



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 3 Number 9, September 2000

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 — Negative information on background checks**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Web-based tracking strings**
- 3. Executive Protection — Proposal for IRS to regulate handguns**
- 4. Technical Issues — Key loggers**
- 5. Real Stories from the Field — Choosing what to have stolen**
- 6. Book and Product Reviews — *The Criminal Record Handbook***
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Negative Information on Background Checks

For four long years, Bronti Kelly couldn't figure out why no one wanted to hire him. He handed department store managers across southern California a résumé full of sales experience, but was rejected hundreds of times. Those rare times when he got a job, he would be fired within days.

Along the way, Kelly filed for bankruptcy, lost his apartment, and became homeless. "For years as this went on, I blamed myself — for not being hired for employment, the conditions I went through," Kelly says.

But Kelly's self-blame turned to anger when he finally learned the real cause of much of his trouble: A man had given Kelly's identity to authorities when arrested for shoplifting and other crimes, and the tainted profile found its way into a range of computer databases used in background checks by employers.

Kelly's plight illuminates the growing threats to privacy in an age of ever-easier computer access to public information. An inaccurate black mark left on a person's profile can be duplicated again and again without the victim's knowledge. The personal details are easily and cheaply obtainable — and open to abuse by crooks trying to dodge the law or make a buck.

It used to be that to get background information you had to trek down to a courthouse, ask the clerk to direct you to the proper records, and thumb through musty files. For another type of information, you had to visit yet another government agency.

But in recent years, more and more information vendors have signed deals with governments and businesses for computer access that enables them to compile virtual dossiers on Americans — from Social Security numbers to shopping preferences.

Crooks no longer have to look for crumpled credit card carbons to steal a person's account number. Now, for nominal fees, personal details such as Social Security numbers can be found over the Internet and used to create a whole new identity for opening an account — and sticking the fraud victim with the bills.

Consumers Union in San Francisco found that half of credit-bureau reports surveyed in 1991 contained errors, about 20 percent of which were big enough to prevent an individual from buying a home or a car.

"The information age permits the exchange of data so quickly with so few safeguards, that you really become a victim before you know it," says

Edward Howard, head of the Los Angeles–based Center for Law in the Public Interest. “Not only do you become a victim, you’re constantly behind the power curve when you’re trying to clean it up.”

Bronti Wayne Kelly, now 33, hardly foresaw the cyber-nightmare that would grow from what seemed an old-fashioned wallet-snatching in May 1990. He reported to police his wallet only contained \$4, along with his driver’s license, Social Security card, and military I.D. for the air force base in southern California where he served as a reservist.

But seven months later, Kelly, a salesman in the Robinson-May department store in Riverside, was ushered into the personnel director’s office and told he had been caught shoplifting by security guards in another Robinson’s.

Kelly produced a letter from his air force commanding officer saying that Kelly was on duty when the crime occurred, but he was fired anyway. He says he was equally confounded by the blur of job rejections that followed, usually with no explanation.

For two years he held on. Kelly’s work as a mechanic at the local air force base earned him about \$700 a month. But in June 1993, the six-year reserve stint was up.

With no job in sight, Kelly filed for bankruptcy to stave off bill collectors. He was evicted from his apartment in San Bernardino, California.

Kelly stayed with friends until he wore out his welcome. He turned to sleeping in his car, then the streets, using public parking garages downtown to shield him from the elements.

He tried to keep clean using a pool shower at his old apartment complex. He applied for food stamps and welfare but was rejected because he had no residence or mailing address.

He finally landed a job selling clothes at Harris department store in nearby Riverside, but the day before his first day of work he was told that his services were not needed.

Kelly, crying at the news, tried to find out why. The personnel manager told him to contact Stores Protective Association, which exchanges information about employees with more than 100 member retail chains.

Kelly wrote to SPA, and received a written explanation in January 1995, pegging him for the same shoplifting offense he thought had been purged from the records four years earlier.

“I couldn’t believe the information was still on file,” Kelly says. “I had never even heard of [SPA] before.”

But the vast majority of employers Kelly had applied to were members of SPA. It took until the next month for the association to remove the false information from its files on Kelly, and then only after a local television station reported his woes.

