

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 10, October 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 — Online banking**
- 2. OPSEC, Economic Espionage, and Competitive Intelligence — Virtual company**
- 3. Executive Protection — Facing airline hijackers**
- 4. Technical Issues — Fake financial documents**
- 5. Real Stories from the Field — Pirates**
- 6. Book and Product Reviews**
- 7. Free-Subscription/Unsubscription/Copyright Information**

1. Due Diligence — Online banking

Internet users should always think twice before responding to e-mail requests for their personal details! Recently, an online bank had the following fraud perpetrated on it.

This is how the scam worked: Bank customers received an e-mail message, supposedly from their bank, saying that some of their details had been lost due to an archive problem.

Because the bank was “serious about security”, it had no spare copies and requested the customer kindly to re-register. A link direct to the bank’s site was provided on the message, to make things easier.

The link in fact was to the fraudster's site, a faithful copy of the bank's. No fewer than 250,000 customers fell for the scam and unwittingly supplied their bank details to criminals.

Criminals are realizing the potential of the internet as an ideal platform for fraud and theft and are actively recruiting the best computer talent to assist them in their various scams.

Law enforcement's reaction was less than satisfactory. The leader of the investigation still wasn't sure how to charge and then enforce the charge made against the fraudsters due to questions of jurisdiction.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Virtual company

Edward and Stuart were sophisticated international businessmen, or at least they thought so. They ran the international division of a rapidly growing telecommunications company that was always looking for money and acquisition candidates. So when they had a chance encounter with a banker who claimed to be a banker and venture capitalist from Japan they asked her some general questions about her firm's services. She referred them to the bank's web site and handed them her card. When she handed these gentleman her card, they recognized the bank's name immediately as a world-class bank based in Japan that had been involved in telecommunications throughout Asia.

The courtship of a business owner and a banker is always a tricky thing said Stuart; it like two porcupines trying to hug without getting hurt. So when she began asking for information so she should conduct her due diligence they were helpful and obliging. For that matter so was she. She came to their offices and viewed their facilities and spoke to most of their key people, major suppliers, attorneys, and accountants. In two months, she had amassed all of the information she needed to make her decision.

The bank and the company negotiated for several weeks thereafter on how the issues of additional financing were going to occur and how the company and the bank were going to work together to acquire some additional companies in Malaysia and Indonesia. Frustrated with the answers of the bank, the company went to speak directly to the acquisition candidates in Malaysia and Indonesia to resolve any potential difficulties in the acquisition phase or in the operational phases thereafter. Agreements were signed setting forth in detail the abilities and positions of both companies. These documents and the corresponding support material were forward to the banker in Japan so she could see with her own eyes the great deals

negotiated by Edward and Stuart. Within two weeks a competitor of Edward and Stuart's snatched up the two acquisition candidates on terms remarkably similar to those negotiated.

At this point Edward and Stuart smelled a rat and called their Japanese banker. She was ever so nice on the phone, but said that these things happen, and not to be put off, but rather to seek other companies out that might also be suitable. Edward and Stuart then called a US branch of the bank and asked about their banker. They said they had never heard of her, but would call Japan to see if they knew of her. Edward and Stuart's hearts sank when there received a call late that night from Japan. It appears that this woman had long been known in industrial espionage circles around the world, and used the position of a banker or of a telecommunication company executive to obtain information about other companies.

She worked for no particular firm, but sold her information to the highest bidders. She targeted the telecommunication industry, and could usually be found in or near any telecommunications conference. Stuart and Edward shook their heads: They had met her in the lounge of a hotel in Las Vegas while attending a conference on new 3G communications.

"The only thing we didn't give her was the key to the men's restroom, and only because she didn't ask for that!" said Edward when he learned the truth behind the lady banker from Japan. The bank they thought they recognized was a name very close to the real name of the bank. The virtual company had copied the real bank's web site with remarkable accuracy, changing only the contact information and a few of the addresses.

3. Executive Protection — Facing airline hijackers

Contributed by Shane Steinkamp, Steinkamp Systems (shane@thelacewithnoname.com).
Contributed articles do not necessarily reflect the viewpoint of the *Business Security e-Journal*.

