



ÆGIS e-journal

Addressing threats that affect your bottom line

Volume 7 Number 6, June 2000

From the case files of

The LUBRINCO Group
<http://www.lubrinco.com/>

and

Financial Examinations and Evaluations, Inc.
<http://www.feeinc.com/>

Concealed assets in fraud, theft, and divorce? Call us!

This month's features:

- 1. Due Diligence — Encouraging theft, fraud, and violence**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Central & Eastern Europe, both paradise and hell for CI professionals: Some special considerations for those on the outside looking in**
- 3. Executive Protection — Being your own protective agent**
- 4. Technical Issues — Protecting your home and small-business computer from crackers**
- 5. Real Stories from the Field — Porn surfers go to Chad, plus a bonus story from the land of Duh!**
- 6. Book and Product Reviews — Against The Gods - The Remarkable Story of Risk
Shoplifters Vs Retailers: The Rights of Both**
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Encouraging theft, fraud, and violence

When we speak of fraud, we generally speak of the *fraud triangle*: *Opportunity*, *Pressure*, and *Rationalization*.

Opportunity is just that: The opportunity to steal, in which we carelessly or thoughtlessly present a potential thief with the active temptation to steal. Opportunity includes such things as leaving your Palm Pilot on the table in a crowded restaurant while you go to the bathroom, not protecting small-but valuable merchandise, allowing the same person to issue purchase orders and pay invoices, and allowing delivery and pickup of merchandise at the same loading bay.

Pressure is an economic need (real or imagined) that causes the person to feel he needs to steal, and can range from illnesses for which he may need money, to a gambling compulsion, or a host of other reasons.

Justification is the reason invented by the thief to rationalize the theft or fraud.

The traditional view has long been that while opportunity is within our control, both pressure and rationalization are not generally as obvious or as controllable. Because of this, most fraud prevention efforts have involved putting in place procedures that reduce the opportunity for fraud, and catch it when it has occurred. As an example, we do not let the person who issues purchase orders accept shipment or pay invoices. And we use auditing to detect when fraud has been perpetrated.

Recently, however, we have seen a trend — for which we do not as yet have hard statistics — toward fraud, as well as theft and violence, in which there was, in fact, *no* economic pressure in the classical sense, and no necessary causal opportunity. Instead, the acts were in retaliation for what was felt to be bad behavior on the part of the company, and for which the attacker is striking back. While the details vary, you will discern is a common theme in the following four examples.

It is a sad fact of life that people sometimes get fired or laid off. Assuming it is not for some criminal cause, a skilled and careful administrator can present this life-shattering event as an opportunity for the person being letgo. It is not uncommon, however, for administrators to *choose* to give someone their walking papers the day before Thanksgiving, Christmas, or some other major holiday. While this may seem clever in a Dickensian sort of way, it breeds ill-will not only on the part of the person fired, but, also, with that person's peers. Sadly, albeit not-unreasonably, some people react poorly to

hostile, thoughtless, and uncaring working conditions. From the employee's point of view this might be considered *theft of dignity*.

Some companies like to get the most bang for their buck from employees, and have them work extra hours without paying them for the extra time. Often this is done by making employees "professional" or "management" employees, since this class of employee does not receive overtime. This allows the company to pay an employee for 40 hours of work, while having the employee actually work 50 or 60 hours per week. For those of you who wonder why the GNP is greater than it should be, this uncompensated time represents part of the missing piece. From the employee's point of view, this might be considered *theft of time*.

Many insurance companies, including HMOs, believe that their function is to take payments from policyholders, but not give it back. It is, therefore, their policy to refuse many classes of claims on first submission, forcing the claimant to appeal the rejection. In the case of medical insurers, procedure payments are booked based on the lowest common denominator of payment, so that generic drugs and standard treatments are more likely to be approved than more-costly treatments, even if those treatments might be more appropriate for the individual patient. In addition, hospital stays are likely to be much shorter.

The up side of this is that, in the beginning, this did cut a good deal of fat from health care costs. Unfortunately, once the fat is gone, further cuts have to come from flesh, and there develops an increased likelihood for inappropriate or inadequate treatment. This is not a problem for those with enough money, but some small number of people are likely to become cranky when their loved ones suffer or die because their medical condition falls outside the desired limits. While an *intellectual* case can be made that certain heroic treatments are appropriate for someone who is (young, smart, cute, famous, *ad nauseam*), on a *personal* level the logic fails the treatment is withheld because the patient is old, or not likely to survive for other reasons, but happens to be your mother or father or sibling or beloved.

