



ÆGIS journal

Addressing threats that affect your bottom line

Volume 9 Number 10, October 2006

From the case files of

LUBRINCO

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

and

FE&E CLARITY FROM COMPLEXITY
Financial Examinations & Evaluations, Inc.

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

Asset location in fraud, theft, and divorce? Call us!

This month's features:

- **Special Announcement: Critical Information and IP Conference**
- 1. **Asset Location and Due Diligence — Cops moonlighting as investigators**
- 2. **OPSEC, Economic Espionage, and Competitive Intelligence — What is critical information?**
- 3. **Executive Protection — Options in collapsible impact weapons**
- 4. **Technical Issues — Déjà vu all over again: T-Mobile's Sharp Sidekick 3**
- 5. **Real Stories from the Field — How United Airlines Flight 93 changed aircraft security**
- 6. **Book and Product Reviews — Identity Crisis**
- 7. **Subscription/Unsubscription/Copyright Information**

ÆGIS will be holding its two day **Critical Information and IP Conference: Identification, Valuation, and Protection of Critical Information and Intellectual Property in Tempe, Arizona in October, 2007.**

1. Asset Location and Due Diligence — Cops moonlighting as investigators

One of our competitors was hired by an attorney who had a client that had suffered the theft from its computers of a list of all of their key employees. The list ended up in the hands of an executive recruiting firm. When cornered, the executive recruiting firm agreed to turn over the list, as well as to allow a computer expert to make an image of their disk and perform some other investigative work, tied to their network.

Our competitor hired a computer forensics expert with the required skills, who concurrently employed in a branch of federal law enforcement. The outside expert did excellent work, discovering that a number of other companies had also been compromised. The president of the client company therefore assembled the stolen information obtained from his competitors, and began the process of calling the CEOs of the other companies to turn over what he had, along with a detailed description of what had happened.

Some days later the attorney for the client called and wanted to know why the lawyers of several other high tech firms (who also had a list of their key employees purloined by the same executive recruiting firm) were calling.

Unbeknownst to the attorney or the investigator, the outside expert – investigator for hire by night; cop by day – had called the other firms whose list of key employees he had found on the network. When confronted with this, the outside expert claimed that, as a federal law enforcement officer he had a “duty to inform any victim of the theft.”

We do not know if this duty to disclose is, in fact, true. Or how this violation of attorney client privilege will weigh in when the case goes to court, which is where it is now heading.

The “expert person” violated attorney client privilege and alerted all of the client’s competitors to the theft of the employee directory. As a DOD contactor, the client may lose some business since the expert’s blabby description of events when calling competitors also violated no small number of trade secrets.

So, if you want to hire an investigator who may use a moonlighting sworn law enforcement office, be forewarned of possible consequences.

We feel great sympathy for the owner of the investigative firm since this event will probably cause them to shut their doors.

2. OPSEC, Economic Espionage, and Competitive Intelligence — What is critical information?

When we talk about preventing information loss, we usually talk about three areas: Identification, valuation, and protection of the information.

We can generally classify information into two categories, intellectual property and critical information.

Intellectual property

Intellectual property includes (in decreasing order of visibility) trademarks and service marks, copyrighted materials, patents, proprietary information, and trade secrets. We have observed that there are too many IP holders who have never performed an inclusive audit of their IP, nor have any listing of their IP inventory, its disposition, nor even the ability to find out whether if there have been lost.

There are also significant issues surrounding valuation of intellectual property (such as IP developed in-house, for example, rather than being acquired outside, has no book value), with the actual valuation of IP being the elephant in the boardroom.

There is little mystery surrounding protection of trademarks and service marks, copyrighted materials, and patents from deliberate and unintentional violation. There is a lot of mystery surrounding the protection of trade secrets and proprietary information from competitive intelligence, economic espionage, and theft.

Critical information

The second is critical information. What do we mean by critical information? We mean information that, if known, would give an advantage to competitors and adversaries. Be aware that in the world of commerce we tend to think of “competitors” and “adversaries” as being synonymous. They are not. Those in the same business as you are competitors. People or groups who try to kidnap or kill your management and staff, blow up your facilities, or rob you are adversaries. A company may have no competitors, yet still have adversaries.

By this definition proprietary information and trade secrets might fall into either category. And, in fact, while protection of public forms of intellectual property (trademarks and service marks, copyrighted materials, and patents) falls into the bailiwick of attorneys and accountants, proprietary information needs to be protected as if it fell into the more-amorphous category of critical information.

