



Addressing threats that affect your bottom line

Volume 15 Number 2, February 2012



<http://www.feeinc.com/>
1-480-838-1728

- 1. Asset Location and Due Diligence - Mining The Meaning From Data**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence - Mind The Snail Mail**
- 3. Executive Protection - Very Private Meetings!**
- 4. Technical Issues - iPhone, Blackberry, Android - Security**
- 5. Real Stories from the Field - The Office Move**
- 6. BSA, AML, & OFAC - Writing Policy Manuals**
- 7. Book and Product Reviews - Help Your Employees Get Through Failure, by Gail Kasper**
- 8. Subscription/Unsubscription/Copyright Information**

Announcements:

Mr. Files will be speaking at the following seminars ...

- [10th Annual Offshore Alert Conference - April 29 - May 01, Miami, FL](#)
- [East West Conference - May 1-2, Lisbon, Portugal](#)

Top 1% Club Expert with Gail Kasper.

I have recently partnered with the Top 1% Club where I am featured as an expert. Not only will you be able to view additional articles from me, but you will also have the opportunity to learn from the Top 1% Club Mentor, Gail Kasper, one of the nation's leading professional speakers, a television commentator, and a life and business coach. Membership costs you nothing and if you join now, at <http://www.top1percentclub.com> you will be eligible to receive a complimentary set of Gail's new books.

Read more under Book and Product Reviews

1. Asset Location and Due Diligence - Mining The Meaning From Data

Our modern corporations are huge consumers and warehouses of data, actually so are our small business, and our households. Never, in the history of mankind, has there been so much information and data about - well - just about everything.

This volume of information in itself is a problem, as now we are required to be more astute consumers of the information.

We are aware of the value of "information" but we are numb to what is good information and what is noise, what is sound information and what is unsound, what is biased, what is timely and what is dated.

This all goes to the 7 points of what matters

- Is this information relevant?

Relevance of information is now very time sensitive. Our ability to perceive and then recognize relevance has an impact on the bottom line. The relationship between information and revenue may or may not be direct one,

but the costs of a missed opportunity or an unanticipated threat can be huge.

Q: What is the hallmark of a professional that recognizes relevant information in a timely fashion?

- What am I missing 1/3 - 2/3 rule

With the prevalence of social media, and blogs and desktop publishing - publication and editorial power has shifted to the individual. The information is available the moment it is produced. Yet the Internet has no editor, or fact checker - thus while the information may not be fact checked - it is also free from an editor's biases. (*I call to mind a story about a company a local paper would not run because the CEO of the company who was the focus of the negative story sat on the paper's board of directors and the company bought a lot of ad space from the paper.*) The shift from edited and filtered information is a positive shift. The search engine weightings, rankings and page numbers all have to do with popularity - not usefulness. The more popular the information the easier to find, the more narrow the topic the harder the information is to find. It will be difficult for the consumer of very narrow informational bits to find all of the bits they may wish to see and weigh.

Q: How do we find that which lurks below the surface?

- Type cast again?

The web uses algorithms to search for the content you may wish to see based upon past browsing history. The retailers use them, the blogs use them, the search engines use them, but that is not who we are. Our tastes are not based upon our past history as much as the whim of our polymath minds or our ever-changing roles in life and work. Once in one of these loops it can be hard to break out of them and these informational feedback loops can be very limiting when looking for new information on new topics.

Q: How do we escape these biased anchored histories in life and commerce?

- Keepers of the knowledge, professional oracles.

Experts are a good way to obtain relevant information with less effort. Specific knowledge on locations, technology, laws and regulations are often a must to make well-informed choices. The experts can also become gatekeepers to access of information, and biased filters of information. Experts that are not delivering information that is relevant to the consumer of the information are more dangerous than no information.

Q: If the experts are giving the same advise to every client, how can I use that expert's advice to have the competitive edge?

- I trust my community, don't I?

