



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 5 Number 6, June 2002

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 — Terrorism and insurance**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Loose lips**
- 3. Executive Protection — Too much, already...**
- 4. Technical Issues — Why you should bring your own driver overseas**
- 5. Real Stories from the Field — HIPAA compliance in health care**
- 6. Book and Product Reviews — Symantec Security Response Mailwasher**
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Terrorism and insurance

Insurance after 9-11

The US had been a virtual island in the sea of the world's political attacks up to and until that day, and financial losses from terrorism were not on the list of an actuary's most-likely or even -costly events. However, that changed dramatically when four planes were hijacked and three were flown into occupied buildings. It was a forty billion dollar blow to the insurance industry.

Most of the financial loss was shifted from primary insurance companies to what are known as reinsurance companies. Reinsurance companies are those companies that insure insurance companies against losses over and above a certain level. For example if a client has purchased a \$1,000,000 liability insurance policy for his gas station, the primary insurance company may purchase from (or lay off to) a reinsurance company \$900,000 of this risk. Thus, if there are any losses the primary insurance company will pay the first \$100,000 out of its own reserve, and the reinsurance company, through the primary insurance company, will pay any balance up to the policy limits over and above the \$100,000. Like loan syndications by banks, reinsurance provides the insurance industry the opportunity to diffuse the effect of major losses by one insurance carrier to a number of insurance carriers.

After a forty billion dollar loss, the reinsurance industry began shedding its exposure to losses cause by terrorism. Losses caused by terrorism became a named exclusion to coverage. These changes occurred, for about 70% of the reinsurance policies, at midnight December 31, 2001. The remaining will incorporate terrorism as a named exclusion to their policies at midnight on July 31, 2002. As reinsurance companies walk away from coverage, it has exposed all of the primary insurance carriers to the losses caused by terrorism until the primary policies with clients have been re-written at the policy renewal dates to mirror the exclusions in the reinsurance contracts.

This overlapping period has a regulatory hurdle to overcome: Before most carriers can change their policies, the changes must be approved by the insurance commissions for the states in which the policy is offered. This caused the Insurance Service Office (ISO), which develops standard policy contract language for use by property and casualty insurance companies, to file a request in every state for permission to exclude terrorism from all commercial insurance coverage. By February 22, 2002, forty-five states, including DC and Puerto Rico, had approved the exclusion. However, most

states already provide that major or sophisticated purchasers of insurance can negotiate their individual policies directly with the insurance companies. Thus, it is assumed – and feared – by many small business groups that most policies were renewed with the terrorism exclusion included, with most business policyholders wholly ignorant of this change.

While this may not seem like a big deal to most small business owners, legislators are already reviewing the “overly broad language” of these so-called terrorism exclusions. Terrorism thresholds for exclusion are from twenty-five to fifty million in serious casualties, with an all or nothing threshold (insurance companies pay nothing if the threshold is reached), or the aggregate losses from multiple incidents with a 72 hour period and across most of North America into one event if the events “appear to be carried out in concert or to have a related purpose or common leadership.” Further, some exclusions go as far as to exclude coverage if their purpose behind the attack was to cause fear and or terror, and was an organized attack.

Interestingly, some states also require that fire insurance cover the losses caused by fire no matter what the cause. So, with the attack on the World Trade Center, a policy would not cover that damage done by the impact but would have to cover the losses caused by the fire, which has been blamed for the subsequent collapse of the towers.

Economic Consequences

The real problem has stemmed from our US legislators and their never-ending campaigning to get their face on the TV or in the newspaper. Many states have passed bills and penalties for domestic terrorism. Many of these domestic terrorism events have to do with domestic incidents and refer to such things as a home or a dwelling and how the occupants in it behave poorly: Shouting, yelling, punching, shooting, etc.... They have nothing to do with political terrorism such as the Puerto Rican Nationalists shooting up DC, the bombing of the Oklahoma Federal Building, or the criminal acts at the Twin Towers and the Pentagon. All of these domestic terrorism bills have provisions whereby a person can be charged with anything from a misdemeanor to a felony for stalking, harming, and threatening to harm. So why is this important?