In order to identify critical information, we must understand the operational goals and objectives of management. We must then aid management in identifying information which an adversary must acquire to achieve their own goals and objectives, or to inhibit or stop management's attainment of management goals and objectives.

Above all, it is important to avoid the trap of looking at what is considered important to you: Information considered important to you should in theory already be protected from general threats and crimes of opportunity by attorneys, accountants, and security.

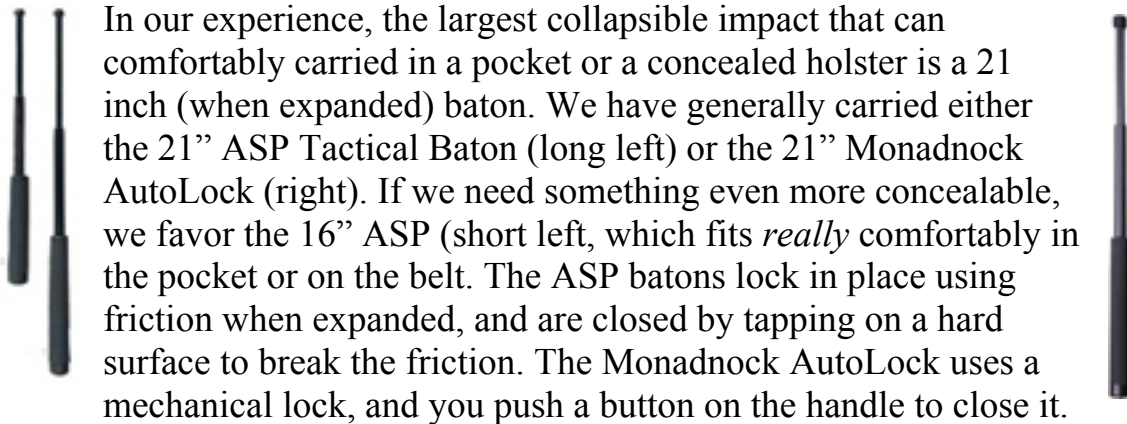
While some critical information (processes and trade secrets) is fairly concrete, in many cases it is not. Thus, for example, the written formulation of a product may be something that you protect assiduously because it is important to you. But if you do not shield your loading docks to prevent people from looking at the raw materials you are buying – these are likely to be roughly equivalent to the proportions of your formulation – keeping the proprietary formula under lock and key may not be entirely fruitful.

While determining what constitutes critical information is a management function, it is not a function that has been generally addressed. By the same token, the practical skill set of protecting critical information is not taught in law, business, accounting, or security courses. This skill sets fall into the area of counter-intelligence.


3. Executive Protection — Options in collapsible impact weapons

In the field of executive protection we occasionally have to use weapons. In most high-threat circumstances not involving war and civil unrest, we prefer not to allow agents to carry guns. We take this stance for two reasons. The least important is that there are often statutory issues involved in the carrying of guns which prevent us from being able to do so legally. More important, however, is the fact that carrying a gun might impel a protective agent to feel brave or aggressive, resulting in his or her wanting to confront a problem, rather than avoiding it.

That said, it is still often of benefit to have less-than-lethal weapons at hand. One is the collapsible impact weapon. Collapsible batons have two tapered metal shafts that fit inside a handle. They extend out, so you have the choice of a full baton for defensive use, or a small device that can be conveniently carried on the belt or in the pocket. Batons have the virtue of allowing you to break glass without getting cut, as well as being used as an emergency safety tool for defense.



In our experience, the largest collapsible impact that can comfortably be carried in a pocket or a concealed holster is a 21 inch (when expanded) baton. We have generally carried either the 21" ASP Tactical Baton (long left) or the 21" Monadnock AutoLock (right). If we need something even more concealable, we favor the 16" ASP (short left, which fits *really* comfortably in the pocket or on the belt. The ASP batons lock in place using friction when expanded, and are closed by tapping on a hard surface to break the friction. The Monadnock AutoLock uses a mechanical lock, and you push a button on the handle to close it.



A relatively recent choice (though it looks suspiciously like the previously-issued Winchester baton) is the *Rapid Containment Baton* (left) from Peacekeeper Products (<http://peacekeeperproducts.com/>). The folks at Peacekeeper Products have been known over the decades for their striking dummies, rather than for batons. Like the ASP, the RCB is a friction lock design. It is 25 grams lighter than the 21 inch Monadnock AutoLock with Hindi Cap, but heavier than the ASP.

The RCB has two features we find attractive. The most important is that the center of gravity in the expanded state is in the shafts – the part that will be striking large muscle mass – not in the handle. We believe this increases energy transfer, which would make this baton somewhat more effective than the others.