We trust those we like and those we interact with. We get our information from ever growing online communities and social media networks. A great deal of this information is very relevant and often you can see real-time dilemmas playing out in an industry if your level of awareness is attenuated to both what and how things are being said. This can produce tremendous insights in to the impact current events will have on a future market place for ideas and or goods and services.

Q: How do I know the community is not being manipulated?

- Ah ha! That's what I was looking for?

You look and look and look for information to help you understand the world around you. You read and digest information from so many sources. How do you keep up with life, work and family with the heavy burden of always and all the time searching for information. Yet the content provided distracts you with internal links and mazes of distractions making it take you much longer to get the information you want. It is good for their pages rankings but a time waster for you. You get overload with noise - but you wait for that ah-ha moment that makes it all worthwhile. Yep overloaded, over overwhelmed, and underwater all at the same time.

Q: What is the different between what I need to know and what I would like to know?

- How do we become aware of new information?

We must keep our eyes and ears open; we must poll others for opinions and ideas - yet we also must clear our minds. Try to practice choiceless awareness. Choiceless awareness is where an individual perceives a given situation or bit of information in an unbiased manner. That means without distortion, without signal noise that colors or distracts. Therefore they will, with complete awareness, act according to this awareness. The choices made will be the manifestation and result of this awareness, rather than the result of biased or managed choice.

Q: How do I process these changes of awareness and provide a referent for context and location?

Due Diligence is about information, about doing your homework, and amassing

knowledge that is both accessible and usable for choice making. Information is stored in different locations, with filters, bundles, edited, un-edited, sorted, unsorted, or colored to fit one consumer's needs making it useless for others, etc....

There are many laws now on the books for distracted driving because the results of distractive driving are so severe and sometime deadly. It is not different for us, as we are finding it extremely difficult not to be distracted by information that is not relevant to our information needs, yet we must stay aware of new developments in a timely fashion as the world now just seems to happen faster.

The state of the information barrage is not going to change - what needs to happen for all of those in the information and choice making professions is to ask and answer the 7 questions posed, for themselves.

2. OPSEC, Economic Espionage, and Competitive Intelligence - Mind The Snail Mail

We seem to be very conscious of e-mail security, but are often oblivious to the security of the "snail mail" we receive at our homes and offices. Recently, in our role as consultants in the due diligence arena, we were asked a series of questions of snail mail and corporate snail mail security. The answers bear repeating for a wider audience.

- What type of mail security should we have?

Each type of company will have its own requirements and each specific company will have further refinements of those requirements. If the company regularly handles payments through the mail with a significant volume of payments arriving via postal mail or courier, a lock box service is often a sensible investment, both for security and efficiency.

For smaller companies, I strongly recommend that all mail go to a post office box, not a private mailbox. Post office boxes are securely constructed and often continuously monitored by CCTV. However, private mailboxes (e.g., from the UPS Store) offer a street address for delivery of packages via courier, and may be more practical but not as secure as private mailbox should be securely constructed of heavy gauge steel and accessible only to employees of the mailbox company. A mail box at a home or office location, if needed should be also be very secure and made of steel with a locking system to gain access to the snail mail.

- How can one segregate mail streams?

Mail drops and drawers can be used to segregate the mail according to the wishes and needs of the company. However segregated, mail in significant volume should be picked up by a trusted employee or delivered by postal services in bulk, ending up in a secure location. If that location is at a company facility, it should be segregated from the remainder of that facility. Mail may be received, but should never be kept or even exposed, at a loading dock.

Once in the secure location, the mail can be delivered to the proper department. The mail can be pre-coded by agreement, such as adding to the address of certain locations or functions by adding additional addressing information such as Station A, Building 14, or to the attention of a specific employee. These codes should not interfere with the regular postal addressing.

- * How should junk mail be dealt with?

