approach we have heard discussed is use of an electromagnetic pulse (EMP) to destroy the circuitry. An EMP will fry most transistors, though it will not affect vacuum tubes. How do you produce an EMP sufficiently high to do what is needed, and no more? While detonation of an atomic device will generate an EMP sufficient to fry every electronic device around (thus explaining why MiGs used tube-based, not transistor-based, circuitry in their avionics), something more localized is needed. Some other form of energy discharge would need to be used.

The bottom line is that an election commission interested in fair and verifiable elections will choose electronic verification and tabulation of paper ballots.

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — Do intangibles matter?**

One of the things that always astonishes us when discussing intellectual property, critical information, and other intangibles is the reality that so many people don't understand the economic impact of the intangible. There seems to be a consensus among public sector financial managers that intangible assets have no real economic value because they are, well, intangible.

This view is validated by the accepted accounting practice, explained to us in painful detail by the PCAOB, that intellectual property developed in-house has no book value. It is additionally supported by the fact that much information is never even looked at as having economic value. True, most recognize that trade secrets have value and need to be protected, but it largely stops there. Indeed, it is rare to find a company that has an audit or accounting of its intellectual property. Yes, we mean that it is rare that a company can even identify all its patents, and what is being done with them!

How do we reconcile this view with estimates from the federal government that losses from competitive intelligence, economic espionage, and theft are costing American companies \$300 billion a year? We can't. But is \$300 billion really significant in an economy as large as ours?

In terms of the total percentage of our GDP, (estimated at \$13,322.6 billion at the end of third quarter 2006, according to the Bureau of Economic Analysis), this loss represents 2.25 percent of our GDP. While 2.25 percent doesn't sound material, we note that agriculture contributes 1% of our GDP.

The not-material claim is one we often hear. We have been told by corporate managers that a loss of \$50 million or \$100 million – even the closing down of a division – is not material to their multi-billion dollar corporations. Yet a loss of \$100 million translates to 2,500 or more people out of work. The \$300 billion lost equates to 7,500,000 jobs lost, which makes it a public policy issue. No doubt this is why the SEC mandates that these losses must be tracked and disclosed.

There is another compelling reason why you should care. Let us assume that you choose to lose \$100 million by failing to implement an OPSEC program. If your company has 100 million shares outstanding, does a reduction of earning of a dollar a share affect your stock price? If your company has 200 million shares outstanding, does a reduction of earning of fifty cents a share

affect your stock price? If your company has 400 million shares outstanding, does a reduction of earning of twenty-five cents a share affect your stock price? Considering the number of times we have seen a stock tank when it failed to “meet street expectations” by a lot less than this, we would say that the market says – screams – YES, we care about intangibles.

### **3. Executive Protection —Protecting inaccessible places**

Recently we were browsing at the Strand bookstore in Manhattan at the same time a co-editor was in a bookstore in Phoenix. We both chanced upon the same book by a burglar from Florida. He would thumb through the pages of a local slick colored glossy socialite magazine, notice what jewelry the socialites were wearing, and choose his next victim based upon the security system of their dwelling. He possessed the sure knowledge that most people’s security systems had gaping holes in them. One story he told was of robbing Mrs. Armand Hammer, whose apartment on a high floor of an apartment building had an inaccessible terrace. He figured that if he could get access to the terrace he could get in. As it turned out he could, and he did.

During this period an alarm system was being installed in our office in Gotham. We protected the door, but ignored the windows, since A) they were relatively inaccessible, and B) they were very visible from the street.

One afternoon we glanced out the window and found ourselves looking at a man looking in at us. As it turned out, some work was being done on the building next door to ours, and they had put up scaffolding that was, by coincidence, installed in such a way as to put a ramp directly to our window.

Now, we weren’t robbed when they put it up: They really were just working on the other building. And we immediately took steps to eliminate this vulnerability, which, by the bye, we would *never* have permitted in the office of a client. What this shows is that when preparing for an unlikely eventuality you need to look at the incremental cost of doing the job right, as opposed to doing the bare minimum. In this case, the incremental cost of alarming the windows was nil. This means that when we balanced the cost (nil) against the risk (also nil), it would have made sense to protect the windows at the outset.

But what if the cost of protecting the windows would have been substantial? In that case the risk would not have justified the cost – we really don’t have anything worth stealing – and we would have self-insured (i.e., borne the risk ourselves). This explains why we did not protect the walls, as we might in, say, a jewelry store. If someone cut a hole in our walls –most internal walls in

modern New York City small buildings are only plasterboard – the thief could walk in, take what he wanted, and leave as he came.

The bottom line is that whenever you are taking protective measures you need to look at the threat, the vulnerability, and the cost – that is to say you need to evaluate the risk – and make some sensible judgment based on this risk. But you must do this with the full knowledge that an event being unlikely – like someone building a ramp to our window – does not mean that it can't happen.

