



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 3 Number 2, February 2000

From the case files of

The LUBRINCO Group

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

and

Financial Examinations and Evaluations, Inc.

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

Concealed assets in fraud, theft, and divorce? Call us!

This month's features:

- 1. Due Diligence — Criminals do it...**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — CI for the small company or individual**
- 3. Executive Protection — Kidnapping in Mexico**
- 4. Technical Issues — Securing today's health care applications**
- 5. Real Stories from the Field — Sports book scams**
- 6. Book and Product Reviews — Undercover // Digital Detective**
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Criminals do it...

We recently worked on a metha-amphetamine production and distribution case. Several officers were sent undercover to pose as distributors and purchase large amounts of drugs. Several other officers, in an unrelated case, ended up assisting the drug's producer in the laundering of the proceeds of the transactions. All of the officers, though in real and great danger, executed their undercover roles with professionalism, integrity, a great deal of success, and without injury.

One of the keys to their success was training, more training, and yet more training still. They were trained in the ways and lingo of the drug manufactures and distributors. They were trained about the drugs and how to test for quality, consistency, and with what the drugs may have been cut.

All drug purchases begin with a sample being tested in the presence of the sellers. Further, each new batch is tested before acceptance: Distributors don't buy drugs cut so much as to be worthless. On several occasions the drug consignments *were* cut, leading to a substantial reduction in the price they were willing to pay for the altered goods. This was a deliberate exercise of due diligence by the drug manufactures: If the altered goods were accepted, the manufacturers would have suspected that the cops were cops, and likely killed them on the spot.

On the money laundering side, large amounts of cash were regularly handled by the drug manufacturers, and placed with a variety of middle men for laundering. As a normal exercise of due diligence, the middlemen would periodically receive counterfeit cash as part of the money to be laundered. If the money launderers weren't technically competent they would get arrested. The drug manufacturer used the counterfeit money as a way of having law enforcement weed out the incompetents in their organization.

The officers posing as money launderers told the drug manufacturer that any counterfeit money sent to them would be kept, and doubly deducted from their final payout. After two instances of counterfeit money being shipped to the officers, being detected, and being (true to their threat) double deducted, no more was sent.

Criminals are risk-averse businessmen. There are no contracts and there is no trust, hence everything must be verified upfront before a transaction is completed. Criminals don't give front money, but always ask for it (this is a familiar theme to our readers). Validation of the goods and payment in a transaction is *always* done up front. Criminals will also do a substantial

amount of due diligence before they ever do business with anyone: They want their suppliers and customers to be whom they say they are, and not rip-off artists or cops.

Criminals do due diligence — why don't you?

2. OPSEC, Economic Espionage, and Competitive Intelligence — CI for the small company or individual

We are often asked whether a small company or an individual can make use of CI, particularly if they have limited financial resources. This question becomes self-answering if it is rephrased as “Should we know what our competition is doing, and where our market may be moving?” Obviously, the answer is yes.

Once stripped of the mystique of the term competitive intelligence, finding out what is going on in your world becomes relatively straightforward.

- Look at trade publications, and at the presentations being made within trade organizations
- Look at newspapers and magazines for stories relating to the field, and to people and companies involved in the field.
- Look on the internet for anything relating to the field or people and companies involved in it.
- Talk to people involved in the field, or business related to the field.

To a large extent this covers most of what is done in CI. It is true that there is information that is most-easily available from for-pay services, but much of it is also available for free, although at a greater investment of time. Your tradeoff therefore becomes one of time against money.

On the other hand, if you are a small enterprise your need for masses of information are much less that of a large enterprise. And, cold as it might sound, your risk is less: If a one-person goes out of business it is tragic for that person and his family. If a company misjudges and closes a business it may be tragic for several thousand people and their families.

One might compare CI to running or some other athletic endeavor. For the beginning runner any shoes which fit comfortably will be acceptable, and a pair of \$200 running shoes will bring no competitive advantage over a pair of \$80 shoes: You are simply not good enough to have the shoes make a significant difference. As you get better and come closer to your personal limits, equipment will start to make a difference. But better running shoes

will not make the difference between running a 3 hour marathon and a 6 hour marathon: At best they will make a difference between a 3 marathon and a 3:10 marathon.

The moral of this is that you need to know your business, and have some idea of the kind of information you need to prosper, and the amount and depth of it. As you grow and your information need grow, then your expenditures on information can grow. Until then, let common sense be your guide in gathering the information you need to run your business.

3. Executive Protection — Kidnapping in Mexico

Contributed by Antonio Benavide, Chief of Police, Escobedo Police Department, Nuevo Leon State, Mexico (ipacitef@prodigy.net.m). Contributed articles do not necessarily reflect the viewpoint of the *ÆGIS* e-journal.