All physical mail should be treated as one would treat e-mail. It should be kept free from the prying eyes and the letter openers of others. Junk mail often originates from companies offering credit cards or financial services. If such mail winds up in the wrong hands, it can lead to identity theft. Yep - even junk mail may have value

Unsecured mail streams are also vulnerable to industrial espionage without opening up a single envelope or parcel and with nearly zero risk of detection. Think of the unopened mail as the cleaner version of dumpster diving, but without the leftover food bits. One just needs to look at the front of the envelope to make conclusions about the company and the receiver. For example, an envelope containing a credit card will never have any identification on the envelope other than a post office box address. But, with a minor amount of research, one can link the address to the proper credit card issuer.

Mail stream analysis can also reveal the identity of a company's clients, the nature of the relationship, the names and addresses of key suppliers, etc. It is also possible to decode Pitney Bowes franking stamps to determine the senders names and physical address of where that piece of mail originated.

Now imagine what about what you can learn about a company if one you can open their mail!

- * How can I tell if the mail has been tampered with?

Look for smudged ink, as many letters are now printed with jet ink printers. The inks will bleed if the paper is treated with chemicals or water (steam) to

pen open the envelope and read the contents. Also examine the corners of the envelope for small tears. They may indicate that a tool was inserted to either spool the contents for removal from the envelope or that a small scope was inserted to read the document while still in the envelope.

Many correspondents will tape over the corners of an envelope to prevent tampering. However, someone who tampers with an un-taped envelope may also tape it over to conceal the tampering. For very high security mailings, wax seals may be employed to prevent tampering and authenticate the sender as well as security envelopes and tamper evident tape and seals. But yet, that too draws attention...

* How can I be more proactive to see if my mail stream(s) are being tampered with?

Have a letter sent to you, at the address of your choice, on a regular basis. Record the number of days it takes to arrive. If you see an increase in the numbers of days it takes for the test letter to arrive, on a consistent basis, this may indicate tampering or the monitoring of your mail stream, as the mailed items must be diverted for at least a few hours for fiddling purposes. This diversion may result in the mailed items missing the cutoff times for sorting and delivery for a day or more.

Include in your own correspondence a small sheet of rice paper inside the envelope. Rice paper turns to goo when it gets moist, such as in from steam when trying open steam open a glued envelope.

Add chemical dots to the paper and envelope that react to the different types of solvents used such as some of the dry cleaning solvents.

Use inks that react to heat, such as lemon juice that turns brown when heated.

Consider sending to yourself regularly a package that contains a mobile tracking device such as a cell phone, thus allowing you to follow your package from the time of mailing to the time of delivery. *Come to think of it I should do that with my luggage I check with the airlines .*

As always, specific recommendations for action depend upon specific fact patterns. If competitors of your business can gain a competitive advantage through surveillance of your snail mail, you'll want to act proactively to prevent such surveillance.

Much thanks to Mark Nestmann for his help with this topic - very cool indeed.

<http://nestmann.com/>

3. Executive Protection - Very Private Meeting.

One of our charges has come up with a very unique way of conducting private meetings. It is not often we learn something new from a client. Please do not take this as a sign of arrogance or indifference but one of reality, as we are saturated with the experiences of all of our team members and clients over many years.

Alphonso, we use this name because it is not his name, has contrived a unique way to have private meetings.

Alphonso travels a great deal, 200,000 a year or better, and negotiates some very unusual contracts for large corporations and wealthy individuals. Much of the work we do with him is to insure nearly no one knows where he is going to be at any given time. His threat is knowledge of his whereabouts - not physical security, per se. Even his arrival in a city, can spawn speculation as to who he might be meeting and what he might be doing. While his travel plans are private his calendar is not always so private for he must manage his time and his meetings and coordinate with the schedules of those whom he is going to meet.

His tactic is simple, he meets other parties, and whether they be clients or professionals is restricted public or semi public locations.

For example, Alphonso met with a professional from London at the J. Paul Getty Museum in Los Angeles. They walked from exhibit to exhibit, enjoying not only the art, but also the setting for the meeting. The counterparty to this meeting was told of the time of the meeting and 45 min before the meeting was told of the location of the meeting. It was a very private meeting as few were around and the museum offered plenty of private space both inside and outside without being overheard or recognized.

