



**ÆGIS** e-journal

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

Volume 4 Number 5, May 2001

From the case files of

The LUBRINCO Group

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

and

Financial Examinations and Evaluations, Inc.

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

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

**This month's features:**

- 1. Due Diligence — CYA?**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Thinking about OPSEC audits**
- 3. Executive Protection — Family help abroad**
- 4. Technical Issues — Worms and other computer problems**
- 5. Real Stories from the Field — Wireless network party lines**
- 6. Book and Product Reviews — Secrets and Lies**
- 7. Free-Subscription/Unsubscription/Copyright Information**

## 1. Due Diligence — CYA?

We were asked to help develop a protective protocol for the annual conferences of a law enforcement trade organization. For some organizations – the *International Narcotics Enforcement Officers Association* comes to mind – a high level of protection is critical: A gathering in one place of the major players in the counter-narcotics field presents a real opportunity for the bad guys, and a tangible risk for the participants. For the training organization we were helping, the risk was markedly less, but the exercise seemed not-unreasonable, if only as an exercise in due diligence. The process of implementing the protocol would be particularly straightforward for this organization, as, between the host agency and its training academy, we had virtually unlimited manpower to deal with a known low level of threat.

As it happens, this kind of protocol is relatively straightforward. You figure out the areas of exposure and the areas that need to be protected. This would include the area where the conference would be held, as well as ancillary areas, such as parking lots, for example, might be covered. In addition, if the entire facility were not being used for the conference, the areas above and below the meeting areas might need to be protected from bomb threats (although, in this case the likelihood of a bomb threat against this particular organization was somewhere between slim and none).

Once the area to be protected is determined, it needs to be secured and inspected *before* the event, and, once secured, kept secure during the event, with no unknown person or thing being allowed into the secured area. All attendees need to be badged (with photo Ids if there is a belief that there might be actual risk), as does all staff. When the event is over the areas that were secured no longer need to be secured, and everyone can go home.

The protocol was quickly drawn up, and clearly explained *what* needed to be done, *how* it needed to be done, *when* it needed to be done, and *why* it needed to be done. The protocol was immediately bounced back to us, because we had forgotten to put in a mechanism that would clearly allow blame to be placed if anything went wrong. It took us a bit longer to re-write the second protocol, but finally managed to produce a document that met management requirements, yet still gave an indication as to what needed to be done.

When the conference took place we were not entirely shocked to discover that, in fact, the protocol had not been implemented. Were we upset? Not at

all! For a start, we knew that there was no special risk associated with this conference, and that, at worst, the membership faced no more than the normal risks of fire, theft, and other fairly standard hazards. Second, we deduced we had been asked to do this on the off chance that if there was a problem, the organization could transfer blame to the host agency.

One might ask if there would have been a benefit to actually implementing the protocol, and if that would have justified the cost? The answer is no, because the risk was so low. While the manpower was already in place, and there would have been no additional costs for having an officer or cadet at every door in a timely manner, there would have been some minor cost in verifying facilities staff and giving them badges (and verifying their use). Since extra protection – beyond what the hotel would normally supply for any meeting – was no more justified than it would have been for a bunch of Boy Scouts, taking no additional effort was probably the appropriate action.

The real question is whether we should have spent the time and money developing a protocol in the first place: That is to say, did the development of the protocol, without its actual implementation, demonstrate an exercise of appropriate due diligence on the part of the organization, which would have shielded it in the case of an actual incident? I suspect that while blame for not putting the protocol in place would have been attempted to be passed to the host agency, it wouldn't stick. Failing the *prior* development of a risk analysis showing that there was no need for additional protection, it would likely be shown that by developing, but not implementing, a protective protocol, the organization failed to exercise appropriate due diligence in the protection of its members.

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — Thinking about OPSEC audits**

There are four reasons (we are not talking of statutory requirements, but, rather of underlying reasons) why audits of *any* type, OPSEC or other, might be performed.

The first reason is that a program may be being implemented, and that we wish to get some baseline indicator of where we stand, in order to gauge what needs to be done, and to judge future progress.

A second reason to perform an audit is to judge the current state of a program. From this type of audit comes kudos for things well done and suggestions for improvement in areas where improvement is needed, either

because the program being audited has not kept up with changes in the environment, or because there have been oversights.

A third reason is to show that something is being well done, generally to bring attention to this to someone higher up the food chain.

Finally, an audit can be done as a thinly-disguised plan to place blame for something, generally on someone – or some group – in particular.

Since most organizations know little or nothing about OPSEC, we will focus here on the first reason for doing an OPSEC audit, which is figuring out where you stand and where you need to be going.