A variation of this is unequal benefits in corporations, a problem brought about by a belief that the primary function of a company is to reward upper management. We have seen cases in which a senior manager receives compensation in the tens of millions, as a consequence of which the other employees are forced to pay for their own health insurance or other benefits.

In other cases, corporate claims officers may take a cue from insurance and health providers, and exclude as many benefits to employees as they can.

From the employees' or policy holders' point of view this might be considered *theft of benefits*.

Finally, we have the case in which companies consider their smaller suppliers to be an interest-free extension of their credit line, and will take 60, 90, or even 180 days to pay. This can be enough to strain, or even break, the credit of a small supplier. This pyramids down, with small contractors then being unable to pay *their* suppliers. From the suppliers' point of view this might be considered *theft of revenue*.

What is the reaction to these various kinds of theft? It varies. The lowest common denominator is that it always results in a lessening of both the quality and quantity of service provided by the victim to the thief. Moving up the scale of retaliation we find an increase of petty theft. For those more deeply hurt it can escalate to more serious theft and fraud, and an increased inclination to sell — or even give away — proprietary information if it will harm the offending employer. Finally, in extreme, albeit rare, cases, it will escalate to violence. In all cases, the problem could have been avoided through proper behavior on the part of the company in question, generally at relatively little — and in some cases no — additional cost.

For many companies theft and fraud are still a balance-sheet issue. This is because most fraud — other than fraud by senior-level management, which appears to have lessened as executive compensation has skyrocketed — is relatively small in nature, and acts of violence are sufficiently rare and can be handled by insurance. Thus, a decision may well be made that it is more cost effective to have lower productivity, theft, fraud, disclosure of proprietary information, and occasional violence than to exercise due diligence in their prevention.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Central & Eastern Europe, both paradise and hell for CI professionals: Some special considerations for those on the outside looking in

Contributed by Central & East European Business Intelligence & Knowledge Management Community

So you are seeking to expand your CI capabilities in Central & Eastern Europe (CEE), eh? Perhaps the best advice in a nutshell, applicable to anyone not yet initiated (i.e., less than a few years on the inside, no local language, and culturally illiterate), is as follows: expect the unexpected, not forgetting that Central and East Europeans, like you and me, are also members of the big family of *Homo sapiens* (humans will be humans wherever you go). While CEE folks traditionally tend not to trust one

another very much, the grapevine has roots deeper and more expansive than almost anywhere else on earth, and not many people here have ever even heard of CI. This adds up to fabulous opportunities for tapping into multitudes of human sources, with success proportionate to your ability to establish trust and some special, even romantic, relationships.

What advice might be most important? Be in for the long haul: Don't wait for big disasters to happen before you deploy your own internal or external CI professionals to focus on these countries. CEE is a nut that must be cracked from the inside out. Lots of weird things — and at least a few major disasters — will happen, so be prepared for them: You don't want to be one of the many foreigners who, after their short, exciting ventures went sour, left CEE with their tails tucked between their legs in total shame.

CI professionals worth the gold in their teeth are very scarce in CEE. What is needed is international experience, in-depth multi-cultural involvement, well-developed language and interpersonal communications skills, special ability to build trust and elicit information, plus all the other skills needed to excel in the fast-paced, modern, business-oriented world of today which were not learned in school, at home or through real-world experience by the bulk of CEE folks. And remember that there are lots of “security” people around, but not many know how to protect companies' assets against modern day CI or economic espionage efforts.

While the price of a loaf of bread in CEE may still be much lower than back home, don't expect that your CI efforts will be less expensive here. The cost of doing business in CEE is rising continually; many things indeed cost a lot more here; it can take more time here to get “publicly unavailable” data; issues of nationality can be important; and if your project may put the future of locally-based CI professionals at special risk, be prepared to pay more than you would like to.