Assume the following: An irate ex-husband throws a Molotov cocktail through the window of his ex-wife’s trailer. She escapes, but the trailer and all of the 10 trailers around it, and a Circle K, are burnt to the ground. Can the

insurance company claim that because the perpetrator was charged with an act of domestic terrorism the insurance company is no longer obligated to pay?

Or take the case of a disaffected employee who begins threatening a company and its employees with harm, destruction, etc.... The ex-employee carries out such a threat by blowing up a small portion of the plant, killing 12 people and shutting down that portion of the business. Can the insurance company claim that since this was an act of terrorism none of the damages are covered? Further, can those companies that have insured the lives of those persons who were lost claim that since their demise was caused by an act of domestic terrorism they, too, are excluded from coverage? Can the liability policy for the company refuse to pay the claims made by those of the decedent's family and of the injured survivors because this was an act of domestic terrorism? It is a thorny problem.

It will be interesting to see how the domestic insurance industry deals with the letterbox bomber who wanted to "put a smiley face on the map" through the plotting of where he put his bombs.

But can you get terrorism insurance? Yes, of course, but like residents in California who live on a fault line, the insurance will tend to have high deductibles and tight limits and criteria on coverage.

The owners of a small Midwestern shopping mall reported that when their all-risk insurance policy on the mall property expired at the end of 2001, they were forced to purchase a terrorism excluded policy because they could not find an all-risk policy that included terrorism. The mall's mortgage lender objected to the terrorism-excluded policy stating that the mall was out of compliance with the "all-risk" policy required in the loan documents. The lender then purchased a "terrorism" policy to supplement the mall's new policy and demanded to be reimbursed for the premium. The premium demanded for the terrorism policy was three times the previous year's "all-risk" (with terrorism not excluded) policy. The mall went to court and successfully obtained a temporary restraining order to prevent the lender from forcing repayment of the terrorism policy premium. The lender argued that it was now being forced to assume the risk that it had not previously priced into the mortgages, and is thus forcing the mortgage holders to obtain coverage. The lender also recognizes that the unavailability or the cost of terrorism insurance will negatively impact the mortgage lender's ability to service the loans or even bundle and sell the loans.

A New York construction firm has been told by its financing sources that they will not provide financing for the 30-story apartment complex unless

the construction firm can get terrorism coverage. Terrorism coverage is not available. The project will not proceed.

An Alexandria, Virginia, office building owner cannot get terrorism insurance as required by the lender for an \$80 million office building. The building will be put into Chapter 11 and operated as a bankrupt entity to prevent the current mortgage holder from foreclosing.

The buyer for an office building in Chicago (for \$300 million) could get terrorism insurance for six million dollars. The buyer had budgeted \$75,000 for all of the building insurance needs, and this new premium represents over 11% of the gross rents of the building. The building is not saleable.

The issues raised by this article are the heart of the debate that has been raised by the GAO and the risk managers of many portfolios whose assets, once thought to be protected, are now exposed by this uncertainty. Many projects have already been cancelled by the project owners when the financing requirements required protecting from terrorism. Projects such as new power plants and water facilities have been the hardest hit. These types of project bonds are typically purchased by very risk adverse funds managers for “widows and orphans” type investments, and require all-risk policies. Other existing projects have had to go bare, without terrorism insurance, since it was unaffordable or unavailable, thus shifting the risk once assumed by the insurance carrier to the owners and lenders. This has affected municipal power companies, water treatments facilities (public and private), ports, and harbors and bridges. The problems are particularly acute for businesses in central business districts, and for privately held facilities considered to be likely potential targets of terrorism such as power plants, water treatment facilities, and the like.

So how does a company today address and assess the potential losses caused by terrorism? Very poorly, if at all. The whole process is currently panic-driven, as reflected in the increases in all of the PC rates including an average jump of 20% in homeowner policies.

