

**The Business and Security e-Journal**  
from the case files of  
**The LUBRINCO Group**  
**International Risk Management Services**  
<http://www.lubrinco.com/>  
and  
**Financial Examinations and Evaluations, Inc.**  
<http://www.feeinc.com/>

**Volume 4 Number 7, July 2001**

The *Business and Security e-Journal* is for senior management, and focuses on areas of business risk that affect their domestic and international bottom line.

**This Month!!!!**

- 1. Due Diligence — The new Euro: A counterfeiter's dream**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Smile and dial**
- 3. Executive Protection — Tracking unexpected visitors**
- 4. Technical Issues — Wireless security**
- 5. Real Stories from the Field — Sticky fingers and stolen code**
- 6. Book and Product Reviews**
- 7. Free-Subscription/Unsubscription Information**

**1. Due Diligence — The new Euro: A counterfeiter's dream**

Currently, the most counterfeited bill is the US \$100. This is because it is a world-wide, easily recognized, standard of value. This is also why the US stopped producing the larger denominations such as the \$500 and \$1,000 bills. These were serious targets for counterfeiters and they allowed, according to US drug policy wonks, too much of a store of value, making it too easy for large sums of money to be moved undetected. Many nations have developed a similar strategy of printing lower denomination currency to reduce the likelihood of counterfeiting. In effect, they try to ensure that the cost of counterfeiting is higher than the cost of the real thing.

The new Euro's larger denominations of €200 and €500 shown below are a temptingly greater store of value than the US \$100. Assuming an exchange rate of \$0.85 to €1, that makes the €200 worth \$170 and the €500 worth \$425.



Some consider this policy decision to be a major blunder that invites counterfeiting. There is a fear that many will exchange marks and francs for counterfeit Euro's while the population is still getting used to the look and feel of the currency. Others fear that counterfeit currency will be exchanged for real Euro's. Others still have simply called the Belgian wonks fools and morons for issuing such high denomination notes that will obviously attract criminals.

But why would the EU do something that is so obviously going to attract so much attention to their currency?

Let's take a short lesson in central banking. Currency issued by a government is an interest-free loan from the user of the currency to the government or central bank. Thus, the world, while using dollars as a currency is giving the US Treasury an interest-free loan. The world's largest amount of circulating currency is the US dollar, with 80% of all physical dollars ever issued circulating outside of the US.

Now, with a larger denomination note, more value can be stored in a given place; thus, people interested in using currency as a medium for international exchange will switch to the item with a higher (more concentrated) value. Thus more dollars will come out of circulation and will be replaced by

euros. When people swap dollars for euros they will now give their interest free loan to the European Central Bank, not to the US Treasury. Some level of thought went into this.

The euro will slowly but surely replace the dollar as the unit for barter and exchange in the cash stashes and the illegal markets. Dollars will be sold and returned to the Treasury, and euros will be bought and flow into the market place. Economies don't care who has the notes; all that counts is that they are out there.

## **2. OPSEC, Economic Espionage, and Competitive Intelligence — Smile and Dial**

We recently did the research for a potential class action suit against a major wholesaler, spearheaded by a potential competitor wishing to gain a foothold in a constrained market. Their target company sells to a small number (100 or fewer) of trade stores in a city of 5 million.

Because of the small numbers involved, we called most of their clients and asked them (the researcher clearly said that the action was in the formative stage and sponsored by an industry competitor, and that this was only preliminary research) the following questions:

- A) Are you happy with XYZ?
- B) What unfair Trade Practices have you seen from XYZ?
- C) What other problems are you having?
- D) What is your average monthly sales volume with XYZ?

The response was unbelievable, both in terms of the potential litigation and in its competitive intelligence value:

- We learned there were no competitors and that when a few of the companies got together to go around this wholesaler, they were buried in the paperwork of litigation.
- We learned that this practice of unfair trade competition could be a monopolistic practice and that it could be actionable.
- We learned that the company's COD policy was very frustrating, and that even a 15 days grace period would be better.
- We learned the names of most of the sales people of the company and their estimated annual revenue.

In short, in 32 billable research hours we had amassed enough information about the target company for both valid litigation and for our client to consider a new marketing strategy.