Each CEE country is unique, and conditions for the practice of CI differ within each country, but there are many common characteristics in terms of behavior, ways of doing things, and the pathways of transformation into new modern entities, all of which are sufficiently similar to draw useful parallels. (The CEE countries referred to in this article are the Czech Republic, Slovakia, Poland, and Hungary. Largely beyond the scope of this article are Russia, Ukraine, Belarus, other points further east, and the former Yugoslavia to the south.)

CEE as CI hell

How might the CEE countries be “hell on earth” for CI professionals?

Well, first, here in CEE it is pretty tough to earn your CI stripes sitting in front of a PC all day and surfing through online databases. While very few CI efforts today, no matter where focused on this planet, can claim true success without intense human source collection activities conducted in the real (non-cyber) world, the problem is further compounded in CEE due to several factors which require lower expectations from “published” sources such as databases, online public records, aggregators, etc. For the most part, court records are not yet entered in electronic information systems (let alone online); credit reports are non-existent; and investigative, objective media reporting, while not totally absent, leaves much to be desired.

But let’s get past the “level playing field” stuff. Other factors which make CI tough to execute in CEE:

- There are too many snobbish, under-qualified, overpaid foreign consultants and investment concerns running around, and many of them operate with low ethical standards.
- Local (and foreign) investigative sources, detectives, and the like won’t hesitate to use illegal means and eavesdropping devices.
- Only a small portion of the population use the Internet (some 5% in the relatively sophisticated Czech Republic, for example).
- Language, cultural, and mind barriers: You don’t know what’s being said, and even if you have the best interpreter, much of what is said is far beyond your understanding due to cultural and thinking barriers. Things *ARE* done differently in CEE. People *DO* have different habits, different values, different morals, different priorities, different ways of seeing things.
- Distractions: Beautiful touristic sights, ancient castles, enticing girls, good (and cheap) beer. Everybody seems so lazy — why not me too....
- Poor telecommunications infrastructure.
- Low level of customer service.
- You can spend lots of time talking to people who are interesting, but don’t know very much.

- You don't know who, if anyone, you can trust, when the going gets tough. Loyalty to a company, organization, etc. is even scarcer here than back home.
- New personal data protection laws may mean that the police can come knocking on your door with a warrant to search your database.
- You want results, fast, but things do not happen so fast in CEE.
- You lack a realistic, long-term CI strategy in CEE: It hasn't been amongst your top priorities.

CEE as CI paradise

On the other hand, CEE is also a CI paradise due to factors including (but not limited to) the following:

- People are not CI-aware. The vast majority are naive and unsuspecting with regard to CI agendas (They will share all kinds of information with you, and don't even require your identification.). Don't get me wrong: For historical reasons CEE people are in many respects less trusting of authorities, other "big guys," and neighbors than their western counterparts, but they, in general, lack much knowledge of the ways of the modern business world. They assume that sophisticated collection efforts aimed at the normal everyday Joe died back in 1989 with the fall of communism. They don't realize that business is war. Next to their dogs ("a dog is man's best friend" really hits home here), they tend to trust nobody more than the skilled CI agent, who gains as much trust as a dog by telling them what they want to hear.
- Human contact and interaction is highly facilitated, largely due to the closer proximity of people in more crowded public places, extensive public transportation systems, streets made for people not cars, and the social nature of the people. Shadowing and surveillance can be easy in the bowels of a big city with streets built for walking as opposed to a typical western grid of streets.
- There is an abundance of attractive, single (or otherwise available) young women, who may serve as anything from helpful companions to focused collection partners.
- There is a tendency to share information without much forethought or hesitation. In a society where the truth was discovered for many

decades mainly through informal, human communications (official sources such as government and media not trusted), great volumes of useful information not to be found otherwise moves in audible form between human beings. It is easy for a talented CI professional to assume a non-threatening role here.

