



ÆGIS journal

Addressing threats that affect your bottom line

Volume 10 Number 7, July 2007

From the case files of

LUBRINCO

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

1-212-695-1759

and

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

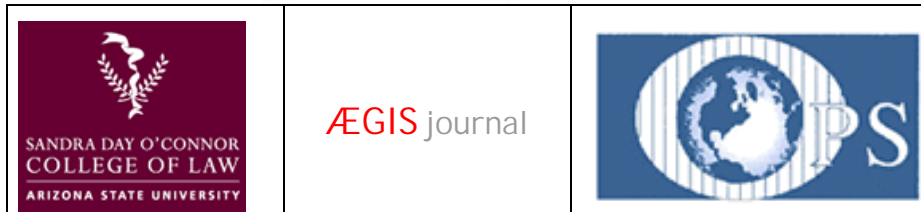
<http://www.feeinc.com/>

1-480-838-1728

Due diligence outside North America and Western Europe? Call us!

This month's features:

- **Special Announcement: IP and Critical Information Conference**
- 1. **Asset Location and Due Diligence — Electronic voting machines redux**
- 2. **OPSEC, Economic Espionage, and Competitive Intelligence — Where are the lawsuits?**
- 3. **Executive Protection — What level vest do you need?**
- 4. **Technical Issues — Satcom on the train**
- 5. **Real Stories from the Field — Preventing theft from checked baggage**
- 6. **Book and Product Reviews — SW991 and Mission MPF1-Ti redux**
- 7. **Subscription/Unsubscription/Copyright Information**



AEGIS journal, in conjunction with
The Center for the Study of Law, Science, and Technology,
Sandra Day O'Connor College of Law at Arizona State University
and
The OPSEC Professionals Society
will be hosting its two-day **IP and Critical Information Conference:**
Identification, Valuation, and Protection of Intellectual Property and Critical Information
For Directors, Finance Officers, and Counsel
At Arizona State University in Tempe, Arizona, **2-3 October 2007**
For information, contact us at conference@aegisjournal.com

1. Asset Location and Due Diligence — Electronic voting machines redux

It is important to make every effort to assure that the electoral process is above suspicion, and try to at least try to reach the 1 to 1.5 percent error figure believed to be inherent in even the best voting system. Without moving in that direction people will lose confidence in the system. Losing confidence in the system could be a precursor to failure of the system.

In looking at voting machines in the January 2007 issue of *ÆGIS*, we came to the inescapable conclusion that error rates with punch cards, lever machines, and DRE (direct recording electronic) devices are so significantly higher than paper ballots that their use should be rejected out of hand.

At that time we felt that the best choice would be tallying well designed paper ballots using optical scanners.

This conclusion was based on two assumptions that appeared to be reasonable, yet have turned out not always to be true. That being the case, we felt that the integrity of the electoral process is so important that this merited another examination.

The first assumption was that optical scanners were simple, and could reliably validate ballots, spitting back bad ballots uniformly across machines, thus allowing the bad ballots to be replaced if needed. It appears that in practice this is not always true. In the Florida presidential election, for example, the machines tended to work properly in white precincts, so that relatively few spoiled ballots that went uncounted. In non-white precincts, however, this feature did not work quite so well, so that many spoiled votes ended up going uncounted. This is bad.

The second assumption was that the tracking of the machine-read votes would be more reliable than other computerized or mechanical systems. While optical scans of paper ballots are far better than anything other than hand-counted ballots, scanners are still computers. Even for something as simple as counting ballots, computerized optical scanners, like other computers, are susceptible to error and tampering. This, too, is bad.

It is important to remember that even if the scan is accurate, and even if there is no voting fraud, bad ballot design can cause serious problems. It is estimated that faulty equipment and confusing ballots cost us 1.5 million to 2 million lost votes.

There are two obvious ways to deal with the problems inherent in using optical scanners to tally paper ballots. The first way is precinct-level hand counting. While there are more precincts in New York or California than in rural areas where hand counting is more prevalent, there are also more hands available to do the work. The advantages of hand counting are:

- (1) Counting of ballots can be done publicly, observed and recorded by the press and everyday citizens who are registered voters in the precinct where the counting takes place.
- (2) Although paper ballots, as with computers, lend themselves to fraud and tampering, security safeguards are much more easily put in place to protect against tampering.
- (3) The cost of hand-counted paper ballots is far less than buying machines.

While hand counting is slower than machine counting, if it prevents recounts it can provide a good alternative to optical scanning.

The second way of dealing with the weaknesses of optical scanners is to recognize the potential problems in their use, and implement measures to overcome these potential problems. In both hand counting and optical scanning you will get better results with well-designed ballots than with confusing, poorly designed ballots.

How do we try to overcome these potential problems? First, ballots should be designed by competent designers, rather than ward heelers, so that what is read reflects the intent of the voter.

Second, optical scanners should be chosen by a competent technician with the goal of picking one that will work, rather than one accompanied by large political contributions.