A second meeting was held at the NYPD Police museum, with a follow up conference on the Staten Island Ferry. The initial meeting was at the museum and when the parties agreed it was time to include two other parties held in waiting near by, they met and concluded the negotiations on the John F. Kennedy Staten Island Ferry.

He has also held meetings in the Prado Museum, Roman Forum, Museum of Asian Culture in Singapore and our favorite - Disneyland, Paris.

Alphonso's free wheeling style is not only very secure for communications the sheer randomness of the meeting locations, engineered at his request, adds yet another layer to the "where's Alphonso puzzle".

We use local agents, as advance team members, to look for places that are both public and offer opportunities for privacy. These locations are communicated via a very private method we choose not to share and only his Sr. Executive Professional knows the location. When the location is chosen and release to the EP team, another advance team arrives equipped anti eavesdropping technology. When Alphonso or his meeting mates arrive locations with the destination are suggested via a well-

placed whisper and off they go.

Alphonso's situation is very unique, but any person looking for some privacy and anonymity as well as a bit of culture can use this technique.

A similar technique can be used when a meeting has been called for a specific location. I was to meet a gentleman in the lobby of the St Regis Hotel and as normal I was a few minutes early. At precisely the meeting time I was paged to come to the phone. My client was on the phone and changed the meeting location to the Pierre, a hotel very near by, but different. This technique is also very good at hindering electronic surveillance.

This Executive Protection article was written or edited by Barron James Shortt, the Executive Director of the IBA. <http://www.ibabodyguards.com>

4. Technical Issues - iPhone, Blackberry, Android - Security

I asked a few different experts in electronic surveillance and cell phone security which of the three most popular smart phones is the safest and which is the worst. The answers were clear and consistent.

- 1.) On all of them it's the user that is the root of the problem.
- 2.) Android has been labeled the worst for malware.
- 3.) Blackberry is pretty good as it cannot have a virus, but it can propagate worms through its memory chip and emails.
- 4) iPhones are great until you "unlock" the iPhone with jailbreak or other programs.

All can have programs installed to do whatever the programmer wants the cell phone to do. One just needs to have physical control over the phone and the time and know how to install or write the program.

In the last half of 2011 almost all of the new malware was programmed for the Android Operating System. While Android is on the rise as a target, by far the largest known number of virus - over 75% are for the various Symbian operating systems - for Nokia Phones. iPhones while getting some targeted attacks are still one of the safest phones - unless they have been unlocked.

With more devices there are more threats and the threats depended upon where you are in the world - in the US the attackers are looking for information about , your phone, what you are saying and doing, where in Latin America and the Far East they are looking for banking information.

Some tips - if the phone has been out of your hands for any length of time and you are in a higher risk profession - dump it. If you have a phone given to you as a gift, dump it or sell it to someone else (*nothing like screwing up a targeted attacked by giving the device to a teenage girl - they will cream the electronic intruder just in fees*)

and messaging), avoid known problems phones and subscribe to anti virus and malware services - even for the Blackberry and iPhone.

Windows Phone 7 - is still new and looks to be more robust - but it too has been hit by some nasty malware. In December a SMS vulnerability was used allowing hackers to carry out a DOS attack on the victim's handset. Oddly this occurred just after MS offered free Windows Phone 7 to those who had Android systems that were getting hacked. Windows Phone 7 has not been out quite a year and we are sure it too will be tested by the hackers as it gains popularity.

5. Real Stories from the Field - The Office Move

The time has come to pass and we are leaving our current office for an owned location. As you read this - HOPEFULLY - we are comfortable ensconced in our new office - wherever it may be. Yep - not sure where we will be come February 1st.

It all began when I was purchasing a location to set up our new office. The offer was made and accepted and ... weeks ticked by... and eventually we were told finally all was fine and we would close in a week or so. So I gave notice to my landlord (*great people by the way*) that we would be vacating our office of some 3 years January 31. This notice was given December 15th.