- People have been conditioned to living in a “normal,” predictable world. They do not want to be seen as abnormal, and are not well prepared to deal with the unexpected (although it entertains them).
- People exhibit a tendency towards comfortable survival. Laziness and preoccupation with the self characterize vulnerable targets.
- “Partners in crime” situations can be discovered and exploited. Much of the wealth of business persons in CEE today is built through some “partners in crime” relationship, where some favors/advantages have been exchanged between parties. These often involve unethical, criminal, or other questionable activities which the parties wish to keep secret — or at least want to keep out of the public eye. These parties each possess potentially-damaging information regarding the other party and, more often than not, goodwill between confidential parties dissolves, or is at least weakened over time or in the face of difficulties. By following cues from third parties, and the public silence that exists between partners in crime, the CI professional can home in on potentially valuable information, and take appropriate measures to obtain it.
- Information technology, the internet, and mobile communications infrastructure and culture is advancing by leaps and bounds. You won’t look weird walking around talking into your mobile telephone or with a earphone hanging out of your ear.
- People think that technology will solve their problems, so they throw lots of money at it, yet remain vulnerable to more human-focused approaches.

Connections to the past

Local business leaders often place themselves in ivory towers, basking in the light of their relative power (in relation to the poor masses), and are vulnerable targets for skilled CI professionals. What makes them weak is also your weakness: Human source CI professionals are scarce (lack of threat) and in high demand.

Almost everybody who was established as a business leader in the early nineties has and/or still has connections to a communist past. The questions to ask are many: Has this person been involved with the typical corrupt privatization practices of state companies? How much of this person's success is rooted in hard work as opposed to manipulating power of connections? What connections does the person have which are most relevant to this person's success and what are their pasts? Has this person been through any unusual personal/professional transformation, such as that gained through studying or working abroad? How does this person react to situations of conflict? Does this person have any modern concept of customer service? How does this person relate to the media and the public?

In the Czech Republic, the database of former secret police operatives — part of which is available at the time of this article at <http://www.cibulka.cz/> (it may soon be banned due to new personal data protection laws so get Cibulka's CD today) — may give some basic indications of strong connections with the communist past. The business register at <http://www.justice.cz/> may reveal some basic business connections. And various Czech media archives may produce a few good leads. Court records are not anywhere near as accessible as in the US, and don't assume that police and other officials are all the "good guys!"

"Communist" is no longer a good label to place on anybody here today simply because times have changed, but human change comes slow. The tendency towards "comfortable survival" characterizes the masses. You can use a different label on the same product if you will: "hard headed," "lazy jerk," "stupid idiot," "rude waitress," "unapologetic imbecile," "shameless gold digger," "hyena," "shark," "lousy salesman," "bad customer service representative" ... or whatever, but perhaps it's better not to use labels in a verbal sense, and rather focus on analysis featuring different models of describing personalities and predicting behaviors that will enhance your CI results. Face it, anybody who was here lacks the kind of skills which are essential for survival in the West. Invest massively in the education of your own people, and exploit the advantage over others who learn too slowly.

And don't forget you cannot understand the present without delving, often deeply, into the past!

A quirky observation regarding local trust

Building trust with human sources is key to opening them up and learning from them, and this often needs to happen within a short period of time.

Ironically enough, in many cases a non-Czech investigator is able to elicit information much better from a Czech than a Czech investigator. Everything boils down to the special capabilities of the elicitor, including sufficient local language skills, deep understanding of the Czech mind, adequate planning, and adaptability to the specific source's personality and situation. An older man in a small Czech town told this investigator recently that he would not trust and share the information that he shared with me with any German or any Czech. Being American does provide some powerful clout with a majority of the people. But again, it always boils down to the individual, and nobody should abuse their status by engaging in unethical and/or illegal practices. The ability to be perceived by sources as a person who can be trusted is an art. Just as the professional lover succeeds in building trust with many partners, so does the CI professional find success in establishing trust with his or her sources.

Small and Medium Enterprises are vulnerable targets but big companies are not much better off

SME managers are too busy trying to get basic business functions operational. A "competitive intelligence unit" is as common as a chocolatecoated asteroid landing in your backyard. Even the biggest companies are quite CI illiterate: There are other "more important" things to do than train local managers. There are scores of big investment funds, venture capital sources, etc. who repeatedly fail with their investments, and it's all due to lack of real CI capabilities based upon experienced local professionals.

Susceptibility to elicitation

The things that people in CEE will tell me within the first few minutes of our initial meeting never cease to amaze me. Sincere effort to elicit information with minimum risk to the source for providing the information is divinely rewarded time and time again in CEE. Consider some basic elicitation techniques such as those ingeniously presented in the recently published book *Confidential* by John Nolan of Phoenix Consulting Group: provocative statement, quid pro quo, simple flattery, exploiting the instinct to complain, word repetition / reflective listening, quotation of reported facts, naiveté, oblique reference, criticism, bracketing techniques, feigned or real disbelief, and the infamous purposely erroneous statement.