Interestingly, while all three batons are roughly equivalent in weight, the thinnest shaft on the milled (rather than extruded) RCB is thicker than the thickest blade on the extruded ASP or Monadnock. While this makes the baton fractionally slower, we are striking people in large muscle groups, not fencing. The balance is good, and we don't feel that even a small officer or agent would over-swing.

The second thing we like is that the handle of the RCB is thicker than that of the ASP or the Monadnock, and felt more comfortable in our hands.

However, it was not thick enough to cause problems for those with small hands. This is clearly a matter of personal choice.

While we are delighted to say that we did not have an opportunity to use the RCB to control a subject (our goal is to avoid problems, not deal with them). However, we did use it on training bags, and on ourselves. It is our impression, unverified by scientific measurement, that there was indeed more energy transfer from the RCB, which we attribute to the somewhat larger striking surface of the larger-diameter shafts, combined with the location of the center of gravity. We suspect – but again have no field experience to back it up – that the thicker shafts may be less likely to cause physical damage than the thinner shafts that we normally use.

We have not yet gone through the training course associated with the RCB (we are instructors for other batons, but not yet this one), but there is training associated with the device, and we will take this training because we will not carry this – or any other – emergency safety tool without being certified in its use.

We like this baton, and would very much like to see a version that is two inches shorter. While the 21 inch version fit in some pockets, a shorter version would be way more appropriate for close protection use.

In any case, if you are looking for a collapsible baton, we would recommend you consider the RCB as one of your choices.

4. Technical Issues — Déjà vu all over again: T-Mobile's Sharp Sidekick 3

As the mobile phone market has become saturated, with voice calls becoming a commodity item, service providers not unreasonably looked to find new sources of revenue, while phone manufacturers have looked to provide terminals for the new services.

As these services have become more popular and more profitable, there has been an increase in emphasis on network (or other) appliance function and a de-emphasis in voice communications. In some cases the emphasis has been on using the terminal as a PDA. In other cases it has been on using the device for getting and receiving e-mail. Some have aimed at providing entertainment centers, complete with MP3 players, FM radios, cameras, and video recording and playing. The T-Mobile Sidekick 3 is aimed at people who send a lot of text messages. It also includes a camera and an MP3 player, as well as a speakerphone and the ability to use a Bluetooth headset. It has a SAR of 0.5, which is good.



We send a lot of messages, so at first glance this looked like an attractive choice. And, if we were thirteen years olds who never traveled abroad, and never needed to make a phone call, this device would indeed be high on our list.

Unfortunately, we are long past our teenage years, and do travel. What we were hoping for was a phone that additionally had the ability to send messages with greater ease. What we found in the Sidekick 3 is a device whose underlying GSM technology is half a decade out of date.

If you are a grownup that travels, and are considering the Sidekick 3, be aware that, as of the last time we checked:

You will have **NO** GSM coverage in Andorra, Angola, Azerbaijan, Bangladesh, Bhutan, Bosnia and Herzegovina, Botswana, Brunei Darussalam, Burkina Faso, Burundi, Cambodia, Cameroon, Cape Verde, Central African Republic, Chad, China, Comoros, Congo, Cook Islands, Côte d'Ivoire, Croatia, Cuba, Djibouti, East Timor, Egypt, Equatorial Guinea, Eritrea, Ethiopia, Faroe Islands, Fiji, French Polynesia, Antigua and Barbuda, Gabon, Gambia, Ghana, Gibraltar, Greenland, Guernsey, Guinea, Guinea Bissau, Guyana, Iran, Iraq, Isle of Man, Jordan, Kazakhstan, Kenya, Kiribati, Korea (North), Kyrgyzstan, Lebanon, Lesotho, Liberia, Libya, Macedonia, Madagascar, Malawi, Maldives, Mali, Mauritania, Mauritius, Micronesia, Moldova, Monaco, Mongolia, Morocco, Myanmar, Nepal, New Caledonia, New Zealand, Niger, Oman, Pakistan, Palestinian Territory, Papua New Guinea, São Tomé and Príncipe, Saudi Arabia, Senegal, Seychelles, Sierra Leone, Swaziland, Togo, Tonga, Tunisia, Turkmenistan, United Arab Emirates, Vanuatu, Venezuela, Vietnam, Yemen, Zambia, and Zimbabwe (six of which countries members of our team have visited this year).

