

ÆGIS e-journal



Addressing threats that affect your bottom line

Volume 2 Number 3, March 1999

From the case files of

The LUBRINCO Group

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

and

Financial Examinations and Evaluations, Inc.

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

Due diligence outside North America and Western Europe? Call us!

This month's features:

- 1. Due Diligence — Canadian SIN numbers**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Dumpster diving, is it worth it?**
- 3. Executive Protection — Back to basics**
- 4. Technical Issues — Data encryption: New stuff and links**
- 5. Real Stories from the Field — Y2K for the fun and education of us all**
- 6. Book and Product Reviews — Transnational Criminal Organizations, Cybercrime, and Money Laundering**
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Canadian SIN numbers

The Canadian SIN is similar to a SSN in that the number is issued to all Canadian citizens and, just like the SSN, it was never intended to be an identifier - but it is. And, just like the American SSN, the Canadian SIN has nine digits. The similarity in how to determine a "real" one from a "randomly printed" one ends there.

There is a formula that can be applied to the SIN that will weed out some of the fake ones. Here goes:

1. Write down the first eight digits (of the nine digit number).
2. Double every second digit. If the number doubled equals more than 10, subtract 9.
3. Add all the odd digits, plus the answers from the doubling exercise above.
4. The ninth digit of the SIN will be the amount needed to make the total from #3 divisible by 10.

This is somewhat confusing, so let's do an example right here.

1. Write first 8 digits of the SIN: 1-2-3-4-5-6-7-8-?
2. Double every second digit: 2 doubled is 4 4 doubled is 8 6 doubled is 12, so subtract 9 = 3 8 doubled is 16, so subtract 9 = 7 This total is now 22.
3. Add all the odd digits. 1+3+5+7+22 (the answer to the doubling above) - which totals 38.
4. 38 + ? is divisible by 10.

Therefore, the "?" is 2. This means that SIN 12345678 - 2 - is the only valid SIN starting with 12345678.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Dumpster diving, is it worth it?

This is a basic article about a basic issue of trash and what we as persons and businesses throw out in the garbage or in the recycling bins. As a training exercise, this occasional author and full time financial investigator, sends new recruits out to sift trash. Most hate the idea, some even think it stupid. "Anybody who has anything, has a shredder." WRONG. People who are sophisticated about protecting critical information have a shredder and even they slip up.

Recent field trips.

We picked up the trash bag, next to the ATM and the front door, at a credit union that handled municipal employees and teachers. At the end of the day we had the home address of 62 people. 11 were police officers, 2 city counsel members, 4 school principals and 14 senior city staff members the remainder were people who worked for the city and schools in many different jobs. We did target the credit union on pay day, but imagine if we took the garbage from this spot every day for a month. Working with county records, property, court and voting, we were able to assemble a full personal profile on the 31 significant people named above. This profile included, full name, spouse, children, property, d/o/b's and SS#'s. The recent class of recruits now thought what we were able to do in 6 hours was - chilling. If we were ID thieves we had 31 prominent people to replicate including financial account information, if we had more evil intentions we had their, job, home and family information.

B. Case - Art Gallery Competitive Intelligence. A Gallery Owner, who specialized in western art, Remington, Cowboy Artists of America, Gorman, etc... had been losing clients to a new, for that part, unknown gallery. An investigator was hired to see if there was anything "sinister" about how this long established gallery was losing business to an upstart. Saving the reader from a long foray into the art world (Being an Art Dealer and a Gentlemen are Mutually Exclusive further duplicity in the art world is more like quintiplicity) the investigation shook out as follows. The client liked to doodle on a pad of note paper on call in leads for paintings, the doodle would than be transferred into the active client book and the doodle would be tossed in the garbage. The new gallery owner thought that these leads were so valuable that the risk of these leads being lost in the garbage was untenable. Hence, he hired a cleaning crew to clean the established gallery owners office and deliver the garbage to him. The new gallery owner just had the cleaning crew undercut the old cleaning crew by half and they had the job.

It was further learned, after speaking to some of the defecting clients that the new gallery owners was pleasant, solicitous of their needs and a please to work with were as the old gallery owner was a loquacious, cantankerous grump and a pain to work with.

C. Garbage of Service Providers. Arizona is a hot bed of new technology in both the medical and semiconductor industries. There are three copy / duplicating shops that deal with these industries and their specialty needs. A

Chinese national was arrested for trespassing when he was found collecting the garbage from one of these printers. The charges were dropped because the trash bin was in a public area and the contents were considered discarded. It appears, according to federal law enforcement, that he was collecting high technology information such as chip blue prints and proposal fragments from the printers and shipping them back to China. It was a federal officer who called in complaint that got the man arrested. They were so frustrated with this fellow because he did seem to be breaking any laws, but none the less was acquiring significant amounts of information. Garbage is a significant source of information. You can disseminate information, collect information and use the process to your advantage or disadvantage. You choose.