Why do most of these techniques work so well in CEE? Well, for starters, CEE folks are simply very human and, second, most of them have never heard of anything such as "elicitation techniques!" These techniques work

like a dream, over and over again in CEE, and certainly much better than in the increasingly wary West. CEE, in many respects, is indeed a paradise for human source CI collection activities, but an expert in elicitation coming from one country to another needs an intensive readjustment period.

Many CEE folks will look at these techniques and then say something like “It’s not practical enough. I’m looking for some new software for searching through....” and then scratch their heads like monkeys when their businesses fail due to elicitation techniques used against them, and their own total lack of active usage of such techniques.

Criminal society perception

Sitting back in the USA or some other far-away, exotic, land, the images of CEE presented by the media may result in the perception that CEE is overrun by criminals, mafiosos, whores, ethnic cleansers, hit men, bandits, and the like. First, the CEE countries which are the focus of this article do not include former Yugoslavia, the Ukraine, Russia, Chechnya, etc., where crime and terror often assume much higher profile (contract killings are quite rare and mass graves are almost nil in the target countries of this article). In fact, these countries to the east and south are sources of many of the criminals who are increasingly spreading like the plague in the CEE countries upon which this article is focused.

Second, the CEE countries which are the focus of this article are, in many ways, much safer than a long list of western countries, with many of the people on many levels better behaved, more trustworthy, and more respectable. These people have a tolerance and a social wisdom which is to be admired. There is much, on a human level, that the West can learn from the East. So, while your CI operations should be very keen to discover any criminal connections, and be prepared to pay more when CI specialists endure larger risks in such situations, the bulk of the real issues here are going to be noncriminal. Something that is announced as a crime is often exposed as to a pre-meditated smear campaign to influence public opinion.

The substance abuse factor

Knowing whether your target smokes and/or drinks is not important. On the light side, taking a source out for a beer or two, or perhaps a candlelit dinner and a bottle of wine, can really help to open communication pathways. Getting heavier, targets with chronic smoking and/or drinking habits are in many ways predictable and suckers for various forms of exploitation. And if

you want to establish your business here, do you want a manager who gets nervous and has to light up a cigarette every 10 minutes and can't get through a day without his dose of Black Death vodka?

The sexual element

The best CEE human source intelligence professionals are keenly aware of the differences between the sexual landscape in CEE and western countries. What's different about females here? Everything: Genetics, the importance of public appearance (dress, makeup, etc.), nonverbal/verbal ways of communication, expectations, games played, attitudes towards work and responsibility, hard-to-please cat-like behavior. With over one-half of the population female, and with most males having close relations with one or more females, you had better bet your bottom dollar that in-depth understanding of the nuances of such relationships are important to your CI efforts. There are many documented cases of entire businesses failing in CEE due to poor treatment of such relationships.

Don't underestimate or overexploit the Central & East Europeans

While you may be convinced that doing business in CEE is too tough and/or hopeless for you, and decide not to risk it, don't take the easy way out and blame it all on the people of CEE. While there are many thieves and scoundrels, whores, and mafiosos, back-stabbers, and lazy idiots in CEE, there are many wonderful, trustworthy and highly capable people in CEE (lots of untapped talent), and don't forget that you have, in some form or another, just as dirty — if not dirtier — scum back home. Don't blame the failure of your business in CEE on the people and conditions, when the true blame should be placed on your failure to adopt and nurture proper CI at an early stage.

It is highly recommended that you do not take the fast and hard "quickie" approach, where you thrust some CI people in on a whim and then pull them out (or let them die off) when the going gets hot. Bad impressions gained by locals as a result of "dirty tricks" performed by US, English, Canadian, German, or whatever nationals tend to spread to the entire nationalities of these countries.

Patience and tolerance in addition to strong personal as well as professional desire to build a future for CEE and its people are essential indicators of a CI professional with true capabilities.

Again, when shopping for CI capabilities, real value will be found with foreign nationals who have behind them the larger count of years on the inside and/or locals who have deeper experience and more extensive training on the outside.