A lawyer for SPA, which Kelly is suing in a defamation lawsuit that also names Robinson-May’s parent, said that Kelly had never given it evidence other than his own statement that he was not the shoplifter. Kelly is seeking unspecified damages and a public apology from Robinson-May.

Kelly’s problem was far more complicated than he suspected. When Kelly contacted the Los Angeles Police Department to try to straighten things out, he discovered that its records showed he had been arrested five years earlier not only for shoplifting, but for burglary and arson as well.

Kelly submitted his fingerprints to prove to authorities that he was not the accused culprit, that instead the miscreant was another white male who had given Kelly’s identity to police. The police gave Kelly a “Certificate of Clearance,” which states that the police had determined that Kelly was not the person arrested.

However, Kelly’s identity remains in police files, even though the most serious charges against the impersonator had been dismissed shortly after his arrest in July 1990. Los Angeles police officials say they need the charges on record in case the impostor is arrested for other crimes.

After SPA removed Kelly’s name from its files, he was still rejected from another 50 jobs, and he is still wondering why. One possibility is that the incorrect information continues to haunt him.

The problem was spelled out last month after The Associated Press hired an information search company to conduct a search of Kelly’s background.

AP simply gave Forefront, a subcontractor to Informus Corp., Kelly’s name, Social Security number, and a \$124 check to search state court records in three counties in southern California.

The search came back showing that Kelly had been arrested in July 1990 for arson, theft, and disturbing the peace.

But Kelly no longer has to worry. Seven years after his wallet was stolen, he has stopped seeking work among strangers. Today, he is employed part-time

cleaning pools in a family business, and shares an apartment in Temecula, near San Diego, with a roommate who has helped him out financially.

Trying to rebuild his self-image, Kelly carries his police certificate clearing him of crimes wherever he goes. One look in the mirror confirms it was not he who dragged down his life.

Says Kelly: “A part of me feels very proud.” But just to be sure, he is thinking of changing his name.

Bad things *can* happen to good people — and do. As a prospective employer or a background investigator you should immediately present any negative information you have discovered to the party being investigated. On one occasion — one among many for us — investigation showed that a Mr. Ragsdale, a slight man who was the president of a medical company, appeared in public records stating that he had physically assaulted 22 people in one night in a bar in Oceanside, California. “Mr. Ragsdale literally mopped the floor with some of his victims,” the report said. When we confronted Mr. Ragsdale with this information, he laughed and asked to see the report. Then he pointed out that the physical description of the bar brawler showed him to be six inches taller and twice Mr. Ragsdale’s weight. It turned out that the brawling Ragsdale was an ex-marine who did not like sailors and mopped up a bar full of them to prove his point.

So what should you do if you come up with negative information in a background search? Present the negative information as soon as you can and allow the person to respond. If he can clear up the problem, it is good for both of you.

It is important in doing background investigations that we keep in mind the increasingly common practice of stealing complete identities so that the miscreant can open credit-card accounts, buy or sell real estate, and commit criminal acts — all in the name of another. In fact, it has reached the point that some insurance companies now issue coverage for “theft of identity.” It is our job in this and all other areas of due diligende to bring the truth to light, not add to the problem by allowing our clients to make a wrong decision based on bad information.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Web-Based Tracking Strings

It is possible to add a “Web Based Tracker String” (WBTS) to Microsoft Word documents. A WBTS could allow an author to track where a document is being read and how often. In addition, the author can watch

how a “tracked” document is passed from one person to another or from one organization to another.

WBTSs are made possible by the ability of Microsoft Word documents to link to an image file that is located on a remote Web server. Because only the URL of the WBTS is stored in a document and not the actual image, Microsoft Word must get the image from a Web server each and every time the document is opened. This image linking feature then puts a remote server in the position to monitor when and where a document file is being opened. The server knows the IP address and host name of the computer that is opening the document. A host name will typically include a company name if a computer is located at a business. The host name of a home computer usually has the name of a user’s Internet Service Provider (ISP). (This is, of course, a moot point if the document never has contact with the internet.)

An additional issue, and one that could magnify the potential for surveillance, is that Web bugs in Word documents can also read and write browser cookies belonging to Internet Explorer. Cookies could allow an author to match up the computer viewer of a Word document to the visits to the author’s Web site.