Customers are a great source of information about a competitor. After all, the ultimate arbiter as to how well a company does is the customer.

### **3. Executive Protection — Tracking unexpected visitors**

Most protective work is a mixture of facilitation, preventing accidents from happening, and dealing with normal crises. Sometimes, however, bad people really do present a risk that must be managed. The risk can range from annoyance on the low end to physical risk on the high end.

In order to manage the risk it must first be identified, and then evaluated. In some cases the risk is identified through the gathering of intelligence, and in other cases it comes through tracking unwanted contacts. These contacts can be written, by email, by fax, by telephone, or in person. In this issue we are particularly concerned with contacts in person.

The people whom we protect can generally be found in any number of known places. They can be at home, they can be in their office, they can be in transit, they can be at public events. When unexpected (and we don't mean one's nephew dropping in) visitors show up, it is prudent to interview them briefly and find out who they are and why they are there. In some cases the people who show up have some valid reason for being there. In some cases they are a possible future annoyance or threat, but if you don't speak with them you will never know who they are.

If possible, they should be discreetly photographed and videotaped so that they can be recognized in the future, and a face put to the name, and vice versa.

By the same token, it often turns out that people causing problems have cased out their target, and should have been noticed. For this reason, it is a good practice to take videos of events where the person you are protecting is appearing. This allows you to identify unknown people who are turning up with unexpected frequency for no apparent valid reason. Their presence can then be anticipated, and they can be given special attention, or even discreetly interviewed, if only through casual conversation.

As always, the more aware you are of your environment, the more likely it is that you will be able to identify potential risks in time to manage them.

#### 4. Technical Issues — Wireless Security

When it comes to wireless surveillance, the federal government has some really neat tools. The FBI has discussed the domestic internet surveillance system *Carnivore*, and the CIA and NSA have discussed their global electronic surveillance *Echelon* with which the United States, the United Kingdom, Canada, Australia, and New Zealand can presumably intercept satellite, microwave, cellular, and fiber optic communications around the world, run them through data warehouses, and gather and read private information. And in May 2001, just weeks after a European Parliament committee hearing on Echelon, the U.S. government released its annual wiretap report: In 2000, sixty percent of the 1,190 wiretaps authorized by federal and state governments were for wireless devices such as mobile phones and pagers.

While some of these government incursions fill legitimate national security requirements, others are based on the belief that the government should know everything on the off chance that something of concern is mentioned. As a former head of the New York FBI office once said, as part of a plea for renewal of wiretap privileges that had recently been removed because of abuse, “If your child were kidnapped, wouldn’t you want us to be able to know what the kidnappers were saying?” This was coupled with the belief that you shouldn’t worry about government surveillance if you have nothing to hide, and an apparently-genuine belief that the system is designed for the common good, and while abuses may have happened in the past – even in the recent and immediate past – they will not happen in the future.

While private industry may have difficulty securing its data from governments, it must still attempt to secure information from others in the private sector who have resources and capabilities which may not be on a level with those of governments, but are still powerful, and not constrained by the benign good nature of the government. Controlling and maintaining a secure information environment has become a security manager’s nightmare, and it will get worse: In three years there will be more than 800 million wireless data users in the world and executives must act now to ensure that employees have wireless access to national networks, corporate servers, and each other.

While few have yet encountered serious wireless enterprise break-ins or hacks, as we noted in *Wireless network party lines* in the May 2001 issue of the *Business Security e-Journal*, this is a matter of timing and chance, not of adequate security levels. Every current danger existing for hard wire line

systems exists for wireless systems, but without the boundary of the lines. New forms of wireless communications will increase the number of threats.

Many believe that they need to focus on where computers and wireless devices overlap, but the truth is that you must defend against the entirety of the problems not just the interface of the two, while actively monitoring for incursions and reacting to them.

The most vulnerable parts of wireless enterprises are where different networks connect. Many security features and standards currently in use were added as an afterthought to existing wireless protocols, and, even if adequate. Relying on any given wireless protocol to safeguard your corporate intelligence, rather than on a balance of technology, monitoring, and reaction, creates a possible opening for criminals (in which category we include corporate spies).

## **5. Real Stories from the Field — Sticky fingers and stolen code**

Six people have been sentenced for the theft by Avanti employees of code from Cadence Design Systems (*People vs Avanti*). The stiffest sentence was one year in the San Mateo County jail.