#### **4. Technical Issues — Heart attack performance review**

One evening last month our home phone rang at 2:25 am. It was a neighbor who said he didn't feel well. We got dressed, grabbed our always-take-with-us bag, and went up to his apartment. We found him clutching his chest, so we called 911. This being New York City, and there fortuitously being no traffic tie-ups in Manhattan in the middle of this particular night, the first responders (firefighters, followed mere minutes later by EMTs), arrived in under five minutes. By 3:25 am he had been transported to Roosevelt hospital where he had been stabilized and given a chest X-ray. By 4:25 he had been transported to Saint Lukes and was already undergoing angio-catheterization.

In evaluating our supporting role in this drama, we had three criticisms.

The first is that when we got the initial call we should have asked what the problem was and whether an ambulance was needed, rather than losing time getting dressed and going upstairs to see for ourselves. We would have saved some number of minutes had we done this.

Our second mistake occurred when we got upstairs and realized that he was having a heart attack. We had our trauma kit with us (as we always do), and should have immediately given him either a regular aspirin to chew, or, more reasonably, several baby aspirin to chew. We had both in the kit, and this would have cut down by a few minutes the time until the first responders arrived and gave him their baby aspirin, albeit with some nitroglycerin thrown into the mix on their part.

The third mistake was technical: We did not start our conversation with 911 by giving our address followed by our name followed by the problem, which assures that if you get cut off they know whom to look for where and why. Rather, we answered their questions as asked. We didn't get cut off, but should nonetheless have started with the where, who, and why.

As it worked out, the sequence of events moved swiftly enough that the minutes we had squandered didn't matter. Even so, this was more a matter of luck than

skill, and the lost time could just as easily have been fatal. While our friend was out of the hospital by Sunday, and more or less back to a quasi-normal routine a few days after that, it could just as easily have gone the other way, with the difference between life and death being a matter of a few minutes.

Independent of the confusion of being awakened from a sound sleep, we should have thought this eventuality through long before an incident occurred, and done better. We will next time....

## **5. Real Stories from the Field — I once was lost, but now am found....**

There has been a rash of recent stories in the press of people lost in the wilderness and dying. The most publicized of these has been the loss on Mount Hood of Kelly James and Brian Hall of Dallas, and Jerry Cooke of Brooklyn. As of this writing, only the body of Kelly James had been found.

It is not our intention here to discuss cold-weather techniques or survival in snow conditions, nor is it our intention to critique the performance of those who lost their lives in these incidents. Rather, it is to discuss the importance of people being able to locate you when you are in distress. We don't really care (until after the fact, so that someone can learn from your mistakes) how you got into trouble. We are interested in getting you out of it.

When you get into trouble there are two primary things you need to do in order to be rescued. The first is to let someone know you are in trouble. The second is to let someone know where you are. Telephones and cell phones are a good choice in many cases (such as our heart attack incident), assuming you have a good signal and know whom to call and where you are. Satellite phones can also be a good choice, as they will often work in places where there is no cellular coverage. But for many emergencies our vote goes to personal locator beacons, which we previously discussed in the October 2003 and December 2005 issues of **ÆGIS**. Recent incidents indicate that it is time to re-visit the subject again.

Let us start by stating that the COPAS-SARSAT satellite system (<http://www.cospas-sarsat.org/>) saves lives. According to NOAA, as of 5 January 2007 over 20,300 people worldwide have been rescued using the COPAS-SARSAT system since 1982, with 5,397 of these being in the United States. Last year alone, 37 people in the United States were rescued because they used their personal locator beacons (the rest of the 272 rescued last year in the U.S. because of the COPAS-SARSAT system were aviation- or maritime-related).

So, what is involved in using a personal locator beacon?

For a start, you need to have one with you during an emergency. For many, the need for a PLB will be sporadic at best, and the wisest choice might be to rent one when needed. *Liferaftrental.com* will let you have a GPS equipped PLB for \$39, plus a \$1.90 per day rental charge, and *plbrentals.com* will rent you one for \$59 per week. This is extremely reasonable, especially if you need to use it!

If you have a more constant need for a PLB – perhaps you hike regularly, or travel by car outside of major metropolitan areas – it might make more sense to buy a unit. There are quite a lot of choices, at a wide range of prices.

We ourselves use the high-reliability Microwave Monolithics' MicroPLB GX (<http://www.micro-mono.com>), which at 1.1" X 2.4" X 5.9" is about 15 cubic inches and weighs in at about 10 ounces, runs for 48 hours at -40 C (class 2), and has a number of virtues that we feel justify its \$1,700 price tag.