The NEM connection

CI in Central & Eastern Europe requires extra emphasis on intensive longhaul development of human sources, and there is a new emerging class of source called "Niche Electronic Media (NEM)" which seeks to provide such solutions even to the relatively new and less established. While beyond the scope of this article, these non-commissioned NEM sources (which this author will discuss in greater detail in an upcoming issue of the *e-Journal*) focus on providing you with in-depth answers to critical questions through the use of "anonymous soft-tasking" and multimedia (video, audio, imagery) reporting.

Conclusion

If your resources are limited and you can only afford one-half a person on the inside, you'd be better served forgetting about doing business in a CEE country. If you can afford one entire person, however, make that person a CI professional, or use the equivalent finances to invest in a capable CI service provider before deciding whether or not you want to invest more in your presence in the country with your own people.

Will your CI operations in Central and Eastern Europe be paradise or hell? You will most certainly get a taste of both, but as to which way the scales tip is entirely up to you.

Central & East European Business Intelligence & Knowledge Management Community (CEE BI & KM Community) <http://www.bikm.com/>

3. Executive Protection — Being your own protective agent

Most of us are not in a position to afford protective agents. In general this is not a problem, because most of us face no danger in our lives, and do not need protective agents, and, in truth, would find their presence constraining and onerous. Even with this being true, under what extraordinary circumstances might we normal people, face the danger of physical assault?

As a rule of thumb, you will find yourself in danger of assault for one of two reasons: Bad judgment or bad luck. In both cases you end up being in the wrong place at the wrong time.

Bad judgment involves your *choosing* to be someplace that you shouldn't be, at a time when you shouldn't be there. Thus, while you have a right to be anyplace any time, this author would not choose to go jogging, alone, in Central Park at 11 P.M.. And it is clear to most of us that there are neighborhoods in which our mere presence evokes some hostility from those around us. To a large extent, we have initial control of the situation, and have chosen to be where we are. There are a lot of things you can do to keep these types of incidents from happening, mostly by exercising prudence and reasonable judgment.

Bad luck is not within our control: We are someplace where we have a reasonable expectation of safety, at a time when we have a reasonable expectation of safety, and are caught up in circumstances beyond our control, and in events so statistically anomalous as to be un-preventable. Thus, one could not be faulted for renewing our license at the DMV on the rare day that a cranky patron becomes crazed. Or in a Wendy's when a former employee decides to violently rob the place. Or in a school when some students, who have, over time, become increasingly and obviously alienated and scary, try to blow (or shoot) the place up. Or on a commuter train when a madman starts shooting. Or in a retail store which is being robbed, again. While these circumstances beyond your control might have been prevented by the actions of others, there is nothing *you* might have done to prevent them.

In some cases in which your life is actually in danger during an assault, a claim might be made that having a gun would have allowed the situation to be ended in a timely manner. While this is true in theory, in practice there are a few problems. For a start, while the likelihood of being involved in such an incident approaches zero, you will still need to carry a gun with you 24 hours a day, 7 days a week in order to have it with you the one time you need it. This may not seem like a big deal, but carrying a couple of pounds of steel strapped to you, always covered up yet accessible, is extremely onerous. Indeed, it is so onerous that most people who get concealed carry permits carry a gun for a few weeks, then, the novelty having worn off, never carry one again.

A more serious flaw is the fact that, unless you have thought it through in advance, you are unlikely to react appropriately in a crisis situation. Thus,

while a gun is used by a civilian in the US about once every 14 seconds, and about 75 lives are saved by a gun in civilian hands for every life lost, most of these are what we might term “normal” uses, where there is a robbery or a similar incident about which you have thought, and where you have the leisure to act in an appropriate manner.

But if you are sitting in a train, and bullets suddenly start flying it is much less likely that you will react appropriately. Thus, unconfirmed rumor has it that there were 7 armed people on the Long Island Railroad when Colin Ferguson started shooting, including 2 police officers, yet nobody intervened. Indeed, during the rather lengthy periods when Ferguson was reloading, nobody took action. Thus, while a gun or other emergency safety tool *in the hands of a trained user able to react appropriately* will end an unexpected violent situation, it is rare for either a civilian or a law enforcement officer to be sufficiently well-trained and mentally prepared to act appropriately in unanticipated and unplanned-for circumstances.