We suggest that, for a start, you should read your policy and keep an up-to-date copy on hand. Further, require the insurance company to provide, in advance, a clear and meaningful definition of terrorism and its exclusions.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Loose lips

We were recently asked to gather some information on a company that had taken delivery of \$800,000 worth of merchandise, but had decided not to pay for that merchandise. The attorney asked us to find out what happened to the merchandise, and where the company banked so a “provisional remedy” could be implemented to attach this company’s funds prior to a judgment.

We sent in an investigator to look at the various types of merchandise sold by this company, and ask specifically for the merchandise that had been delivered but not paid for. It appeared, according to the store manager, that all of this equipment was shipped to a new company in another city that was a spin-off of the old company. The sales person was very knowledgeable both about the equipment and the business. We were told that the company had experienced some hard times and used the spin-off to settle a debt with another company and to lower the overhead by shifting employees and stores from the current brand to a new brand. This is more or less a chapter-and-verse description of a fraudulent conveyance of the creditor’s property secured by a UCC 1 Financing Statement. The ghost shopper continued to shop and when they had decided on a piece of equipment, offered to pay via a bank wire. The accountant, who was in the back office, provided the full coordinates for the bank-to-bank transfer of funds. These were given, and in 15 minutes the investigator had all of the information for a fraudulent conveyance action on top of a collection action, using the bank account information. For thoroughness, the investigator called back and said that since the wire was from overseas, a different bank would be preferable, and did they have a different bank that could accept the wire? Yes, according to accountant, they did: They had a Merrill Lynch money market account, and supplied the wire coordinate for that, with the accountant adding, “Gosh I hope this works; these are the only two accounts we have.”

For the investment of a few hours, including writing up the report, our investigator went to the store and got the entire recent history of the store from one of the sales persons. With a small-added pretext of trying to wire funds, he also got all of their demand-account information.

This was a collection matter involving a large sum of money and a debtor not behaving too well. But is this much of your information shared with those that will share it with the world? Have you identified what information is critical to your business and should not be shared? If your organization

has not identified information that is of value, and that shouldn't be discussed, you can have some measure of confidence that it has been and will continue to be shared with those who shouldn't know it.

3. Executive Protection — Too much, already...

A small but very prestigious law firm in Los Angeles received several threats against its employees. The partners agreed to retain a protective-services specialist to protect their staff, their workplace, and their homes, without fully understanding the implications. The specialist began by setting up certain protocols for the office and its staff and professionals to follow. The procedures were, in fact, not entirely unreasonable (we aren't really discussing the appropriateness of the suggestions here), and, had they been discussed with, understood by, and agreed to by the staff, probably would have, in a modified-to-produce-agreement form, worked well. As it turned out, things went well for the first few hours, at which point everything fell apart because the program successfully and simultaneously alienated the attorneys, the staff, and the clients.

For a client to come to the firm they needed both an appointment and a picture ID to enter the lobby of the building, and needed to be escorted to the elevator, and have all of the buttons pushed for them so they could not wander around the law offices. This may seem reasonable, since, as it happens, access control is the primary tool for building security. However, having picture ID has no more security value in getting to see an attorney than it does in getting onto an airplane (which is to say none).

Some celebrity clients did not want to show their driver's license for fear their real date of birth might end up in a tabloid somewhere. Some demanded to see their attorney whether or not they had an appointment. Attorneys, not wishing to lose their paying clients, came down to the lobby to pick up their irate clients, apologizing for the problems and stated that "of course this doesn't apply to you – you have been with us for years." Since the attorneys knew their clients, this was a far more sensible way to deal with clients than was the implemented program.