The problem was discovered in 1995 by a Mr. Markhan when he saw a demo of Avanti's ArcCell and noticed a misalignment that he had recently corrected in the Cadence product, Symbad. In defense, Avanti's lawyer argued that much of the code, including, presumably, the misalignment, came from public domain software.

In response, the prosecutor showed a picture of a tape labeled "Backup Wuu tape 00 02/09/91." The Cadence witness said that Wuu means Steven Wuu, a co-founder of Avanti, and "00" means you downloaded a complete folder. The tape contained about 30,000 lines of code from Cadence's Symbad database software. The code contained words that were consistently misspelled in Cadence's Symbad *and* in the data base code found in the suspect products.

On the Avanti defense side, Chi Ping Hsu, a member of Avanti's technology staff, says that when he was at UC Berkley he laid out the building blocks for *all* of the products being discussed in this case. He says that he developed most of the code, and posted this code on the Berkley Building Block Layout (BBL) system in the early 1990's. This has been a shot in the arm of the Avanti defense.

The current argument is over the amount of restitution. Avanti is arguing for a settlement of \$16 million and Cadence is arguing for a settlement of \$700 million. The judge is still hearing the case on damages and is expected to rule soon.

## 6. Book and Product Reviews

*The National Directory of Public Record Vendors*

BRB Publications, Inc., ISBN#: 1-879792-63-X \$59.50

<http://www.brbpub.com/> 1-800-929-3811

The book contains 1188 pages of information on retrieval specialists in 50 states broken down by the various counties in which they operate. We have used this book to find public records researchers in several different states. All of the records retrieval personnel have been knowledgeable, but not all are equal. For the same services we have had quotes that differed by a factor of four, so it pays to shop around. It also contains an index of pre-employment screeners and tenant screeners.

The book is very helpful in the amount of time it cuts from playing hunt-and-go-see for information from a far off location where you have no local knowledge or contacts. It has been, and continues to be, a valuable resource for our investigative and research practice. If you do any public-information record searches outside of your local area it will pay for itself in time-savings with the first use.

## 7. Free-Subscription/Unsubscription Information

•• *The Business and Security 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 L. Burke Files ([LBFiles@lubrinco.com](mailto:LBFiles@lubrinco.com)), Mary Clark Fischer ([MCFischer@lubrinco.com](mailto:MCFischer@lubrinco.com)), and Richard Isaacs, CPP ([RBIsaacs@lubrinco.com](mailto:RBIsaacs@lubrinco.com)).

Risk management is about increasing productivity and profit. **The LUBRINCO Group** provides senior executives with specialized risk management assistance in areas that affect domestic and international bottom lines.

**LUBRINCO** provide service in three areas of high risk typically outside the expertise available in-house:

- OPSEC: The identification and protection of information that would be of value to your competitors and adversaries.

- International financial investigation and due diligence and enhanced due diligence consulting (with particular emphasis on Central and Eastern Europe, the offshore financial centers, Beijing and Shanghai, and Latin America) relating to:
  - Anti-money laundering and financial fraud issues under the USA Patriot Act and the EU Revised Money Laundering Directive of 2001.
  - Establishment of business relationships and strategic partnerships.
  - Location and recovery of substantial (greater than fifty million dollars) missing assets.
- Protection of management, staff, and families in the high-risk environments of Latin America, Africa, the Mid-East, and Southeast Asia, and when traveling and living overseas, or when transporting high-value (greater than fifty million dollars) items.

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

To sign up for a **complimentary subscription** to *The Business and Security e-Journal* or the *Business and Security 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 *The Business and Security e-Journal*, please send their e-mail address to [ejournal@lubrinco.com](mailto:ejournal@lubrinco.com).

If there is a topic in the business and security fields 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 *The Business and Security 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 *The Business and Security 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 *The Business and Security 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 *July 2001 Business and Security e-Journal* (© 2001 BSEJ), to be found at <http://www.lubrinco.com/> .

The *e-Journal* is a forum for the exchange of information, ideas, operating styles, theories, and related topics for corporate managers who make decisions in areas of high risk 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 the *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 the *e-Journal*.

Please be safe, and be smart.