Most organizations have information that, while not actual trade secrets, is best kept private. This is because organizations have adversaries or competitors who could use this information to their advantage and your disadvantage. Sometimes this information is direct in and of itself, and sometimes the information is an *indicator* that information is out there. As an example of an indicator, if your employees suddenly start attending conferences in some specialized field it is probably an indicator that you are either looking to do something in that field, or are actually doing something in that field.

There are two things that must be done when you begin an OPSEC audit. First, you must identify who are your adversaries. This means specific adversaries, not generic adversaries. The reason for this is that you will be under attack by specific individuals, groups, or organizations, each of which will have different interests, histories, and capabilities.

The second task is, once the adversaries are identified, figuring out what information is valuable to *them*. Remember that what you think is important may not be important to your adversary. Also remember that life is not perfect, and you may make a judgment call that is reasonable, but wrong. Unfortunately, the nature of risk management is such that you can never completely eliminate risk. As an example, some time ago a company invented a new longer-lasting bulb, based on a newly designed filament. A foreign competitor was taking a tour of the plant, and was deliberately shown only the generic manufacturing processes, and nothing to do with the new filament. This gave the manufacturer some feeling of comfort – until their product hit the market first in the hands of their competitor. As it turned out, the filament specifications had been previously stolen in an act of economic espionage, but the company was lacking some of the base manufacturing knowledge for the simple construction of the bulb, information that was being given away.

While we have emphasized the importance of identifying specific adversaries and their information requirements, this does *not* mean that you should not identify the information that you think might be important: You will need to deal with this, also.

Once you have identified information that might be of value to others, and who those others might be, you will be ready to start dealing with the protection of that information, which we will address later.

### **3. Executive Protection — Family help abroad**

When we talk of executive protection we tend to talk primarily of reducing danger for our target client, whether this danger be from attack, accident, or embarrassment. Protective services is about risk management – vulnerability management, actually – not risk elimination, and its goal is to maximize the ability to be productive within an environment of risk. Because of this, we often also discuss the role of the protective specialist as *facilitator*, freeing the client to do productive work, and leaving the non-productive, or organizational work, to the protective specialist.

When discussing protective services abroad, we tend to discuss health issues and issues revolving around physical danger, such as kidnapping. We sometimes forget that in many overseas circumstances the issue that can be most destructive is not physical danger, but the psychological condition of the client's family. This is particularly true in areas that are culturally different, yet not fraught with danger.

An example of this is taking an assignment in Central (and sometimes even Western) Europe. While there will be comparatively little likelihood of physical danger, the environment is sufficiently different that, without appropriate preparation, the client's family is likely to have great trouble fitting in, and, in some cases, may even end up going back home. Whether or not the client stays alone or returns, their mission and productivity will, if they are appropriately family oriented, be damaged.

In most cases these problems can be prevented through appropriate use of the protective services staff, which is either in a position to make the family aware of the cultural differences they will encounter, and help them have at their disposal the tools to deal with the stressful situation, or to acquire the information from people like us.

By taking advantage of this internal or external expertise, the transition to comfortable living in a new environment can be more easily made. This leaves the client free to deal with business issues, rather than being

preoccupied with avoidable family issues. This is an important service that we, as professionals can offer. Make use of it!

#### **4. Technical Issues — Worms and other computer problems**

We have someone close to us who smokes cigarettes and doesn't wear a seatbelt. At some point he is likely to die from one or the other of these (hopefully not taking us – or anyone else – with him in the process) and we will feel bad, but not astonished. In much the same way we feel bad but not astonished when individuals and organizations who ignore publicized computer threats and solutions, are hacked or struck by viruses or worms.

As an example, someone we know finally got around to putting an antivirus program on his computer. When he ran his first scan it indicated **97** infected files! One wonders how many machines he infected. By much the same token, companies struck by the *Red Worm* before the patch was available have my sympathy and understanding, as do those hit by denial of service attacks coming from other infected machines. On the other hand, it is no easier to be astonished about that fifty percent of organizations running Microsoft Internet Information Services (IIS) who *didn't* to apply the **free** patch, once the problem had been publicized, than it is to be astonished about smokers having lung problems, or drivers without seatbelts being injured in automobile accidents.

In truth, there will always be vulnerabilities in computer programs and systems. And there will always be some period of time between the discovery of the vulnerability to the development of a patch for the vulnerability. However, once vendors make the fixes available, it is appropriate for individuals and organizations to update their systems.