WBTSs are used extensively today by Internet advertising companies on Web pages and in HTML-based e-mail messages for tracking. They are typically 1 pixel by 1 pixel in size to make them invisible on the screen to disguise the fact that they are used for tracking. Short of removing the feature that allows linking to Web images in Microsoft Word, there does not appear to be a good preventive solution. To stop WBTSs, it is best to disable cookies in a software patch. In addition to Word documents, WBTSs can also be used in Excel 2000 and PowerPoint 2000 documents.

One reason to use this tracking ability is to monitor the path of a confidential document, either within or beyond a company’s computer network. The confidential document could be “instructed” to alert someone each time it is opened. If the company’s Web server ever received a “server hit” from an IP address for the bug outside the organization, then it would learn immediately about the leak. Because the server log would include the host name of the computer where the document was opened, a company could know if the organization that received the leaked document was a competitor, a media outlet, or something else. All original copies of a confidential document could also be numbered so that a company could track the source of a leak. A unique serial number could be encoded in the query string of the WBTS’s URL. If the document is leaked, the server hit for the WBTS will indicate

which copy was leaked. A serial number could be added to a WBTS in a document either manually right before a copy of a document is saved or automatically through a simple utility program. The utility program would scan a document for the WBTS's URL and add a serial number in the query string. A Perl script (Perl being a computer language much used on the internet these days.) of less than 20 lines of code could easily be written to do this sort of serialization.

Another use of WBTSs in Word documents is to detect copyright infringement. For example, a publishing company could "bug" all outgoing copies of its newsletter. (the *ÆGIS* e-journal does not do this, as we encourage sharing of our experience). The WBTS in a newsletter could contain unique customer ID numbers to detect how widely an individual newsletter is copied and distributed.

A third possible use of WBTSs is for market research. For example, a company could place Web bugs in a press release distributed as a Word document. The server log hits for the WBTS would then tell the company what organizations have actually viewed the press release. The company could also observe how a press release is passed along within an organization, or to other organizations. In an academic setting, WBTSs might be used to detect plagiarism.

A document could be tagged before it is distributed. An invisible WBTS could be placed within each paragraph in the document. If text were to be cut and pasted from the document, it is likely that a WBTS would be picked up also and copied into the new document.

The use of WBTSs is not an issue unique to Word. Any file format that supports automatic linking to Web pages or images could lead to the same problem. Software engineers should take this privacy issue into consideration when designing new file formats. This issue is potentially critical for music file formats such as MP3 files where piracy concerns are high. For example, it is easy to imagine an extended MP3 file format that supports embedded HTML for showing song credits, cover artwork, lyrics, and so on. The embedded HTML with embedded WBTSs could also be used to track how many times a song is played and by which computer, identified by its IP address.

Recommendations: Short of getting rid of the ability of Word documents to link to Web images, there really is no solution to being able to track Word documents using WBTSs. This linking ability is a useful feature. However, the Web browser cookies could be disabled inside Word documents. There

appears to be very little need for cookies outside a Web browser. In general, cookies should be disabled by default any time Internet Explorer is reused inside other applications such as Word, Excel, or Outlook.

Users concerned about being tracked can use a firewall such as ZoneAlarm (available **free** at <http://www.zonelabs.com>) to warn about WBTSs in Word documents. ZoneAlarm monitors all software and warns if a program for which you have not given explicit permission to do so is attempting to access the Internet. (In this case it will ask if you want Word to be able to access the Internet. The prudent answer is NO.) ZoneAlarm is designed to catch Trojan horses and spyware. However, because Word typically does not access the Internet, ZoneAlarm can also be used to catch “tagged” Word documents.

3. Executive Protection — Proposal for IRS to regulate handguns

The following is a copy of a Senate bill as proposed.

S 2099 IS

106th CONGRESS

2d Session

S. 2099

To amend the Internal Revenue Code of 1986 to require the registration of handguns, and for other purposes.

IN THE SENATE OF THE UNITED STATES

February 24, 2000

Mr. REED introduced the following bill, which was read twice and referred to the Committee on Finance.

A BILL

To amend the Internal Revenue Code of 1986 to require the registration of handguns, and for other purposes. Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the “Handgun Safety and Registration Act of 2000”.