Putting aside these incidents so statistically rare that they make the front page of every major newspaper in the world, what emergency safety tools other than guns might be available to help deal with more defensible assaults. One that springs to mind is personal defense sprays. This author was responsible for the general commercial introduction of pepper-based sprays to the law enforcement community at the 1988 conference of the American Society of Law Enforcement Trainers (ASLET), for the introduction of training for law enforcement in the use of personal defense sprays at the 1989 ASLET conference, and for the introduction of a civilian program at the 1990 ASLET conference. At that time personal defense sprays based on tear gas (CN and CS) had fallen into disfavor within law enforcement: CN was in disfavor because it was too mild, and worked poorly on pain-resistant subjects, with about a 30% failure to control rate. CS was more effective with about a 12% failure to control rate, but there was still a cloud over it because of its use on civilians in the ‘60s. (Note that there are now also CS/OC blends, which give roughly an 8% failure-to-control rate.) Philosophical objections aside, the major problem was that CS and CN are irritants and work by causing pain, and, by definition, pain-resistant subjects don’t feel pain.

Pepper-based sprays, often referred to as aerosol subject restraints (ASRs) (or *OC*, because the active ingredient is generally *oleoresin capsicum*), unlike teargas, are *not* irritants and do *not* work by causing pain. Rather, they are *inflammatory agents*, and work when the atomized vapor is inhaled, causing the capillaries of the trachea to dilate, producing uncontrollable

coughing. And, important from the view of law enforcement, because they are bronco-dilators, rather than bronco-constrictors, they were unlikely to harm those with asthma.

The good news was that, *in the hands of a trained user*, ASRs had a *near-zero failure-to-control rate on pain-resistant subjects*. The bad news was that in the hands of an *untrained* user they could have up to a 70% failure-to-control rate. Since the average police department devotes less than 4 hours per year to firearms training, the urge to train adequately in use of a personal defense spray often seems hard for a department to justify.

But even assuming that one had an appropriate emergency safety tool and training in its use, and the mindset to use it in a crisis situation, the goal of personal safety still remains one of *avoiding* confrontations, rather than winning them. This is the subject of a book, not an article. Fortunately, this author has written just such a book, and has made it available for download **free** on the Internet.

For more information about personal safety in general, including use of personal defense sprays, you should read *The Seven Steps to Personal Safety*. With over 20,000 copies in print, this book is widely regarded as the leading book for civilians on dealing with violence. *The Seven Steps to Personal Safety* can be downloaded in its entirety, **free**, at <http://www.lubrinco.com/7steps.html>.

4. Technical Issues — Protecting your home and small-business computer from crackers

There is increasing concern about attacks on computers, with the commercial losses from attacks being in the hundreds of millions of dollars. This has led to concern among many people about how to protect their computers, even at home, from evil attackers, with the evil falling into two general categories: Malicious viruses, and crackers taking over your computer while you are connected to the internet and either stealing data from it or using it as a site participating in denial of service attacks. As with any scary statistic, it is a good idea to look a bit closer at the numbers to see how much risk you face.

For a start, in one recent study about 45 percent of all commercial losses were from unauthorized insider activities. The home equivalent would be a child deliberately erasing something on your hard drive. About 30 percent of the losses were losses of proprietary information, much of which is sold or given away by insiders. Some was from outsiders, who need little more than a browser to get proprietary information off your web site. About 15 percent

was be telecom fraud, and about 7% was from viruses. The rest was stolen equipment, outside crackers, denial of service attacks, and the like.

What does this tell us? It tells us that our biggest concern should be having a good anti-virus program that you keep up to date! The better programs allow you to get updates from the Internet, and this author checks for updates daily.

You should also look to see what is used to transmit viruses. At this time, many virus-developers use Microsoft Outlook to transmit viruses. While Outlook is a fine program, this author has moved to Eudora for email, thus sidestepping the problem, at least until virus developers start using Eudora.

You should also check for security updates on a regular basis. Microsoft regularly puts updates online that deal with security problems. These should be installed when available.