History

Kidnapping in Mexico began to grow from background criminal events to the current forefront of criminal activity during the early 1990s. Both the crime itself and the methods appear to have grown out of the activities of Colombian crime organizations, and were exported to Mexico along with the cocaine trade and thousands of “bad guys” who invaded the streets and schools of Mexico in the 1970s. In the 1980s the kidnappings spread throughout South America, where the methods and target selections process were refined and then exported to Mexico.

During the early 90s, political terrorist groups like EPR, EZLN, and others carried out a series of important kidnappings in Mexico. One of the first was the kidnapping of the president of BANAMEX, the most important bank in the country. That was followed by the taking of a Japanese executive at Tijuana B.C. These kidnappings were about money, terrorism, and political change.

Kidnappings today are just about money. They are carried out by criminals who include former police officers, former military personnel, and drug dealers. There are few or no political warriors, just thieves like Daniel “earcutter” Arizmandi, kidnapper of more than 100 people in Mexico City and the surrounding area between 1995 and 1998, when he was captured. The targets are the wealthy, owners of restaurants and jewelry stores, landowners, and ranchers: people who have money, but no bodyguards or armored cars. Currently, Colombia holds first place in the kidnapping and extortion sweepstakes, with Mexico in second place and Brazil coming in third.

In Mexico the issue has become a political one that reaches to the President's office. In 1998 it resulted in the resignation of a state governor, Carrillo Olea of Morelos, whose chief of police was revealed to have been involved in the murder of hostages by his officers, and whose officers were responsible for most of the state's 6 kidnappings each day. Following a relentless press campaign and demonstrations on the streets of Cuernavaca, the capital of Morelos, President Ernesto Zedillo was forced to call for an investigation, which resulted in the conviction of the chief of police.

Today, the highest crime rate are in Guerrero, Oaxaca, Michoacan, Jalisco, Sinaloa, Morelos, and Mexico City. Most of these states are located in the south, where drug cartels and guerrilla groups operate, and where the situation is compounded by poor police training and systemic corruption.

Methods

The most popular method is the "express kidnapping," in which someone hits your car from behind and waits for the driver to get out to discuss the accident. The driver is then seized and forced to withdraw money via credit card at the nearest ATM.

Another method is to wait for a likely victim near an ATM or cash point, forcing them into a car and demanding money and jewelry. The kidnappers will often claim to be police officers, and produce a fake badge, or pretend to carry out an arrest. Occasionally they *are* police officers, as was the case in Oaxaca City where four federal officers were prosecuted for kidnapping in November, 1999.

With the growth of the problem, the Federal Government has begun to organize special teams into police departments. The PGR (federal police) and some State Police have proper SWAT teams trained by FBI instructors and Surete personnel from France.

While systematic kidnapping and extortion aimed at foreign corporations is not yet widespread, this does not mean that there is no danger, nor that foreign corporations will not be targeted in the future, nor that a high level of security in this high-risk environment is not called-for. As always, prudence in this regard is well advised.

4. Technical Issues — Securing today's health care applications

Contributed by Mike Rothman, mrothman@shym.com, executive vice president of SHYM Technology, a software company that makes secure transactions using PKI less costly, faster to implement, and more manageable. Contributed articles do not necessarily reflect the viewpoint of the AEGIS e-journal.

The healthcare industry is beginning to rely on the Internet as a fast and effective way to share information. Electronic transactions have the potential to dramatically reduce the growing cost of medical paperwork, estimated to be more than \$10 billion annually.

As healthcare industries increasingly turn to electronic communications, it is necessary to utilize information security technologies to ensure that confidential patient data remains confidential. Electronic credentials used to assure identity become a critical part of the process for securing sensitive patient records and proprietary clinical research data. Often, these electronic initiatives create security concerns and headaches for time-pressed IT managers, as they constantly strive to keep passwords synchronized and up-to-date, while simultaneously handling the flurry of requests regarding forgotten passwords and other complaints. As a result, many hospitals, and other businesses looking for the most advanced security technology, are turning to digital certificates.

Digital Certificates Prove Identity

Much like a passport proves identity in the offline world, digital certificates issued via Public Key Infrastructure (PKI) technologies deliver a way to prove identity in the online world. PKI is fast becoming the cornerstone of the information security infrastructure. PKI is the only security technology that ensures people are who they say they are, provides a digital audit trail of activity, and also proves that documents haven't been tampered-with. These are critical functions in all healthcare activities from confidential patient data to clinical trials.

How Does PKI Work?