You will have **INCOMPLETE** GSM coverage in Afghanistan, Albania, Algeria, Argentina, Armenia, Aruba, Australia, Austria, Bahrain, Barbados, Belarus, Belgium, Benin, Brazil, British Virgin Islands, Bulgaria, Cayman Islands, Congo (Democratic Republic of the), Cyprus, Czech Republic, Denmark, Dominica, El Salvador, Estonia, Finland, France, French West Indies, Georgia, Germany, Greece, Grenada, Hong Kong (China), Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Jamaica, Jersey, Kuwait, Laos, Latvia, Liechtenstein, Lithuania, Luxembourg, Macau (China), Malaysia, Malta, Mozambique, Namibia, Netherlands, Netherlands Antilles, Nigeria, Norway, Philippines, Poland, Portugal, Qatar, La Reunion, Romania, Russia, Rwanda, Serbia and Montenegro, Singapore, Slovakia, Slovenia, Somalia, South Africa, Spain, Sri Lanka, St Lucia, St Vincent and the Grenadines, Sudan, Suriname, Sweden, Switzerland, Syria, Taiwan,

Tajikistan, Tanzania, Thailand, Turkey, Uganda, Ukraine, United Kingdom, and Uzbekistan (13 of which countries members of our team have visited this year).

On the bright side, you will at least have full GSM coverage in Anguilla, Bahamas, Belize, Bermuda, Bolivia, Canada, Chile, Colombia, Costa Rica, Dominican Republic, Ecuador, Guam, Guatemala, Honduras, Mexico, Montserrat, Nicaragua, Panama, Paraguay, Peru, St Kitts and Nevis, Trinidad and Tobago, Turks and Caicos Islands, United States, and Uruguay (7 of which countries members of our team have visited this year).

It is our understanding that moving from the obsolete tri-band chipset used to a current-technology quad-band chipset could have increased the manufacturing costs of this \$350 device by up to a whole dollar!

Nonetheless:

- Danger (<http://www.danger.com/>) should be ashamed of designing a telephone using technology that has been obsolete for half a decade.
- Sharp (<http://www.sharp-world.com/>) should be ashamed of manufacturing a telephone using technology that has been obsolete for half a decade.
- T-Mobile (<http://www.t-mobile.com/>) should be ashamed of accepting a design based on technology that has been obsolete for half a decade.
- Reviewers should be ashamed of not mentioning that the design of this telephone uses technology that has been obsolete for half a decade.
- Purchasers – even unsophisticated children – should be ashamed to be seen carrying a terminal that uses technology that has been obsolete for half a decade.

5. Real Stories from the Field — How United Airlines Flight 93 changed aircraft security

When United Airlines flight 93 crashed in Pennsylvania as passengers fought the hijackers that had taken over the craft, the paradigm for aircraft security changed. The previous paradigm was that individuals should not take responsibility for their own safety: This was the job of professionals representing the state. Because of this, self-defense was frowned upon, and often punished, independent of the circumstances. We suspect it is the reason that those on board have not been given any official posthumous honor by the government.

Did this leave-it-to-the-pros paradigm improve safety? This author certainly remembers people getting on international flights in the dim past with loaded guns in their pockets, and having some feeling that the flight was safer because of this. And recently, a friend of ours was summoned to the flight deck, where he was told by the pilot that his bag was being pulled so that he could take out and wear his weapon. He obviously didn't have to do this: He could always take another flight. The pilot apparently felt that having an armed man on the plane increased safety, so our friend complied.

Now the paradigm has changed. Passengers know that if there is a problem onboard it is their responsibility to deal with the issue. What does that mean in practical terms? What it means is that all the meaningless security theatre surrounding aircraft security serves no valid security function.

Security theatre is important from a political point of view. While it serves no valid security function – indeed is often counter-productive – it allows politicians to claim that they are taking action, and possibly even comforts some of the more gullible passengers. You can, after all, fool some of the people all of the time...

From the perspective of aircraft safety, what should now be done is to get rid of unproductive gate checks and identification requirements, as well as the myriad other silly security-theatre regulations. If you have a valid ticket, you should be able to get on board. And we should allow all sworn officers – of which there are about 310,000 in the U.S. – to carry their weapons onboard if they feel so inclined.

These two actions alone would free up millions of dollars and markedly increase actual aircraft security.

6. Book and Product Reviews

Identity Crisis: How Identification Is Overused and Misunderstood

Jim Harper

Cato Institute ISBN: 1-930865-85-6 288 pages \$13.95

<http://www.nbnbooks.com/> 1-301-459-3366

We often quote Bruce Schneier's dicta on judging policy and practice:

1. What problem is the policy or measure trying to solve?
2. How can it fail in practice?
3. Given the failure modes, how well does it solve the problem?
4. What are the costs, both financial and social, associated with it, and flowing from its unintended consequences?