The attorneys themselves had a fit that afternoon when they saw that all of the assigned parking spaces with names on the spaces were painted over, and they were told to find a random spot and to *back* in. The attorneys objected to the removal of a prestigious-and-always-available parking spot, and the parking management firm, which of course had not been consulted, objected to the backing-in of the cars, since that was against *their* policy. As it

happens, named parking spots represent a real risk if there is an actual threat, as it positively identifies the target (much like being met at the airport by someone holding a sign with your name), but unless you understand the threat, the vulnerability, and therefore the risk, what you as the user see is a valued perk and bit of prestige being withdrawn.

By the end of day one, the primary life that was at risk was that of the well-intentioned consultant.

So what do you do if you are in peril? Or think you may be in peril? Or think it sounds sexier to your clients if you are in peril...?

- 1.) Retain a professional that understands the nature of both their and your business, and the fact that all risk management, no matter how small, affects your freedom to work and act at will.
- 2.) Review all of the proposed policies and make sure they address a specific set of threats and vulnerabilities (i.e., they make sense based on the risk), and send these policies to your employees for their comment. If they understand the risk, your employees will probably be able to judge what will work, as well as what is overkill and what is actually appropriate.
- 3.) Send appropriate notices to clients and vendors who may visit the facility to alert them in advance of the changes of which they need to be made aware. Remember: You are giving people the information they need to know, not producing a full disclosure document.
- 4.) Review all policies and procedures daily for the first week, weekly for the first month, and monthly for the first six months. Subsequent reviews should be undertaken on a three-month basis, or any time major changes take place at the facility (such as construction, layoffs, new projects, end of projects, etc).

If your countermeasures are appropriate for your risks, you will have minimum disruption and inconvenience.

4. Technical Issues — Why you should bring your own driver overseas

If you work abroad you may well be working in an area of higher or high risk, and certain security measures may be provided for you. For most of us, we imprudently assume that the people handling our security are knowledgeable. When it comes to security – particularly security in high-risk environments – “assume” might not merely make an “ass of you and me,” but can leave you kidnapped, injured, or dead. One area in which this is particularly true is the hiring of drivers.

Drivers have several responsibilities. One is to drive in a manner that is conducive to your safety. Security driving is a skill that requires a good deal of training, and if your driver has not been trained appropriately, you have a potentially serious problem.

There is an additional problem. In most cases where local drivers are hired, not only are they rarely appropriately trained, they generally don't make a lot of money, and are constantly being warned that if they damage their precious car they will be in big trouble. The reason this is a problem is that one of the primary rules of driving in high-risk situations is that in case of trouble you need to keep moving. What happens when there is a hijack attempt, and someone blocks your car with their car? Ideally, the trained driver will ram the bad guy's car, moving it out of the way (you can move a car two or three times your car's size), and you will drive to safety.

This maneuver is not overly difficult and is pretty safe, but it does involve training (which is fun, but leaves a trail of wrecked training cars). If your driver has not been trained, however, they will not have the knowledge or skill to do what is needed. If your driver *has* been trained, but has been told their career depends on bringing the car home unscratched, they simply will not be able to ram another car. Your own trained driver, brought from home, *will* be able to do so, thus greatly increasing your chance of survival.

5. Real Stories from the Field — HIPAA compliance in health care

HIPAA contained a provision that gave Congress until 21 August 1999, to pass comprehensive privacy legislation. When Congress did not enact privacy legislation by that date, the law required the Department of Health and Human Services (HHS) to craft such protections by regulation.

HHS published the final Privacy Rule on 28 December 2000. The final rule took effect on 14 April 2001. This rule gives patients greater access to their own medical records, and more control over how personal health information is used. The rule addresses the obligations of health care providers and health plans to protect information. By law, covered entities (health plans, health care clearinghouses, and health care providers who conduct certain financial and administrative transactions electronically) have until 14 April 2003 to comply. Small health plans have until 14 April 2004.

The HHS Office for Civil Rights (OCR) has implementation and enforcement responsibility for the Privacy Rule. OCR will conduct extensive outreach to consumers and health care providers to explain what the rule

means for them. OCR will also provide technical assistance and guidance to health care providers and other covered entities to help them comply.