Here's a simplified look at state-of-the-art PKI *passports*, how they can be applied in several healthcare application scenarios to increase security, how they improve productivity, and how they reduce the number of passwords users must remember — and that IT administrators must track and manage.

PKI uses *keys*, which are extremely long prime numbers, to identify users. Two keys are involved: A private key, to which only the key's owner has access, and a public key, which is stored in a public directory and can be accessed by anyone. The two keys work together so that a message scrambled with the private key can only be unscrambled with the public key and vice versa. The more digits in these keys, the more secure the process.

Just as identities are proven by handwritten signatures offline, *digital signatures* are used to prove identity online. But without actually seeing the sender sign the document, how can it be proven that the sender is who he says he is? This is where public key cryptography comes into play. A piece of data is run through a complicated mathematical computation to generate another number, which is called a *hash*. The original data and the hash are inextricably linked. If any part of either changes, the hash will not match and the message cannot be decoded.

To digitally sign a document, a hash is taken of the document and then signed with a user's private key. Data scrambled with a private key can only be unscrambled with the corresponding public key. The receiver can verify the validity of the document and the identity of the sender by unscrambling the hash with the shared public key and then checking that against another hash computed from the received data.

If the hashes match, the data was not tampered-with, and the sender's identity can be verified. However, since the receiver did not witness the sending of the message, how can one be sure that the sender's identity was not forged? This is where the concept of *trust* enters the system, creating the need for a certificate authority (CA) to verify all online identities.

The CA is similar to an online passport bureau: A trusted entity that makes the PKI system work. All users on the system have software within a browser that generates both the public and private keys. As part of the certificate issuance process, the public key is sent to the CA, which verifies a user's identity (using credit reporting information or other offline credentials), and then signs the user's public key with its own private key, also known as the *root key*. The combination of the user's public key and the signature of the CA forms an individual's digital certificate. The root key is similar to the machine that applies watermarks to the passports. Digital certificates represent online passports, and are validated by the CA's root key.

Through the use of digital signatures, patients can feel secure when confidential data is placed online. The Internet allows information to be shared instantaneously, allowing doctors to care for patients in a more effective and efficient manner. For example, a patient's general care physician can easily share the patient's medical history with a specialist at another location. The general physician would use the specialist's public key (stored in the specialist's digital certificate) to scramble the message. When the specialist receives the message, the private key is used to unscramble it.

Since no one else possesses the specialist's private key, only the owner of this key can unscramble the message.

The process is similar in complex transactions. Let's say a doctor at a medical facility wants to look at the latest test results for a patient who is hospitalized. The doctor simply logs on to the hospital's extranet, after completing the process of obtaining credentials from a trusted CA. The doctor then uses the assigned private key, which can be stored on a machine, smart card or another device, to send a digital signature to the extranet server. The server receives both the doctor and the CA's digital certificates to validate the signature. This transaction requires only a few seconds and, because all information needed is electronically stored in the server, is actually simpler than a traditional ID/Password login. A user only needs to ensure that his or her private key is activated, and this is accomplished by entering in a password authentication, or inserting a smart card into a reader. And, unlike a simple ID/Password login, PKI authentication cannot be sniffed, spoofed, or compromised in any way. Digital certificates also provide a legitimate audit trail of the process.

Benefits of Digital Signatures

Every facet of the health care industry has traditionally relied on volumes of paper to track down patient history, treatments, and insurance claims. In the electronic world, it is critical that health care organizations be able to track *who* is changing documents, *when* they changed them, and *why* they were changed. In fact, the FDA has mandated that electronic signatures be added to documents filed electronically, to provide some measure of accountability to the transactions.

Digital certificates allow the creation of a digital audit trail that highlights what documents have been accessed, who accessed them, and for what purpose and for how long they were accessed. The near-certainty of litigation for claims or malpractice makes it all the more important that changes to the electronic documents are tracked and validated.

We can take the example of a standard operating procedure (SOP) which has been filed with the FDA. Many pharmaceutical companies house the SOPs in a document store, such as *Documentum*. The specificity of drug manufacturing (as well as what is at stake) requires a change to be filed anytime the process is altered. Attaching a digital signature to the change request allows the FDA to validate that an authorized entity requested the change, and provides an audit trail in the event of dispute.

Digital certificates also help provide reduced sign-on functionality to electronic transactions and systems. With traditional client/server or Internet-based systems, users typically log into each system they use individually. Not only does this require enormous time and energy, the user must remember a significant number of passwords. To cope with lots of passwords, users often choose a single password for all applications, and change them infrequently. IT managers must not only be track an ever-changing pool of employees and passwords, but also deal with the flurry of help desk calls revolving around forgotten, expired, or altered passwords. This creates a potential liability when dealing with patient records, since it is imperative that these documents be viewed only by appropriate parties.