We have been getting a lot of requests about what to do when faced with hijackers onboard an aircraft. In reality, there are many other threats that you are more likely to encounter in your everyday life that are more dangerous than air travel. Like many of you, we travel quite a bit on airlines both nationally and internationally. The likelihood of the aircraft being commandeered is usually at the bottom of our threat assessment list.

In the interest of discussion, however, there are a few things you can do to increase your security at airports and onboard commercial aircraft. The first thing, of course, is simple awareness of your surroundings. While in the airport or boarding the plane, observe your fellow passengers. If you see,

hear, or smell anything suspicious, you should immediately report your observations to the proper authority.

While you are much more likely to encounter an intoxicated or unruly person onboard a commercial airliner rather than a hijacker, your course of action is generally the same when dealing with either. Previous experience once taught us that cooperation with the hijackers was the best course of action for passengers, but those rules have changed now that the objectives of hijackers seem to have changed.

Before we discuss weapons, we need to discuss tactics. First and foremost, any hijacker – or unruly person – must be denied access to the cockpit (a risk which will diminish in the future when cockpits are better secured). Once a bad person is in the cockpit or at the controls, your tactical situation is extremely poor. If you are going to board a plane with other people known to you, you should discuss possible scenarios with them. You should seat women, children, or your client at the window, and you should sit at the aisle.

Since the World Trade Center crime, the only agency that has over-reacted has been the FAA. Airport security has been confiscating even innocuous things like nail files, but make no mistake: Weapons can still be brought on board an aircraft by persons with malicious intent. You must think ahead when boarding a plane in order to provide yourself with options. Not necessarily weapons mind you, but options. Perhaps a heavy leather belt with a heavy buckle can be used as a flail, a whip, or as a restraint device. Heavy boots or shoes may also be beneficial and provide options. Think about your choice of clothing, and always use the thickest and strongest bootlaces you can find. We carry *Tuff-Tie* cuffs (<http://www.tufftie.com/>) because handcuffs aren't allowed on commercial aircraft.

If you own it, always wear your body armor (vest) and be prepared to identify yourself to security when they demand to know why you are wearing one. If there is a person or persons with a firearm on board, you become the bullet sponge, something in every other confrontational situation we advise against. Unfortunately an aircraft is a fragile environment, and a bullet in the wrong place might bring a plane down, so you need to confront the person with the fire arm at close range and should that weapon discharge before you disarm the individual, it is best that the weapon discharge into your vest.

Going from bad to worse, a bomb should be given all due respect, but access to the cockpit must still be denied. We understand that bombs are an unknown element to many people, and dramatic Hollywood portrayals of

bombs being defused has added to their mystique. We encourage everyone in the trade to study the manufacture and construction of bombs and explosives to demystify them.

Usually dealing with a bomb is easy: Call the bomb squad. Unfortunately, you do not have that option in the air. You may be forced to deal with an armed explosive device, or, worse, one with a countdown timer. Many of these devices can be dealt with simply by removing the batteries or disconnecting the detonator. You should familiarize yourself with different types of devices so that you can recognize and handle them on an emergency basis if you have to do so. The simplest 'bomb' is a stick of dynamite with a detonator and a fuse. Once the fuse is lit, however, you still have options. You can remove the detonator from the stick, or cut the fuse. (Don't try to remove the fuse from the detonator, since it's crimped on and trying this can cause the detonator, and hence the dynamite, to explode.) Other devices are often simple, having a timer and/or switch, a battery or other power source, wires, a detonator, and the primary explosive. The green wire, red wire, blue wire question often portrayed in movies simply does not apply to these simple devices.

Let's take another simple bomb: A grenade. A grenade is a safe unit, even if the pin is pulled, so long as the lever has not been released. If you can get the grenade away from the individual, then just keep it in a safe place until the plane lands or unscrew the detonator from the grenade body. Grenades, and other 'simple' bombs should all be handled in the same way: Don't fool with them if you don't have to, and keep them safe.