It seems the new location, a commercial condo, has a small problem. A former manager slipped and fell, sued the association for defects in a property he was maintaining, and won a large judgment well in excess of the policy maximums. The association did not declare bankruptcy and the law firm representing the injured former manager is now in possession of all of the common areas. So while the title to the office condo is OK, the relationship with the association is ??? We, needless to say - we did not close.

How did we find out about this odd situation - we did our due diligence and found out the problems that were unknown to either the listing agent, the buyer's agent or the title company? So for a period of time our phones will be forwarded to a web based phone services and we will have to work in disjointed fashion as I scramble to find a new suitable location.

I am also reminded of the AMA article I read some years ago. It was a poll taken from companies that had recently moved. Of the "managers in charge" of the move - fully 2/3 were no longer with the company or had taken a demotion. While one can plan and plan and plan - often one's moving plans do not survive the encounter with the many seemingly random externalities of a given move.

This encounter with a property purchase and a move also reminds me of the phrase, you know what you know, you know what you don't know - and you don't know what you don't know. Due diligence helps with all three possibilities, but yet still one must find a way to plan for the unplanned.

6. BSA, AML, & OFAC - How to Write a Policy Manual

In the last several seminars we have conducted, as well as clients we have visited, a consistent constant question has arisen, How to write an effective policy manual?

Well the first thing is to be honest with ourselves; companies steal (*make effective use of existing copy*) to compose the first version of the AML manual as well as several sections of the manuals of other companies. Yep - you took what existed and began to adapt prior copies for your use, and that is OK.

The second is to cut from the manual those things you are not going to do. If the manual says you are going to scan outgoing wire transfers for XYandZ and you are not going to and or your firm is not a bank - cut that part of the manual. Seems simple, but if this were not a real problem - we would not have mentioned it.

Cut ALL adjectives and adverbs - if you need to color a situation - explain the color with out use of adjectives or adverbs.

Cut all words, nouns, verbs, etc.... that can be interpreted in different ways. If you are required to use nouns and verbs that are vague, immediately footnote the word and explain how you are using this word in context. I watched a large bank and the regulators got to battle over the meaning of the word "fiduciary". Honestly - there was not a wise mind in the room during that battle - geesh.

Avoid exclusionary words such as always and never. Never says that you will always do KYC research so you never get a bad client. Nuff said.

If you describe an action you will take - do it. If you are not going to do - do not say you are going to do it. If you say you will scrub the list of client against the OFAC list every 30 days - do it. Do not scrub the list on the 31st day, for you will have already violated you procedures set forth in you AML manual. Do not offer to do something every month. Scrubbing your list of clients against OFAC on January 31 and than again on Feb 1 - is not effective and it looks like every two months based upon days.

AML policies are living documents, they change and are amended as the laws change as your business changes, as technology changes, etc... For example, Molly drafted your AML policy and it was accepted by FINRA, FDIC, OCC and you insurance company. Molly has done well and was promoted, and her spot in compliance was filled by Carl - call began to automate some of the work and thus changed the AML policy to reflect the automation. Carl was hired away by an executive recruiting firm and Lars was hired to replace Carl. This is a common story for many very diligent people in compliance. Lars was on the job for 30 days when an event occurred and the regulators have come to see if you followed your policy. They will have read the policy you on file with them and will be surprised to find that you have not followed your policy. This is the beginning of a feeding frenzy for the inspectors for they live to find fault with anyone they investigative (I admit that is a dramatic overreach -

well, kind of), but it is true that this is how many of the regulators think.

How does one avoid this - simple, but your diligence is still required. Track all updates changes and why the policy was updated or changed. Send copies of the update AML Manuel to the appropriate regulatory authorities as well as your insurance company. Thus all are informed and cannot say they were not informed of the changes.

This level of diligence is also impressive to both regulators as well as insurance carriers and should help in addressing any questions these stakeholders in your compliance might have, and demonstrate not just your honesty but also your authentic attention to detail and compliance.