Digital certificates and the policies underneath determine the access levels and authorization of the user, providing a single authentication mechanism for all PKI-ready applications and systems. For example, a PKI-ready application could challenge the user to present his/her electronic credential, in the form of a digital signature, to access the system. Users would not have to keep logging in as they access various parts of medical documents, as the other applications would directly ask the system for the needed electronic credentials in lieu of an ID/Password login.

Administration will continue to be a huge issue as more applications and critical patient data are exposed to external constituencies in the form of doctors, specialists, and insurers. The ability to utilize one credential to gain secure access to many systems will have a drastic impact on system administration costs, especially given the fact that upwards of 60% of an organization's security budget is spent on administrative tasks like resetting passwords. Reduced administrative costs would allow for money to be spent on other critical medical functions.

Securing the Healthcare Industry

While PKI is slowly gaining popularity, it is important that the thousands of applications used throughout healthcare today become PKI-ready. Applications must be designed to ask users to sign data, and know how to validate that data using the certificates. Tremendous progress has been made recently to extend PKI to the application level, but there is still a long way to go. E-mail, a key business application, provides rudimentary support for digital certificates, yet it's still very complicated to use. Third party software providers allow enterprise applications such as *Documentum* and *Lotus Notes* to support PKI. As PKI becomes a widely-used technology, it will be possible to bring the healthcare industry to the Internet in a secure manner, resulting in more effective and efficient patient care.

5. Real Stories from the Field — Sports book scams

Before we get into the specifics of sport book scams, it is important to know how a sports book makes money. It makes money on the *vigorish* or *juice*. This is the difference between what they will pay on both sides of a bet and what you wager. The vigorish or juice is usually about 10% of the *action* (action is the amount bet). It is also important to get the wagering to be equal on both sides of a game: \$100 dollars on team Bee and \$100 on team Flower is \$200 in action and represent a \$20 profit no matter who wins or loses. If the betting is lopsided, such as having \$150 on team Bee and \$50 on team Flower, this is still \$200 in action, but the bookie now effectively has a \$100 uncovered exposure (wager) against team Bee. A good bookie is not looking for risk, he is looking for an actuarialized profit. The insurance industry grew out of modern mathematics and gaming, and the language of insurance is also the language of a good bookie.

The scams

Tout sheets

Re-prints of a subscriber newsletter from the *Lombardi Sports Wire* in Oceanside California are identical except for the paragraph on the game to bet. The game was Pitt v. Notre Dame. In one letter the Notre Dame is touted to beat Pitt by 30 points, in the second edition of the newsletter Pitt is touted to beat Notre Dame by 14 points. Both were touted as “Guaranteed Blowouts.” At a minimum this generates even action, so the bookie can make profits on an actuarial basis. These letters also remind me of the old gold or stock broker solicitations. 100 contacts are made and 50 are touted on something going up and 50 on something going down. These touts are followed by letters saying the same thing. Once a significant move is made the 50 touts and letters that were correct are called back and touted again: 25 about the price of a something going up and 25 about something going down. After the end of each round the potential investor is solicited to open his account with the touter since the touter is obviously giving his valuable and quality advice not for free but to get people to open accounts. This pressure is continued all the way up the chain of touts, each time showing the persons receiving the letters showing how much profit one would have made by investing with the touter on each of the recommendations. The touter will continue to call until the person either invests or tells the touter to get lost. The same thing is true with the sports book people.

1-900 numbers for sports betting

Many 900 numbers charge only \$2.00 per minute, but they talk slower than molasses in January.

Consensus services

While consensus services are a good way to improve your odds, several of the consensus services just make up the numbers as they go, and, thus, don't actually represent the strong plays versus the light plays.

Sports Service Monitors

Last, but certainly not least, are the sports service monitors. The sports service monitors supposedly rank all of the touters on their performance, but in truth most of their results are rigged, and rigged in favor of those who pay them the most. Typically for a fee of \$300, the book can call in all of the picks for college and pro-football on Friday and Saturday. But for a Fee of \$1,500 they can call in the picks that following Tuesday!

Recognizing a bad sports betting operation is fairly easy: The first question out of their mouth is "What is your phone number?" If so, then you have a problem. They are looking for bodies to bet with, or to sell your name and phone number to a *mooch list* compiler. You will also notice that several of the firms have different prices for different picks. Some are \$300 per month and some are \$1,500 a month. The higher rated picks go to those at the \$1,500 per month fee and the lower rated picks go to those at the \$300 per month level. They are all good picks, but like wines, some are better than others. These people are selling an intangible service, and some believe that if you pay more you get more. Not so: Quality is only determined by results, not by cost.