If the pin is pulled and the lever released, you have seven seconds to unscrew the detonator from the grenade body. This is not always possible or advisable. What do you do with it then? You've got an object that is going to detonate in a very fragile environment with lots of people who have nowhere to run. You cannot stop this event, but you can control where it detonates. The 'best' scenario is to locate the grenade on the floor in the center aisle of the plane and lay on top of it – or, better, lay the individual to whom it belongs on top of it. Remember your vest? Well, it won't save your life, but it will save the lives of others. The floor of an airplane isn't very strong, and the blast will go through the floor and into the baggage area. This is better than the blast zone being inside the cabin - albeit not much better. Grenades and other small low brisance devices aren't usually very powerful, and can be contained in some way.

Complex bombs, bombs made from high brisance explosives, and large bombs are beyond the scope of this document, but learning their component parts and how they work will allow you to make choices in a difficult situation.

If you have really prepared ahead, you can make a 'bullet proof' briefcase or valise. When you retire your old vest in favor of a new one, cut it apart and cut the Kevlar panels to fit inside a pocket of your valise or glue it into the lid of your briefcase using a non-hardening glue such as rubber cement. (Hard glues, like resins, epoxy, cyanoacrolates (superglue), and other glues that dry hard will decrease the effectiveness of the Kevlar.) This case can even be modified to have side handles like a shield. (Some bags have such 'handles', but they are for holding an umbrella or a newspaper.) If this is handy, you can use it as a shield or on top of a soon-to-detonate device. (Unfortunately, experiments with 'bomb bags' that would contain the shrapnel have proven ineffective.)

If we go from worse to better, and the subject or subjects are armed with edged weapons, your tactical situation is much better. Keep remembering that your first tactical goal is denial of access to the cockpit, then work to restrain or eliminate the subjects. Good training is your first, last, and best tool in this situation, so make sure you have it.

When faced with weapons other than firearms or bombs, remember to look for things in your environment and access your tactical situation.

Fortunately, an airplane is full of useful tools. Remember the words in the 'emergency lecture': "In case of a water landing, your seat cushion can be used as a flotation device." Every seat cushion on every airplane is removable, and can be used not only as a flotation device, but also as a shield if necessary. They even have nifty straps that let you hold them like a shield. Carry on luggage with wheels often has telescoping handles that can be yanked out of the bag forcefully and used like a baton. (You may wish to purchase such a bag and modify it so that the handle pulls out readily.)

Magazines, books, laptop computers, and other items can be thrown as 'distractors.' Soda cans, and other beverage cans or bottles can be retrieved from the drink service cart or attendant area and thrown. Three or four men with good arms and fifty cans of soda can persuade even the most cheerful person that he is having a bad day. Seatback trays can be torn away from the seat back if necessary. Overhead compartment doors can be torn away, albeit with difficulty.

Our final recommendation is this: Every time you are going to board a plane, buy a lottery ticket. Why? Because you're far more likely to win several lotteries than you are to ever be hijacked.

4. Technical Issues — Fake financial documents

ICC's Commercial Crime Services announced the recent closure of an online banking fraud involving fake documents worth US \$3.9 billion.

CCS Commercial Crime Bureau (CCB), which carried out investigations that reported fraud feasons had published fake banking guarantees on many websites to lure potential victims to invest in projects and finance schemes.

The web addresses gave the impression that the scam sites were run by either Euroclear Bank, the international clearing system for the settlement of transactions in securities and Eurobonds, or Bloomberg, the information services provider. Examples of these domain names are <http://www.euroclear30.50megs.com/> and <http://www.bloomberg.50megs.com/> .

Advance fees of hundreds of thousands of dollars were paid for the issue of these fraudulent guarantees, and the websites were used to validate the documents. The amounts represented on the fraudulent sites ranged from 50 million to over 400 million dollars.

In addition to being used to procure advance fees these guarantees were to be used in bogus High Yield Investment Programs (HYIP) that promised high returns from low risk financial instrument trading.

The bank guarantees were confirmed to be fraudulent, and Euroclear Bank and Bloomberg were alerted to the intellectual property breaches. The big risk is that these frauds could rock the trust that the banking, finance, and insurance industries are built on.

This method of fraud has been run by many, on several occasions. The international Monetary Fund (IMF) and the US Securities Commission (SEC), the Federal Reserve Banks (FED) and Offices of the Comptroller of the Currency (OCC) have all published issued warnings.