On 6 July 2001 OCR issued the first guidance materials answering some of the questions about requirements for doctors, hospitals, other providers, health plans and health insurers, and health care clearinghouses. It also clarifies some of the confusion regarding the meaning of key provisions of the rule. The guidance and other technical assistance materials are posted on the OCR Privacy Web site at <http://www.hhs.gov/ocr/hipaa> .

But as often happens, a good idea has gone wacko. The cost of implementation for the privacy and portability issues required by this legislation are cost-prohibitive for most private physician practices. Most practices are just filing the required extension since most of them cannot afford the cost of compliance. In many offices there is one set price for medical services, but many different amounts to be paid for each service as is set by each individual insurance carrier and third party provider. It is not unusual for 60% of all charges to go uncollected, and for third party payees of medical bill to take 45 to 90 days to pay for a service. An average of 43% of the expense at a medical practice is related to administrative costs related directly to dealing with compliance issues and payment issues.

So, for the foreseeable future, compliance with the provisions of HIPAA will be postponed until an uncertain future date.

6. Book and Product Reviews

Symantec Security Response - Virus Definitions Download Page

Symantec Norton AntiVirus

<http://securityresponse.symantec.com/avcenter/defs.download.html>

While there are a lot of security issues with computers, for most of us the main one is the threat of viruses. It is critical that anti-virus protection be installed, and that virus definitions be kept current.

Many companies have put in mechanisms that will update virus definitions on a regular basis. As an example, current versions of Norton Anti-Virus have a live update feature that will download the most-current version of virus definitions – and sometimes program upgrades, generally on Wednesday afternoon.

While this is probably adequate for most of us, Symantec actually releases virus definitions *daily!* These updates are to be found at <http://securityresponse.symantec.com/avcenter/defs.download.html> . If you

happen to use NAV, we strongly urge you to bookmark this page, check it daily (or have someone check it daily for you, and that you download the updated virus definitions as they occur. The files are around three megabytes, which takes relatively little time to download, and the increase in security seems well worth the minimal effort.

It may well be that other vendors also update their definitions daily. Check with your vendor to see how they handle this issue.

MailWasher

Nick Bolton and eCOSM 2001

<http://www.mailwasher.net/>

Junk e-mail is an annoyance, a waster of resources, and a danger because of the potential exposure to unknown viruses and worms. Spam filters, which capture e-mail as it downloads and sends spam unseen to a special folder reduces the annoyance, but not the consumption of resources or the potential danger.

MailWasher is a free (you can make a small donation if you choose, and we understand that soon there also be a commercial version) e-mail **preprocessor** that allows you to look at mail on your POP3 server **without downloading it**, which can save a lot of download time, and avoids the risk associated with downloads. You can *delete* messages directly from the server. You can *bounce* messages (*MailWasher* will send a fake “address not found” message to the spammer, reducing the likelihood of getting repeat spam, then delete it from the server without downloading). It can identify spam (it can look at spam databases, plus has its own logic for identifying spam) and some viruses, and mark them for deletion (you can un-mark these if you choose).

MailWasher will also allow you to set up filters to mark messages, based on criteria you choose, for deletion or bouncing, either displaying the item or not, as you choose, and to identify e-mail addresses as friends or to blacklist them for automatic marking for deletion or bouncing.

We recommend deleting but not bouncing. Although bouncing may reduce the amount of spam you get, it also increases the amount of traffic. Since there is so much junk e-mail (we get between 9,000 and 10,000 pieces a month), it seems kinder to merely delete it on the server, and not burden the system with another 10,000 pieces of junk.

This is an excellent program, and well worth downloading and using as an email pre-processor before downloading your e-mail. When the commercial version appears we will recommend that, too.

7. Free-Subscription/Unsubscription/Copyright Information

•• ÆGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2002 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 2002* and the *EU Revised Money Laundering Directive of 2002*.
- **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 June 2002 ÆGIS e-journal (© 2002 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.