Realistically, however, could comfortably make do with one of the excellent 24 hour Class 1 (-4 C) GPS units from ACR (30 cubic inches, 12 ounces, list price 883, street price \$550 <http://www.acrplb.com/>) or McMurdo Pains Wessex (38 cubic inches, 11 ounces, list price \$650, street price \$550 ([http://www.mcmurdo.co.uk/products/product.html?product\\_type=2&product\\_sector=4&product=47](http://www.mcmurdo.co.uk/products/product.html?product_type=2&product_sector=4&product=47))). These take up some about 30 to 38 cubic inches and weighs in at about 12 ounces, and have a street price tag of \$550 (*liferaftrental.com* will sell you one that is as good as new for substantially less). 24 hours is more than enough unless you are adrift at sea, or stuck in a hole and need to wait for a low earth orbit satellite to pass overhead.

While we certainly hope that none of our readers ever find themselves in a situation where a PLB is needed, we also hope that if you do, one will be near at hand.

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

### **Motorola V195**

<http://www.motorola.com/consumer/v/index.jsp?vgnextoid=0fe32c1cef62d010VgnVCM1000008206b00aRCRD&show=productHome>

**and**

### **Palm Tungsten E2**

<http://www.palm.com/us/products/handhelds/tungsten-e2/>

It recently became clear that our mobile phone was dying, and we began the search for a replacement. The base criteria were that it be A) a quad-band GSM terminal B) with no camera. The lack of camera is important because of

the increasing frequency that cameras, including phones with cameras, need to be vouchered when going into plants and offices and restaurants and gymnasiums and theaters and schools, et cetera. We wanted a phone, not a PDA/computer/video player/MP3 player/coffee maker – with a phone thrown in as an afterthought – because we have never encountered one of these hybrids that had acceptable voice quality.

The choices were painfully few in number, because as mobile phones became a commodity item in the hand of every child, business travelers shrunk to a market no longer worth addressing. Even so, we thought our minimal criteria would give us a reasonable set of choices. We were wrong.

We finally discovered the Motorola V195s, which is a current incarnation of the V190 series, but with an internal antenna, offered by T-Mobile. The V197 appears to our untutored eye to be essentially the same phone as the V195s, but offered through another set of service providers.



As we have come to expect of Motorola products, the V195 is well designed and engineered. Much of the body is some softish composite which feels nice in the hand, and looks as if it will not scuff or scratch easily. RF seems to be to the usual high Motorola standard, and battery life is excellent. From a GSM point of view, we have only two minor complaints. The first is that Motorola didn't implement confirmation of receipt of text messages (or the ability to send a text message to an e-mail address stored in the phonebook. The second is that they didn't implement use of dual SIMs (we use DuoSim – <http://www.duosim.com/> – for this, which we will discuss in an upcoming issue). While neither is a deal breaker, even for we who use these features, their absence is still an inconvenience.

The user interface is typical Motorola, handling the basics comfortably and lacking most of the niceties one has come to expect in the 21<sup>st</sup> century. Since our goal is to make phone calls, and our base criteria were quad-band and camera-free, the user interface was of tertiary consideration at best. The V195s meets both our criteria, and has good RF so that we can make our calls. Because of this, we highly recommend the device for anyone who travels on business, and therefore cannot have a camera in his mobile.

Of concern to some might be the SAR rating. The SAR limit set by the FCC and the Canadian regulatory authorities is 1.6 W/kg, and 2.0 W/kg by the Council of the European Union. The SAR of this phone is listed at 1.6 W/kg (we prefer it to be under 0.5), so if this is an issue that concerns you, use a headset.

We were delighted to see that the V195 now has more memory than did the V188, which means you can get more entries in the phone book. And the phone does have a calendar function, so you could use the V195s to act as a mini-PDA if you so chose. The easiest way to do this is using Motorola Phone Tools, currently in Version 4. The V195 is not, even with the most current update of the software available as of this writing, one of the phones that will be detected or even listed in the manual installation section, but Motorola says you can select the V190. The calendar function is quite convenient, as is the ability to send text messages from the keyboard. The phonebook entry section allows input of the name, number or e-mail address, and quick-dial number. This last is convenient if you want to shuffle quick-dial numbers around. It also displays (but does not let you change) the category.

In truth, however, just as a phone is a better choice than a PDA with a phone thrown in as an afterthought, even so a PDA is a better choice than a phone with a PDA thrown in as an afterthought.

A good choice for PDA to go with the V195 is the Palm Tungsten E. Both are Bluetooth devices, and can interact. This means that if you keep your contacts in your E2, you merely select the contact in the E2, tap the QUICK DIAL icon, tap the number you want (we assume that you have several numbers for each contact), and your cell phone will, as if by magic, dial the chosen number! This is much more convenient than typing the number into the phone while looking at the Palm.



You can also send a text message from the E2 via Bluetooth on the V195s. You could even use the painfully slow GPRS connection on the phone to connect the E2 to the Internet, but GPRS is still not-quite-ready-for-prime-time, so this is as torturous as using GPRS on the V195 itself. We did not test the WiFi card that can be used with the E2, and did not look at the Tungsten TX, which has WiFi built in.