International Sports Books

Many sports books are going to the international scene and communicating through the mail, internet, and telephone to service their customers. Most of these services are legitimate but have heavy and significant operational difficulties. Many operate out of countries where they are licensed to take bets, and to do so from citizens that are betting from within a county where the bet maker is *not* recognized may be an illegal act. In the past, many of these operations could and would take a credit card as a method of payment. However, Visa, Master Card, and American Express do not like their credit being used for gaming, and have suspended or removed privileges from

merchants and banks that knowingly accept credit generated from gaming for deposit.

Also, a recent decision in a New York court allowed a woman to regain almost \$85,000 in losses she had accumulated with an offshore sports book charged against her credit card. The court's decision was very clear. Gaming was illegal, and a contract for an illegal purpose was not enforceable. All losses were ordered refunded to the woman from her credit card company. Most offshore sports books are working against house accounts established through the wiring of funds to these wagering houses, and are distancing themselves from credit cards.

The Future

It is probably only a matter of time before legislation in various countries, or economic pressure, forces many of the offshore books to be excluded from business in certain countries. Also, with the increasing costs of transacting business, the cost of operating a sports book are going to increase. That includes both fixed and variable costs. This economic change, too, will have its effect. Books in low-overhead but properly regulated jurisdictions such as Dominica, St. Kitts, Bahamas, and Antigua (to name a few) will probably survive any down-turn in business.

6. Book and Product Reviews

Undercover - 2nd Edition

Motto and June

CRC Press

<http://www.crcpress.com/> 1-800-374-3401

This is an excellent book. It takes the reader throughout the career of Carmine Motto with his service to many communities, different branches of law enforcement and several operations. The stories told are entertaining and clearly illustrate the points made in the text. They are not all success stories: No career can be completely successful unless you're lucky, make one bust, and quit. But, rather, through successes and failures the points, and the importance of police undercover operations, are demonstrated. Sections of the book include chapters on working with informants and setting up and conducting undercover operations. Tactics are discussed throughout the book, preparation is strongly (and correctly) emphasized, and attitude and psychology for the undercover officer are presented. This is a strongly recommend purchase for anyone training undercover agents, and a strong

buy just for the readability of the book. Well done Carmine Motto, Dale June, and CRC.

Digital Detective

CBT Training 1(800) 482-0211

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

This is a comprehensive interactive CD for the high tech investigator. It covers hardware, software, networks, computer safety, hacking, investigative training, computer forensics, and current laws. It contains approximately 1,200 hours of training for the computer investigator, and has some real benefits over a classroom. The student can go back over the material if it is unfamiliar, and skip those areas with which they are familiar. We had three different professionals review the CD: An attorney, a computer expert, and an investigator. The attorney skipped the legal sections and went right into the computer and software stuff. The computer expert ignored the stuff on hardware and software but real enjoyed the section on law and investigations. The seasoned investigators said that if one in 10 cops, prosecutors, or judges knew some of this stuff it would make his life a great deal easier in trying to get computer crimes prosecuted.

7. Free-Subscription/Unsubscription/Copyright Information

•• AEGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2000 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 2001* and the *EU Revised Money Laundering Directive of 2001*.
- **Protection of management, staff, and families.**
 - In the high-threat environments of Latin America, Africa, the Mid-East, and Southeast Asia.
 - When traveling and living overseas.
 - When transporting items of substantial value.

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

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

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

To subscribe to our AvantGo channel, go to http://avantgo.com/channels/_add_channel.pl?cha_id=1773

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

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

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

If you would like to submit an article for publication in ÆGIS e-journal, send it as an attachment to an e-mail to ejournal@lubrinco.com. Submission of an article certifies that (a) all information in the article is in the public record, or (b) that you are authorized to release any personal or corporate proprietary information contained in the article, and (c) that none of the article has previously been copyrighted. The submission of materials for publication in ÆGIS e-journal constitutes a license to The LUBRINCO Group Ltd, Inc.,

and/or Financial Examinations and Evaluations, Inc, their assigns, associates, or affiliates, to abridge and/or edit said submission, and to copyright and publish/republish any submitted materials in whatever written and/or electronic form they may choose.

If you would like to go beyond normal fair-use in reproducing articles from this issue of ÆGIS e-journal, you may do so freely as long as appropriate source, copyright, accreditation, and link to the LUBRINCO website is included. This should be in the form

Article Title, from the February 2000 ÆGIS e-journal (© 2000 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.