Companies get into trouble when they don't have any processes, or when they have a process - but they don't follow the process.

7. Book and Product Reviews - Help Your Employees Get Through Failure

By Gail Kasper, Author and Mentor of the Top 1% Club <http://www.gailkasper.com>

I am sure many of you, like me, have had to lend a supportive ear to an employee or associate. If you're a manager, business owner or boss, you're well aware that not every employee is a star performer. Some members of your team might struggle more than others. They may experience a greater incidence of failure. But even your best-performing employees will run into failure from time to time. That's because where risk and success are involved; failure is part of the territory. As the boss or head of the team, you can take steps to help all of your employees – those who struggle and those who shine – get through failure and get back on track. First, review the steps of my Systematic Attitude Development-Technique™ (SAD-T™), a proven program for achieving extraordi-normal results. Then do the following:

1. Set up a meeting. Don't let your employee languish in his or her misery and defeat. Saying nothing will only magnify your employee's feelings of failure. Set up a meeting in your office to talk to your employee and help put things into perspective. Keep this a one-to-one, face-to-face meeting. Don't bring others in, as this might prove intimidating.
2. Keep it logical. Be sure to keep your comments fair, kind and balanced. This is not the time to make your employee feel worse by bringing judgments and emotions into the conversation. Instead, talk about what's working well, what needs improvement, and where to go from here. Point out the fact that all great successes are preceded by failures. It's simply part of the learning curve. Without failure first, there is no ultimate success.
3. Define an action plan. The best way to defeat failure is to put a plan for

success into action. What steps can your employee take to improve his or her performance? How can you help your employee do a better job? Would the employee benefit from taking classes, attending a seminar, reading a book, or working with a mentor? Together, you and your employee can develop an action plan designed to make them a winner.

4. Follow up. Every week, follow up with the employee to see how they're doing. During these follow-ups, be sure to build your employee up by praising both effort and success. Modify the action plan as needed to maximize its effectiveness. Remain positive and optimistic, a source of encouragement. Once your employee is back on track, you won't need to check back weekly, but do follow up from time to time. By staying in the loop, you'll help resolve issues before they escalate, and your employee will know that they can count on your support, come what may.

As the Top 1% Club Mentor, I invite you to be our guest <http://www.top1percentclub.com> and receive a list of 50 Ways To Fix Communication Mistakes: Essential Keys To Improve How You Communicate With Others.



8. Subscription/Unsubscription/Copyright Information -

•• ÆGIS is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2012 by The Aegis Journal, LLC. It is edited jointly by L. Burke Files (LBFiles@feeinc.com), Gregg Lowney (Greg@feeinc.com) and Shaun Hassett (SHassett@feeinc.com).

Financial Examination & Evaluations, Inc. (FEE, Inc.) provides services in three areas, too specialized to be dealt-with in-house, that can adversely affect domestic and international bottom lines.

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

information.

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

FEE, Inc. 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 more information please visit [Financial Examinations & Evaluations, Inc.](#)

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

Subscription to **ÆGIS** is available for \$15 per year in North America and \$25 per year outside of North America.

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

To be removed from the subscription list, send an e-mail to unsubscribe@aegisjournal.com.

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

If there is a topic that you would like to know more about, please send your request to editor@aegisjournal.com and the editors will consider it as the topic for an article in an upcoming issue.

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

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

Submission of an article for publishing consideration certifies that:

(a) all information in the article is in the public record, or (b) that you are authorized to release any personal or corporate proprietary information contained in the article, and (c) that none of the article has previously been copyrighted.

The submission of materials for publication in **ÆGIS** constitutes a license to **Aegis Journal, LLC** their assigns, associates, or affiliates, to abridge and/or edit said submission, and to copyright and publish/republish any submitted materials in whatever written and/or electronic form they may choose.

If you would like to go beyond normal fair-use in reproducing articles from this issue of **ÆGIS**, you may do so freely as long as appropriate source, copyright, accreditation, and link to the **ÆGIS** Web site is included.

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.