3. Executive Protection — Back to basics

This editor recently met a young man, interested in becoming an executive protection agent, who asked what handgun he should buy. More recently still was a brief involvement in a case where essentially all overseas protective services were dropped as part of the cost-cutting of a company merger. While money was saved, short term, a senior executive was kidnapped by a group that apparently didn't understand the new cost-cutting rules.... This reminded me that there are a lot of misconceptions about protective work, and that a review of some basic principles is in order.

It is critical to understand that in protective work we are NOT police officers. We do not pursue bad guys and arrest them. Rather, our job is to *avoid* incidents where possible, and *escape* them if unavoidable. Only if we have failed at our two primary goals would we need to *deal* with the incident. Unfortunately, if you reach this state it is generally too late to do anything effective.

Keep in mind also the difference between the private sector and the public sector. In the public sector there may be only one target for a particular group or individual to attack: There is one president, one governor, one secretary of state. If this individual cannot be kidnapped or assaulted then the alternative most acceptable to the criminal may be assassination. In the private sector, however, if one subject is inaccessible then another subject, more accessible, will generally be equally desirable. To a large extent, therefore, our job in the private sector is to make *our* client so unattractive through planning, actions, and lack of visibility that kidnappers and assailants will go after someone less well protected.

How likely are we to need a handgun to make our client an undesirable target? Well, as an indication, the US Secret Service has *never* fired back at anyone during a protective detail. As it works out, while guns are sometimes carried on protective details overseas in high-risk environments, they are rarely carried domestically. Often, both in the US and overseas, it may not even be possible to carry weapons, because of country, state, or local laws. In these cases, if armed personnel are necessary, one has to hire local police officers or other locally licensed weapons carriers.

More to the point, many feel that carrying a gun on a protective detail is counterproductive: In the environment in which we work, both domestically and overseas, it is best to be the rabbit avoiding danger for the client, rather than the lion confronting danger and exposing the client to risk. What then is the job of the corporate or private protective agent? Who should be protected? And when should protective services be supplied? In order to answer these questions we must be aware of three things: First, protective services can be very intrusive, with the intrusiveness directly proportional to the level of risk faced.

Second, protective services are very expensive (figure on something in the neighborhood of \$175,000 a year for a low risk subject), with the expense directly proportional to the level of risk faced.

Third, unless incidents happen on a regular basis to those being protected, or to associates of those being protected, those involved - the people being protected and the people paying for the protection - become less than sensitive to the risks, and eventually feel that the intrusion and cost outweigh the risks. This leads to a feeling in many organizations that it is better to trust to luck that nothing will happen, and to rely on the government, as well as kidnapping-and-ransom insurance policies, to deal with any problems and associated costs that might arise. Even in high-risk areas many organizations — including large and wealthy organizations that should know better — often decide not to provide needed protective services.

In the US, where risks are generally low, protective services cover the obvious of keeping the client safe and healthy. What does this mean specifically?

The most obvious area of risk is driving. Automobile accidents remain a leading cause of death and injury in this country, and a well-trained driver can make the difference between a client arriving at work or being killed on the highway. (Be aware that the power of a driver is limited. As we saw with Princess Diana, a driver does not have the power to force a client to wear a

seat belt. For most of us, getting even our parents, friends, or siblings to buckle-up can be difficult.)

In addition, having a trained driver can reduce the risk of kidnapping and attack, both of which, if they occur, are likely to happen in or near a car. The car is the danger zone because most people leave in a car from their home in the morning and drive to their office. And they routinely leave in the same car from the same office every afternoon and drive home. Kidnappers and other assailants generally spend weeks or even months observing these routines. While it can be difficult to induce clients to depart from their homes and offices at random times each day, or take random (and therefore longer) routes each day, a competent and well-trained driver can nonetheless be a factor in inducing criminals to target someone else.

A second area is health and safety. People in the corporate world who merit protection are generally not young, generally lead high-stress lives, and may not exercise enough or have healthy diets, which means that health risks are more likely than physical assaults. Because of this, a grasp of emergency medicine is important, even if the protective agent is not a paramedic or EMT. The agent should be aware of his charge's medical history, the medicines they are taking, and the location of the nearest medical facilities to where they are at any given instant.

In this same category is the elimination of safety hazards. If the client slips on a bar of soap overlooked on the floor of the shower stall, or a badly-placed lamp cord, there could be an injury, which, *de facto*, is the fault of the protective agent.

On a slightly different line, it is also the job of the protective agent to prevent embarrassment and PR gaffes.