How about something like a personal firewall, which makes your computer invisible when connected to the internet? In theory the likelihood of needing a firewall if you are connected via modem is somewhere between slim to none, and slight if you are connected via a DSL line or cable modem. On the other hand, slim is not the same as nonexistent, and good personal firewalls vary between inexpensive to ZoneAlarm, which is available for download **free** for personal use (<http://www.zonelabs.com/>). Firewalls are easy to install, and, once running, are unobtrusive. Not to install a firewall is foolish.

Most important of all, however, is protecting your data by regular backups. With the arrival of Zip and Jaz drives, even large amounts of data can be conveniently backed up. This author uses a program called *Back Again* (<http://www.cds-inc.com/>), which is one of a number of good backup programs available for home and small business use. The current approach is a full backup of all data and other important files, then, at 5 A.M., the program automatically does an incremental backup of everything changed on the computer since the last incremental backup. When the Zip disk containing the incremental backup gets full, a new full backup is done, and the cycle starts over. In addition, a copy backup is done daily, and carried when leaving. This means that even if the building burns down all the data is safe.

Finally, a number of companies provide encrypted storage online. Some, such as X-Drive (<http://www.xdrive.com/>) provide some amount of **free** storage, with more being available at a nominal cost. The virtue of this is that you have access to the data from anyplace where you have internet access.

5. Real Stories from the Field — Porn surfers go to Chad, plus a bonus story from the land of Duh!

Telephone subscribers have been complaining about "free" porn Web sites that make their money by disconnecting Net users' phones and reconnecting them to an Internet provider in Africa at up to \$7.31 a minute. According to a telephone company spokesman, the scam is apparently legal, because the sites have small-type disclaimers warning that porn-hungry viewers may be rerouted for a fee.

The sites ask users to download a dialer program that, when launched, redirects their internet connection in exchange for viewing the 'free' porn. What they're doing, unfortunately, is perfectly legal. Read the fine print....

The scamsters learned their trick from a 1997 incident in which internet users visiting a certain web site and installing a piece of software were reconnected to a phone number in Moldova. That case was, in fact, fraud because you were not told what was happening, not even in fine print.

Experts have said that foreign governments sometimes make deals with companies running psychic hotlines, sex chat lines, or other premium phone services, in order to receive a portion of the revenue from the service.

Story from the land of Duh!

A new internet business was created by Equinix as the "Fort Knox" (Fort Knot) of the internet. The building is located in a nondescript section of San Jose. The reporters who were brought in were required to sign a nondisclosure agreement regarding the building they were going to see: As part of the building's security they could not disclose where the building was located. The next day the San Francisco Chronicle printed the address of the building, as well as a picture. It seems the building was tracked down over the Internet through its business license. Duh!

6. Book and Product Reviews

Against The Gods - The Remarkable Story of Risk

Peter L. Bernstein

John Wiley and Sons, \$27.95

This is a wonderfully written book about the discovery of how to measure and quantify risk. It begins with the mathematical calculations Blaise Pascal and Pierre de Fermat used to solve the odds of simple game of chance. And

how those simple solutions of the 1600's have lead to the solid foundations of the insurance industry, and catalyzed economic growth generally.

Shoplifters Vs Retailers: The Rights of Both

Chuck Sennewald

New Century Press ISBN 1-890035-18-1 95 pages \$11.95

<http://www.shoplifting.com> 1-800-519-2485 1-619-476-7400

Chuck Sennewald brings both expertise in retail security and a keen sense of presenting information in a useful manner to this 95 page book. Much of the book is given over to twenty scenarios, viewed from the perspective of the customer as well as the store employee.

The scenarios are quite varied, and include cases in which the customer was shoplifting and those in which the customer was, in fact, *not* shoplifting; in which the store employees behave properly, and those in which the store employees behave improperly. It covers most of the likely cases, and anybody reading this will have a very good idea as to how to behave in most cases they are likely to encounter. Best of all, it gives enough information for people to apply common sense in their dealings with possible shoplifters.

We recommend this book for anyone involved in those aspects of retail security where they might be interacting with possible shoplifters, and for anyone responsible for managing or training those retail employees who might be interacting with possible shoplifters.

7. Free-Subscription/Unsubscription/Copyright Information

•• AEGIS e-journal is supported and maintained by voluntary efforts. This 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 June 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.