A Certificate of Deposit (CD), is a receipt issued by a bank for the deposit of a sum of money. Forged CDs have been used as bait for high yield investment schemes by con artists. The following is a checklist to help identify whether or not Certificates of Deposit are genuine:

- High interest rate
Check that the interest rate is stated on the certificate itself and not just in the accompanying documentation. The rate of interest in genuine documents is usually around base rate. If higher rates are stated, check for further explanation of how the trading of the certificate will generate the higher yield.
- Uneven time period
Time periods should be stated in clear periods such as “one year”. The addition of an extra day, week or month is characteristic of many fictitious transactions.

Red flag phrases, including:

- “funds of non-criminal origin” ...
No bank would use this phrase because it could not validate such a statement.
- “the funds are blocked”
As far back as March 1995, the Comptroller of the Currency, Administrator of National Banks in the United States issued a warning on the use of this phrase. It is not known to exist in the legitimate banking community.
- ‘KTT’ payment mode
This phrase is favored by fraudsters. It refers to an encryption test of the Telex Machine Key Tested Telex or KTT, not a payment method.
- UCP 500
Fake documents often refer to erroneous international standards or rules. A common example is UCP 400 which has now been superseded by UCP 500.
- Mistakes in these documents are often intentional. Fraudsters may also drop in legitimate-sounding phrases to establish whether the targeted person knows what they’re talking about.” It is a way of assessing their mark for the fraud.

5. Real Stories from the Field — Pirates

Pirate attacks rose last year by 57% compared with 1999 figures and were nearly four and half times higher when compared with 1998.

In its annual Piracy and Armed Robbery Against Ships report for 2000, the IMB, a division of the Paris-based International Chamber of Commerce (ICC), reports a total of 469 attacks on ships either at sea, at anchor or in port.

The violence used in the attacks rose to new levels, with 72 seafarers killed and 99 injured in 2000, up from 3 killed and 24 injured the previous year. The number of hostages taken was halved to 202 seafarers. Ships were boarded in 307 instances and a total of eight ships were hijacked.

It is believed by professionals in the industry that large numbers of attacks remain unreported. The figures, compiled for January to December 2000, show an alarming rise in piracy and armed robbery in the seas off Indonesia, Bangladesh, the Malacca Straits, India, Ecuador, and the Red Sea.

Indonesia recorded the highest number of attacks, accounting for almost one quarter of the world total, with 119 incidents. 86 ships were boarded, two ships were hijacked, and attempted attacks were made on another 31 ships. It was also the location where the greatest violence was experienced, with many of the pirates armed with knives. The IMB says there are no signs that the number of attacks will drop unless Indonesia takes serious steps to address the problem.

The Malacca Straits witnessed a dramatic rise in attacks, up to 75 from 2 in 1999, despite the efforts of the Royal Malaysian Police to step up patrols in the area to tackle the problem. Its special task force captured two groups of pirates, but there are still known to be several other groups attacking and robbing ships as they transit this busy waterway where the threat of an ecological catastrophe also looms.

Bangladesh, with 55 attacks, is up from 25 attacks in 1999. The Bangladeshi authorities have since taken action of their own, which resulted in a drop in attacks during the latter part of the year. Other substantial rises were recorded in India (35, up from 14 in 1999), Ecuador (13, up from 2 in 1999), and 13 attempted boardings on ships in the southern part of the Red Sea, where previously there had been no pirate activity. One of the few areas to see a downturn in activity was the Singapore Straits (5 incidents, down from 14).

Attacks still occur in the Caribbean, especially along the coast of Nicaragua, where a majority of the ships that disappear are thought to have had the occupants robbed, killed, and the boat taken and re-flagged.

A proposal to limit the attractiveness of this type of piracy was floated by the International Maritime Bureau with a call to stamp the hulls of ships with

a permanent identity code, saying it would reduce crimes that involve the masking of ships' origins.

Fraudulent ship owners are using increasingly sophisticated techniques to produce forged identity papers for ships and their cargo. By fooling the port authorities, they can take a stolen or un-seaworthy ship into a port, load it with goods, and sail off. Once at sea, all it takes is a new flag, a quick repaint, and another set of false identity papers, and the phantom ship is nearly impossible to trace. Few ports check the authenticity of registration certificates with the issuing office.