SEC. 2. REGISTRATION OF HANDGUNS.

(a) HANDGUN INCLUDED IN DEFINITION OF FIREARM-

(1) IN GENERAL- Section 5845(a) of the Internal Revenue Code of 1986 (defining firearm) is amended by striking “and (8) a destructive device” and inserting “(8) a handgun; and (9) a destructive device”.

(2) DEFINITION OF HANDGUN- Section 5845 of the Internal Revenue Code of 1986 (relating to definitions) is amended by adding at the end the following:

“(n) HANDGUN-

“(1) IN GENERAL- The term ‘handgun’ means any weapon (including a starter gun) which--

“(A) is designed to or may be readily converted to expel a projectile by the action of an explosive, and

“(B) has a short stock and is designed to be held and fired by the use of a single hand.

“(2) DISASSEMBLED PARTS INCLUDED- Such term shall also include the frame or receiver of any such weapon, and any combination of parts from which a handgun can be assembled if such parts are in the possession or under the control of a person.

“(3) EXCLUSION- Such term shall not include a firearm classified as ‘any other weapon’ under subsection (e).”.

(b) TRANSFER TAX IMPOSED ON HANDGUNS- Section 5811(a) of the Internal Revenue Code of 1986 (relating to rate) is amended by inserting “or as a handgun under section 5845(a)(8)” after “section 5845(e)”.

(c) TAX ON MAKING FIREARMS IMPOSED ON HANDGUNS- Section 5821(a) of the Internal Revenue Code of 1986 (relating to rate) is amended by inserting “, except, the tax on any firearm classified as a handgun under section 5845(a)(8) shall be at the rate of \$50 for each such firearm made” after “firearm made”.

(d) IMPORTATION POLICY CONTINUED-

(1) IN GENERAL- Section 5844 of the Internal Revenue Code of 1986 (relating to importation) is amended by adding at the end the following: “This section shall not apply to any firearm classified as a handgun under section 5845(a)(8).”.

(2) CONFORMING AMENDMENT- Section 925(d)(3) of title 18, United States Code, is amended by inserting “(without regard to paragraph (8) thereof)” after “section 5845(a)”.

(e) SHARING OF REGISTRATION INFORMATION WITH STATE AND LOCAL LAW ENFORCEMENT AGENCIES-

(1) IN GENERAL- Section 6103(o) of the Internal Revenue Code of 1986 (relating to disclosure of returns and return information with respect to certain taxes) is amended by adding at the end the following:

“(3) TAXES IMPOSED ON TRANSFER OF HANDGUNS- Returns and return information with respect to taxes imposed by part II of subchapter A of chapter 53 (relating to tax on transferring firearms) on any firearm classified as a handgun under section 5845(a)(8) shall be available in an on-line format for inspection by or disclosure to officers and employees of--

“(A) any Federal law enforcement agency, and

“(B) any State or local law enforcement agency, whose official duties require such inspection or disclosure.”.

(2) CONFORMING AMENDMENTS- Section 6103(p)(4) of the Internal Revenue Code of 1986 is amended--

(A) in the matter preceding subparagraph (A)--

(i) by striking “or (o)(1)” and inserting “(o)(1), or (o)(3)(A)”,

(ii) by striking “or (l)(6)” and inserting “(l)(6)”,

(iii) by inserting “or (o)(3)(B),” after “(16),”, and

(B) in subparagraph (F)(i)--

(i) by striking “or (l)(6)” and inserting “(l)(6)”, and

(ii) by inserting “or (o)(3)(B),” after “(16),”, and

(C) in subparagraph (F)(ii), by striking “or (o)(1)” and inserting “, (o)(1), or (o)(3)(A)”.

(f) TRANSITION RULE FOR NONREGISTERED HANDGUNS-

(1) IN GENERAL- Any person possessing any firearm classified as a handgun under section 5845(a)(8) of the Internal Revenue Code of 1986 not registered in the National Firearms Registration and Transfer Record maintained by the Secretary of the Treasury under section 5841 of such Code shall register such handgun--

(A) within 1 year of the date of the enactment of this Act, or

(B) upon the transfer of such handgun before such 1 year anniversary date.