*Red Worm* and *Red Worm II* (and III, and all future variants) only infected computers where the appropriate patch was not applied. And the same holds true of other computer vulnerabilities: Once there is a fix easily available, it is *sort of* your fault if you do not bother to apply it. However, the truth is that A) not all systems will get patched, and B) it is not fruitful to blame the victim. Instead, we should remember that detection and response are as important as patches.

For individuals not running servers, the problem is even easier to deal with: Install a personal firewall and get good anti-virus software that you update regularly. What constitutes regularly? Well, when we sign onto the internet in the morning we check for updates. If there is one, it is downloaded, and a scan of the system is run. In the evening another check for updates is made.

If there is one, it, too, is downloaded and run. Assuming there is no update, the system is scheduled to do a complete scan in the middle of the night.

In addition, keeping up-to-date with software patches and upgrades is as smart an idea for individual users as it is for business users. Services such as *Big Fix* (<http://www.bigfix.com/>) are free, and let you know when upgrades are available for certain software.

Does doing all this make us *invulnerable*? Absolutely not! We get several infected email attachments a week (all of which, so far, *appear* to have been caught by our anti-virus software). This being the case, we could as easily as the next user be caught by a new virus for which there is not yet a tracked signature. But between twice-daily checking for new signatures, regular checking for system and vulnerability updates, a personal firewall, and a near-pathological backup regime, we have some confidence that we are managing the risk as best we might.

## **5. Real Stories from the Field — Wireless network party lines**

Some years ago a friend had his telephone line crossed with that of the Brooklyn DA, turning it into a party line. While there was some minor amusement in listening into conversations about the witness protection program and high-profile cases, it was mostly an annoyance to not have access to his phone. (He finally solved the problem, the phone company being indifferent to it, by calling the DA's office to offer helpful suggestions. When he explained how he had all this information, the DA was mysteriously able to get the phone company to unscramble the lines in something under ten minutes.)

Today's equivalent to the crossed line – actually closer to a party line – is the wireless network, some of which are being installed by corporate IT departments, and some of which are being hooked up by users without IT knowledge. In either case, if you drive around business areas with a laptop in which you have a wireless network card, you face a high probability of being able to access somebody's wireless network.

“Ah,” you might say, “but you still need to sign in.” Well, in many cases authentication is missing, and you will be able to capture much of the confidential information zipping around the network.

“Ah,” you might say again, “we run Wireless Encryption Protocol (WEP), and are protected.” Well, we note again, Adam Stubblefield, a 20-year-old math major working as a summer intern at ATT labs finally broke WEP, which has been under attack for some time.

On the bright side, while WEP may be dead, administrators can take other measures, like implementing IPsec, a set of protocols currently in wide use to implement Virtual Private Networks (VPNs), as well as turning on the protective features that come with the wireless network.

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

*Secrets and Lies*

Bruce Schneier

John Wiley and Sons, ISBN 0-471-25311-1, \$29.99.

There are a lot of misconceptions about computer vulnerability, and a lot of unrealistic expectations about what is and is not possible. The truth is that completely reliable computer systems are impossible to achieve, and secure computer and networking systems are equally impossible. When this is understood, one is, at last, in a position to recognize risk and manage it.

*Secrets and Lies* gives the clearest explanation we have yet seen as to the fundamental problems faced when dealing with technology. If you are responsible, directly or indirectly, for data protection, you need to understand that it is impossible to make a program that is error-free. In addition, as programs become larger, more complex, and more connected with other programs on other machines, they become even more prone to errors and to errors caused by interactions among systems.

Once you recognize this, it becomes clearer that the approach to dealing with issues in computers is the same approach needed in all other areas, which is to say one of risk management. This means that while you need to keep current on patches, mere technology will not keep you safe. As with other areas, you must also rely on active monitoring of the activity on your machines, and on being pro-active in case of attack.

*Secrets and Lies* will, in our opinion, give you a very good overview of the philosophical state of the art. It is, as an added benefit, quite readable. If you haven't read this book, do so.

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

•• ÆGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2001 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](mailto:ejournal@lubrinco.com).

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

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

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

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

If you would like to submit an article for publication in ÆGIS e-journal, send it as an attachment to an e-mail to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com). Submission of an article certifies that (a) all information in the article is in the public record, or (b) that you are authorized to release any personal or corporate proprietary information contained in the article, and (c) that none of the article has previously been copyrighted. The submission of materials for publication in ÆGIS e-journal constitutes a license to The LUBRINCO Group Ltd, Inc., and/or Financial Examinations and Evaluations, Inc, their assigns, associates, or affiliates, to abridge and/or edit said submission, and to copyright and publish/republish any submitted materials in whatever written and/or electronic form they may choose.

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

*Article Title*, from the May 2001 ÆGIS e-journal (© 2001 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.