5. Given the effectiveness and costs, is the policy or measure worth it?

This approach seems critical to us in judging recent demands for increased use of identification. Thus, for example, one might look at the demands for identification before getting onto an airplane. Imagine that this policy had been in full force on 9/11. Would this have made a difference? No, because all the bad guys had perfectly legitimate ID.

At present there seem to be three forces behind the new identification policies.

The first is the political need to give the impression of doing something. Because of this, security theatre is often thought to be adequate because the question being asked is not related to security. Rather, it is related to the political need to be seen to be taking action, with intrusive – albeit fruitless – measures being most visible and thus most successful.

This carries over to the civil sector. In one recent case we went into a building where they had “high security” processes in place, where you had to leave ID with the security desk, visit verification calls were made to the person being visited, and your possessions were X-rayed. Our group’s possessions included knives, guns, personal defense sprays, batons, and a smoke mask containing a canister of some unknown gas (oxygen, its user might hope). All passed through even though all the weapons were clearly visible and elicited some comment, because the building knew that it faced no likely threat, but got an insurance break by having an X-ray machine. The what-problem-are-we-trying-to-solve question building management dealt with was lowering insurance premiums.

Another part, of course, is the assumption that bad guys are drooling idiots who will make no attempt to examine the system they are trying to defeat. Thus, many policies assume that a terrorist will fill in *occupation* as “terrorist” on forms handed them. This, of course, influences enforcement. In one recent case, a group (the leader of which had a diplomatic passport) was held up in INS for several hours because his four year old daughter’s name was on the terrorist watch list.

The most critical part of the rationale for these increased demands stem largely from a lack of understanding of identity, and the distinctions between identity and authentication and authorization. It is to address this issue that we strongly recommend Jim Harper’s book *Identity Crisis*. It is our hope – as it is his – that if more people understood the concept of identity that its use might be more sensible.

It is not our intention to summarize how *Identity Crisis* addresses the broad area of identity: The book is a quick read, and you should read the whole thing, not a quick précis by us. The important thing to know is that there is strong demand for government increases in demands for changes in identification use, including looking toward a national ID card. This book gives enough information for a reader to understand why a national ID card serves no valid security purpose, though it may have tax and commercial implications of benefit to the issuing jurisdiction.

Because increased identification demands may have a drastically effect on civil liberties and privacy, and because changes in social policy and convention are difficult – almost impossible – to undo, this book is important, and should be read by everyone concerned with social policy.

The information in *Identity Crisis* will help you can ask and answer the questions that should and must be asked of these security policies and measures.

7. Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2006 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@feeinc.com).

LUBRINCO provides services in three high-threat areas, too specialized to be dealt-with in-house, that can adversely affect domestic and international bottom lines.

- **Corporate counterintelligence.**
 1. American businesses lose \$300 billion annually to competitive intelligence, economic espionage, and information theft.
 2. Sarbanes-Oxley requires internal controls tracking the costs, and impact on valuation, of competitive intelligence, economic espionage, and information theft.
 - LUBRINCO provides private sector access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information from competitive intelligence, economic espionage, and information theft.
- **International asset location and due diligence.**
 - Location of concealed assets in fraud, theft, and divorce.

- Due diligence to prevent fraud and loss in China, Central and Eastern Europe, Central Asia, the offshore financial centers, Latin America, and the Caribbean.
- Financial fraud and anti-money laundering program development and training for compliance with the US *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 **LUBRINCO** and its services, or for the archive of all past issues of **ÆGIS** in PDF format, please go to <http://www.lubrinco.com/>.

Subscription to **ÆGIS** is available for \$15 per year in North America and \$20 per year outside of North America.

To sign up for a **complimentary subscription** to **ÆGIS** or the **ÆGIS** PDF notification list, go to <http://lb.bcentral.com/ex/manage/subscriberprefs?customerid=7768> or send an email to aegis@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 aegis@lubrinco.com.

If you know of anyone else who should be receiving **ÆGIS**, please send their e-mail address to aegis@lubrinco.com.

If there is a topic that you would like to know more about, send it to aegis@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**, send it as an attachment to an e-mail to aegis@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** constitutes a license to **LUBRINCO**, 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**, you may do so freely as long as appropriate source, copyright, accreditation, and link to the **LUBRINCO** Web site is included. This should be in the form

Article Title, from the October 2006 **ÆGIS** (© 2006 **LUBRINCO** & FEE), to be found at <http://www.lubrinco.com/>.

ÆGIS 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** 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**.

Please be safe, and be smart.