(2) **TREATMENT OF REGISTRATION AS TRANSFER-** For purposes of any tax imposed by part II of subchapter A of chapter 53 of the Internal Revenue Code of 1986 (relating to tax on transferring firearms) on any firearm classified as a handgun under section 5845(a)(8) of such Code, any registration of such handgun under paragraph (1)(A) shall be considered a transfer of such handgun.

(3) **NONAPPLICATION OF PENALTY-** Section 5861(d) of the Internal Revenue Code of 1986 shall not apply with respect to the possession of any handgun before the date of the registration of such handgun under paragraph (1).

(g) **PROVISION OF REGISTRATION FORMS-**

(1) **AVAILABILITY-** To promote and assist compliance with the handgun registration requirements under the Internal Revenue Code of 1986, as amended by this section, the Secretary of the Treasury shall make available such registration and fingerprint forms as may be required by the public for compliance with such requirements--

(A) to State and local law enforcement agencies and facilities of the Department of the Treasury throughout the States, the United States Postal Service, and such other agencies and departments of the Federal Government as the Secretary determines would aid in making such forms available to the public; and

(B) through the Internet in a downloadable format.

(2) **SINGLE FORM-** The Secretary of the Treasury shall make available registration forms that allow an individual to register the possession or transfer of more than 1 firearm classified as a handgun under section 5845(a)(8) of the Internal Revenue Code of 1986 on a single form.

(h) **PROGRAM OF PUBLIC AWARENESS-** Within 60 days after the date of the enactment of this Act, the Secretary of the Treasury shall commence a program to broaden public awareness of the handgun registration requirements under the Internal Revenue Code of 1986, as amended by this section. Such program may include voluntary cooperative efforts with Federal, State, and local law enforcement agencies and public service announcements as deemed appropriate by the Secretary.

(i) AUTHORIZATION OF APPROPRIATIONS- There are authorized to be appropriated such sums as may be necessary for the Secretary of the Treasury to carry out the provisions of and amendments made by this Act.

(j) EFFECTIVE DATE- The amendments made by this section shall take effect on the date of the enactment of this Act.

4. Technical Issues — Key Loggers

Key loggers enable one to capture every keystroke entered on a computer and then to replay them later. There are a number of reasons, both legitimate and illegitimate, to do this. One would be to act as an emergency backup, allowing the recreation of everything that had been done, keystroke by keystroke. Another, used by employers checking on their employees as well as by those engaged in industrial (and other) espionage, would be to intercept what others have typed, keystroke by keystroke.

There are four capture formats:

- a) a module containing a flash memory (to store the information for later extraction and playback) connected to the wire between the keyboard and the computer
- b) a module containing a transmitter (to send the intercepted information to a receiver elsewhere) connected to the wire between the keyboard and the computer
- c) a board containing a transmitter inserted within keyboard itself
- d) software that stores the keystrokes on the computer's hard drive, so that the information can be recovered later. We are given to understand that some computer companies are now supplying this software as standard, so that parents can track what their children are doing online.

In formats a and b, installation is simple: Unplug the existing keyboard cable from the computer; then plug the module into the computer and plug the keyboard into the module. One advertisement says of its product: "The KeyKatch is a tiny inexpensive supervision module that clips onto your keyboard cable. It logs all keystrokes typed on the computer. It doesn't require an external power source and it installs in less than 10 seconds. <http://www.codexdatasystems.com/keykatch.html> Dealer inquiries invited."

Format c is more difficult as it requires opening the keyboard to install the board. (Note that it is useful to know in advance what keyboard is being used so that opening and closing it is not too frustrating *in situ*.)

Format d is just a matter of installing the software.

All four formats require access to the keyboard and computer — but not for too long.

In flash memory, the memory chip can be extracted and placed in a reader (or the whole module can be removed). In formats b and c, transmission occurs as each stroke is made; at a remote radio receiver the character can be displayed in real time and simultaneously recorded.

Variations to the system are available and start around \$2,500 for the basic 10-milliWatt transmitter module and receiver. The price rises along with the module's capabilities. For example, one version has a test beacon to confirm that the unit is functioning, as the system only works when the target computer/keyboard is switched on.

Performance on most keyboards is accurate and reliable.