In addition, the E2 allows encryption of either everything on the E2 or of specific private records. This means that you can keep information that you might like to have with you, but don't want available to others if your Palm is stolen or lost. Encrypting everything is straightforward: Tap on PREFERENCES, SECURITY, ENCRYPT DATA WHEN LOCKED. You can choose to encrypt only specified applications (contacts, memos, and expense seem reasonable), and can hide private records. You can choose between AES or RC4 encryption, with either being perfectly acceptable.

If you do implement the encryption features, we recommend using a passPHRASE rather than a password. Be aware that when you are asked to

enter your password, the E2 presents you with a password screen that replicates a touchtone dialer, allowing you to pseudo-spell-out the passphrase, with the E2 actually putting in the number, not the letter. As you tap in a letter it shows, and then is replaced by an asterisk when you type the next letter, so that the entire password is never visible to anyone near you. This is a good system, and would, in fact, be the appropriate approach if Palm had used this entry screen consistently.

Unfortunately, when you need to show private records you are NOT presented with this screen, but with a screen that wants direct entry of the passphrase, i.e., the ten to twenty numbers themselves. This means that if you use a long passphrase you will need to pull out your cell phone – or print out a copy of a touchtone keypad layout and paste it onto the back cover of the palm – so you can figure out which keys you should press.

One way around this is to ignore the original password screen, and instead tap on the ABC symbol in the data entry area. This gives you a mini-typewriter that you can use to enter the entire passphrase, including capital letters and punctuation. Unfortunately, this leaves the entire passphrase visible every time you enter it. This is clearly undesirable.

Palm technical support said of the inability to get the right screen that “This is a limitation of the Palm OS®.” We translate this to meaning that protection of data was at the bottom of the developer’s list and never tested, so that nobody ever realized that the wrong screen was being shown when the user was asked for the password before showing private data.

An additional oversight is that while the Palm Tungsten E2 is made for business people, the charger supplied is 120 volts only, even though the additional cost of making a dual-voltage charger that would work anywhere in the world is essentially nothing. While you can buy Palm’s travel charger for \$29.95, we don’t think it is fruitful to reward bad design, and suggest you go onto ebay and spend five dollars for a knockoff universal travel charger.

The V195s is an excellent handset. We use it and recommend it if you, like us, need a camera-free quad-band GSM handset. The Palm Tungsten E2 compliments the V195, and the two work very well together.

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

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2007 by The **LUBRINCO** Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard

Isaacs (RBIsaacs@lubrinco.com), L. Burke Files (LBFiles@feeinc.com), and Terry Phillips (TPhillips@aegisjournal.com).

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

- **Identification, valuation, and protection of intellectual property and critical information.**

1. American businesses lose \$300 billion annually to competitive intelligence, economic espionage, and information theft.
2. Sarbanes-Oxley requires internal controls tracking the costs, and impact on valuation, of competitive intelligence, economic espionage, and information theft.
  - LUBRINCO is the leading private sector provider of access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information from competitive intelligence, economic espionage, and information theft.

- **International asset location and due diligence.**

- Location of concealed assets in fraud, theft, and divorce.
- Due diligence to prevent fraud and loss in China, Central and Eastern Europe, Central Asia, the offshore financial centers, Latin America, and the Caribbean.
- Financial fraud and anti-money laundering program development and training for compliance with the US *International Money Laundering Abatement and Anti-Terrorist Financing Act of 2001* and the EU *Revised Money Laundering Directive of 2001*.

- **Protection of management, staff, and families.**

- In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.
- When traveling and living overseas.
- When transporting items of substantial value.

**LUBRINCO** identifies and quantifies threats and vulnerabilities, and their associated risk, then manages the vulnerabilities so you can transfer or live with the residual risk. We prevent disastrous financial loss to your company, and physical harm to you, your family, and your staff.

For information on **LUBRINCO** and its services, or for the archive of all past issues of **ÆGIS** in PDF format, please go to <http://www.aegisjournal.com/>.

Subscription to **ÆGIS** is available for \$15 per year in North America and \$20 per year outside of North America.

To sign up for a **complimentary subscription** to **ÆGIS** or the **ÆGIS** PDF notification list, go to <http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to [subscribes@aegisjournal.com](mailto:subscribes@aegisjournal.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 [unsubscribe@aegisjournal.com](mailto:unsubscribe@aegisjournal.com).

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

If there is a topic that you would like to know more about, send it to [editor@aegisjournal.com](mailto: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](mailto: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 **LUBRINCO** Web site is included. This should be in the form

*Article Title*, from the January 2007 **ÆGIS** (© 2007 **LUBRINCO** & FEE), 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.