While every ship's official IMO identification number figures on its identity documents, the number is rarely visible on the ship itself. It is proposed for the IMO number to be embossed on the hull of the ship so that pilots, port authorities and customs authorities can immediately distinguish the number of the vessel and check its identity. All ships around the world would then be visibly identifiable from the day they leave the shipyard through to when they are scrapped. This could prove to be an important crime prevention measure, especially against phantom-ship crimes, which rely on fake documents. Unlike current maritime documents, a number embossed on the hull of a ship is difficult to tamper with. If anyone interferes with it, it will be more apparent.

If adopted it will take at least five years to implement. Proponents believe the cost is far outweighed by the benefits to the shipping industry, the environment and to international trade if ships' identities can be properly regulated. It is also an invaluable aid to buyers of second hand vessels to easily verify the origins of the vessel.

6. Book and Product Reviews

ESSEX Victim Rescue Unit (VRU)

ESSEX PB&R \$375 (10 year service life)

1-618-659-9070 <http://www.smokehoods.com/>

(http://www.smokehoods.com/VRU_main.htm).

It has often been said that while a burglary can cause you harm a fire can put you out of business. Or kill you. Indeed, fire, along with automobile accidents, accidents, and medical emergencies, is one of the major preoccupations of protective work.

Since it is the smoke that is liable to kill you in a fire, not the fire itself, smoke masks or hoods are very important to have if you are caught in a fire, and we intend to work our way through several different available devices.

There are two ways to classify these devices. One is by whether they are *masks* which fit on your face, or *hoods* that go over your head. The second is whether they filter the air, or contain their own air supply. In looking at filtering systems to evaluate, we have chosen to look only at systems that include the ability to deal with carbon monoxide, as well as particulates and other gases common to modern building fires.

The *Victim Rescue Unit (VRU)* is a hood (as opposed to mask) escape unit that uses its own supply of oxygen, rather than filtering the ambient air. This means you don't need to worry about whether any particular gas or other contaminant can be filtered. The device was developed by Dupont a decade ago in response to several incidents, including an otherwise survivable (the aircraft was on the ground) aircraft fire that killed 55 people. The U.S. Air Force has over 100,000 of these devices, covering every passenger on its passenger-carrying aircraft. Other government agencies also use them, as do corporate customers, both on corporate aircraft and for protective work. As you might expect, you can't take the VRU on a commercial flight.

The VRU comes in a canvas carrying bag with shoulder strap, and is roughly 9 ½ inches by 8 ½ inches by 1 ¾ inches, and weighs about a pound and a half, which means it is small enough to toss into your carry-on or attaché case when traveling by car or company plane, or your flight bag if you are a pilot, or your desk drawer at work, or the bug-out bag you keep next to your bed at the hotel. The carrying case of the one we tested was a sort of international orange color, making it visible in the day, with a luminous strip visible in the dark. While it has belt loops, it is too big to normally carry on your belt.

The device is straightforward. You take the sealed pouch out of the canvas bag, tear open the pouch, remove the hood, turn on the oxygen flow by grabbing the bottle in one hand and the red ball on in the other hand and pulling it, and then put the unit over your head. The hood is made from multiple layers of Teflon® and Kapton® and goes over your entire head. It has an elastic silicon neck seal. There is no front or back to the VRU, eliminating concern as to whether it is on correctly.

An advantage of a non-demand oxygen supply (as opposed to a filtered system) is that the *VRU* can be used with an unconscious or otherwise disabled person, or a small child who might be able to use a mouthpiece but whose lungs are insufficiently developed to draw air through a filter, or an infant. In the case of a baby, you can activate the VRU and stick the baby into the hood, letting it fasten about the infant's waist.

Our testing was non-scientific, in that we were interested in discovering whether the *VRU* is practical to use in an emergency situation. We are confident that we would be able to make our way down a smoke-filled stairwell in a hotel or building fire wearing the *VRU*.

7. Free-Subscription/Unsubscription/Copyright 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), Mary Clark Fischer (MCFischer@lubrinco.com), and Richard Isaacs, CPP (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.

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 *The Business and Security e-Journal*, please send their e-mail address to 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 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. 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 *October 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.