We purchased two devices for testing. The average installation time was 25 seconds for the in-line model. We were able to capture everything a that was typed. They do have some limitations, however. For example, moving to a bookmarked Web page will not be captured because it does not require a keyboard entry. We took the device off the computer, then reinstalled it on another machine and recovered all the data. Laptops don't have cables connecting the keyboard to the computer, so some devices can't be used on them. As part of security checks, we are now checking all keyboards. The device looks like an adapter of some sort, and the average person would believe it was supposed to be there.

The key loggers we have seen have 128K of flash memory, require no power supply, and need no software. About 500,000 keystrokes can be stored (to make this a trifle more meaningful, typing in this e-Journal would require fewer than 35,000 keystrokes), and they can record keystrokes even if the computer is started from a floppy disk, unlike software that is required for the versions that are on computer hard drives.

How do you tell if a key logger has been installed? By physical inspection of the device, and by examination of the system for large files or programs that are automatically started and are creating an increasingly large file (the filling of which sometimes makes the system run slower). If you don't know anything about computers, you will need a more technically skilled person to do this for you.

5. Real Stories from the Field — Choosing what to have stolen

We got a call from a couple who had been robbed. As it turned out, they had been renting out their apartment on short-term leases through an agency whenever they traveled. Their personal papers were in unlocked files, and their valuables were cunningly hidden in a hollow book.

Unfortunately, their valuables were not as cunningly hidden as they thought because when they got ready for their next trip, it turned out that their valuables were gone. They had lost their passports, birth certificates, a vault key (carefully labeled with bank address and box number), gold coins, their father's heirloom watches, and a few other bits and pieces of economic or sentimental value.

Who had robbed them? Well, it could have been the last, very respectable, renters. Or it could have been building staff, who had keys and had been in and out of the apartment a number of times on legitimate business. Or it could have been the cleaning people. Or it could have been less-than-scrupulous friends or acquaintances (remember: without trust there can be no betrayal). In truth, they will probably never know.

After the incident there was much gnashing of teeth and many regrets about renting the apartment. But that missed the point. The point is that robberies take place, and we control what is there to be stolen. How you choose what you will allow to be stolen is very much a personal choice.

Some items have some economic value but little sentimental value. Some items are not easily disposed of. Some items expose you to the risk of identity theft. Some items have great value but are little used. In some circumstances your risk of pilferage is high, and special care must be taken.

For small items of great economic or sentimental value, it is worth taking extra care. Jewelry, gold, silverware, heirlooms, important papers, and other similar items probably should be made inaccessible. In many cases this means that they should be put into a safety deposit box or locked in a real safe (as opposed to a small home safe that can be carried out of the house in a trash basket and broken into at leisure).

Special circumstances also affect the degree of risk considered to be acceptable. For example, if this editor were renting his apartment to strangers, he would leave behind nothing worth crying over, not even if cleverly hidden. Another special case is that of the aging. This editor's mother is 93 and now requires some transient help from time to time. Because of this, her personal items such as valuable jewelry, important

papers, and silverware, all of which are unlikely to be used on a regular basis (if ever), are locked away, secure from all but the serious burglar, which means that petty theft is not an issue. Quality-of-life articles, such as paintings, are not locked up, as they do not lend themselves to petty theft.

Look around your home. What would leave you in tears, or greatly concerned, if it were stolen? What items must always be there, even when you are away? How can you protect these items? Are they covered by insurance? Do you have adequate access control?

If you can ask these questions and either answer them – or get us or someone like us to help answer them, then you are on your way to keeping them.

6. Book and Product Reviews

The Criminal Record Handbook
Total Information Services, Inc.
1-800-331-9175

The book covers criminal records, what they are, what the legal terms mean, how to obtain information from a prospective employee, why you need to do a criminal records check, and some guidelines for the decision-making process. The issue of criminal records and employment is serious: It can be very costly if you hire someone with a criminal record and he causes harm to a third party.

Should you hire someone with a criminal record on a case-by-case basis or should you refuse to hire anyone with a criminal record? That is up to you, the hiring entity, to decide, and not the prospective employee to decide through obfuscation.

This is a good book, attractively laid out and should be part of the reference section of anyone doing background checks, and every human resources manager.

7. Free-Subscription/Unsubscription/Copyright Information

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 September 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.