In higher-risk areas the goals are the same, but the protection offered may be more continual, in greater depth, and may extend to the family of the client: If a wife or child is snatched it can be just as distracting as if the client were kidnapped. So who needs protection on an individual basis? Someone whose injury or loss would have a negative impact on an enterprise such that the sums involved in providing protection are deemed cost efficient when compared to the alternatives. Note that by this definition there need not be an exceptional threat involved.

Note also that this means that in a low-risk environment the protective services provided can be much less intrusive (and far less costly) than in a high-risk environment. Since it is unlikely that a team of armed men will burst into a client's home in the U. S., round-the-clock protection may not be

necessary. Instead, a trained driver to take the client to and from work, and to and from lunch, may be all that is needed. In some cases a weekend out-of-house driver may also be appropriate.

As always, each particular situation should be scrutinized by professionals to determine the appropriate kind and level of protection needed, and to plan for the contingency of an incident.

4. Technical Issues — Data encryption: New stuff and links

On the 31st of December, 1998 US Commerce Department released new regulations implementing looser guidelines for cryptography exports:

<http://jya.com/bxa123198.txt>

The new rules eliminate many restrictions on selling data scrambling products to subsidiaries of US corporations. In addition, they relax controls for encryption products to health and medical organizations in 44 countries for almost all foreign subsidiaries of US companies.

List of countries: *<http://www.bxa.doc.gov/factsheets/EncCountryList.htm>*

According to the Center for Democracy and Technology's analysis of the regulations, the plan helps big companies while still ignoring the concerns of individual or small business users.

The policy does not address the needs of individuals online, human rights groups, or other noncommercial users. the analysis stated. It continues to use export controls as a club to force the adoption of risky 'key recovery' systems without addressing the privacy concerns raised by government (any government) access to data. The governments that are the most egregious at "reviewing" encrypted data are: United States, North Korea, China, and France.

News reports (news items are taken off the Web relatively quickly, and *may* be gone by the time you look for them):

<http://www.news.com/News/Item/Textonly/0,25,30414,00.html>

<http://www.usatoday.com/life/cyber/tech/cte066.htm>

http://www.andovernews.com/cgi-bin/news_story.pl?108205

5. Real Stories from the Field — Y2K for the fun and education of us all

More stuff on Y2K - this is just some stuff we have accumulated over the last several months for the fun and education of us all.

- Swedish Taxi Meters and Gas Station Payment Computers Fail
<http://deseretnews.com/dn/view/0,1249,30004467,00.html>

- Police Computers Fail at Stockholm Airport
<http://www.theaustralian.com.au/masthead/theoz/state/4114277.htm>
- The West Virginia company Lynn Electric couldn't close its 1998 payroll because all documents converted to 1944, which is the date arbitrarily chosen by a number of PC programmers to use as state date for operating system clocks.
- The Food and Drug Administration (FDA) has reported that two medical devices - an external defibrillator and a multi-parameter patient monitor - will fail to display, print or store the correct time of the products' operation (thereby creating incorrect records but not endangering patient health).
- Shocking report on the state of nuclear plants & the power grid
http://www.worldnetdaily.com/bluesky_exnews/19990111_xex_bad_news_pow.shtml
- Some utility companies say they won't make it
http://www.boston.com/dailynews/wirehtml/010/BLACKOUT_Utility_compani_01_10_.html
- Think airports will work? Read this...
<http://www.amcity.com/denver/stories/1999/01/11/editorial3.html?h=bug>
- Health care industry not even close to compliance
<http://www.techweb.com/se/directlink.cgi?IWK19990111S0018>
- Time Magazine - Millennium Madness
http://cgi.pathfinder.com/time/reports/millennium/end_world.html
- Y2K Information & Alert Updates <http://www.y2knewswire.com/>

6. Book and Product Reviews

Transnational Criminal Organizations, Cybercrime, and Money Laundering

James R. Richards

CRC Press 1-800-272-7737 \$29.00

This is an excellent book and a recommend read for the novice, the expert, and the voyeur. It combines into a very readable format the present and the future of international crime, how it uses money laundering for transshipment of their gains and the criminal future using computers and new money technology to make their job, and ours, as investigators, much more difficult. The book contains extensive examples of how the crimes are committed, trails and documents to look for and examples of crimes and how they used the tools and how the investigators finally made their case.

It is also a well-written book that flows logically from beginning to end, including the Appendices.

If there is a shortcoming it is the focus of the book on the more visible crimes of drug traffickers and smugglers. It does not touch upon, to a great extent, the white-collar crimes, including securities fraud and embezzlement that are beginning to outstrip drug trafficking in some European nation as the source of illegal funds to be laundered. But, I'll tell you this, if James R. Richards, authors a second volume on Financial Crimes, we would like to be the first to purchase it.

7. Free-Subscription/Unsubscription/Copyright Information

•• AEGIS e-journal is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 1999 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 March 1999 ÆGIS e-journal (© 1999 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.