Third, we need to implement procedures to deal with less-than-perfect marking. As an example, suppose you make a mark, change your mind, put a big X through the bad mark, and then mark the candidate you really want, drawing an arrow to it. A dumb machine will bounce this as a bad vote, while a smarter human will immediately interpret the intent of the voter. So, ALL questionable votes need to be examined by a person. Will there still be bad ballots with lost votes? Sure, even with well designed ballots there will be spoiled votes, but many fewer of them.

Fourth, we need to deal with the reality that the machines can go down. In this case the ballot can simply be accepted for subsequent counting. After all, it is the ballot which is the vote, not the calculated total by the machine.

Finally we need to deal with the problem of machine error and tampering. This can be dealt with by random audit. We are assured that a statistician can tell us how this auditing needs to be structured in order to detect and obviate error and tampering.

Other issues

Besides voting machine issues, here are three other sources of lost votes that must also be addressed. The least significant of these (though we have no clue as to the scale of this problem), are losses associated with handling of absentee ballots.

More significant are losses associated with polling place operations. We have seen cases in which someone can't find a key to open the polling place, or unlock a piece of equipment. As well as cases in which voting has been delayed by hours in precincts when machines went down, or provisional ballots were not available. And cases in which already registered voters' names were missing from the rolls. Whether deliberate or accidental, it is estimated that at least a million votes are lost due to polling place operations.

The most significant problem is the registration process. It is estimated that between 1.5 million and 3 million votes are lost because of registration issues. In some cases this is because of unintentional error, and in other

cases it is deliberate. We know one voting activist in New York State who was threatened with arrest during a registration drive. Fortunately, she was accompanied by an attorney and a journalist, thus easing the problem (and making the front page of the local paper, which hopefully helped further diminish the problem). While voter intimidation, exclusion, and fraud might have been acceptable in the past, they shouldn't be acceptable today.

How meaningful are these problems in real-world terms? Well, in the 2004 presidential election 121,480,019 votes were collectively registered as having been cast for Mr. Bush, Mr. Kerry, and Mr. Nader. With 62,040,606 votes, Mr. Bush had a lead of 3,012,497 over Mr. Kerry's 59,028,109 votes.

Imagine that in this election there were no registration, polling place, absentee ballot, or voting fraud losses. Instead, we simply had to take cognizance of the best-case system error of 1.5 percent in an entirely clean election. To have won the popular vote in the last presidential election on the basis of actual votes cast (rather than system error), one would have had to have more than half the votes plus 1.5 percent. Put another way, to win the 2004 presidential popular vote by actual rather, rather than system error, you would need to have more than 62,350,388 votes. Which means that with 62,040,606 votes, Mr. Bush's margin fell within the 1.5 percent system error. If we throw in the more realistic 6 million lost votes, it is impossible to say which candidate received more cast votes.

Do we think a lot of voting fraud is taking place? Well we spend much of our lives dealing with fraudsters in the world of business. When you consider that the line between politics and business has blurred to the point of invisibility, we would have to be blind, deaf, and dumb – combined with just having fallen off the turnip truck – to assume that the world of politics, money, and power has less fraud than the world of money and power. Since votes these days tend to be so close, a little tampering goes a long way toward fixing an election.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Where are the lawsuits?

The other day someone asked us where the lawsuits were over loss of intellectual property. After all, we (among others) have been saying that at \$300 billion a year, the preventable loss of intellectual property and critical information to competitive intelligence, economic espionage, theft, and inappropriate disclosure would soon come with a costly penalty attached.

As it happens, there have been a number of such lawsuits, but in each case they have been settled long before reaching court. This is no surprise: If the company went to court over preventable losses for which they did not have required internal controls, it would have been even more expensive. Plus, the likelihood is that had any of these cases actually gone to court it would have forced the involvement of the SEC, which would have been more costly still. This is because the SEC allows companies to determine for themselves what constitutes being material. But if they decide wrongly, as shown by shareholder suits, the SEC is likely to appear on the scene doing its best imitation of a dropping ton of bricks.

How expensive was the experience for the companies involved in these lawsuits? Unfortunately, settlements tend to be confidential, so we don't really know. But all indications are that the settlements cost a great deal more than it would have cost to implement a best practices OPSEC program, which would have prevented the lawsuits from being filed in the first place. In fact, we would guess that the cost of litigation was more than it would have cost to implement an OPSEC program!

And this doesn't include the losses themselves! Again, the best estimates are that the average cost of an incident in a manufacturing environment is \$50 million, and \$500,000 in a non-manufacturing environment, with a second and third incident commonly being discovered. While corporate counsel may assure you that losing \$100 million is not material, your CFO, who understands the importance of money and who has to put his signature on your financials, should tell you otherwise. In Jeremy Hope's *Reinventing the CFO* (which we will discuss in a future issue), American Express CFO Gary Crittenden discusses measures which saved \$100 million a year. If \$100 million matters to American Express, it probably matters to you.

And don't think that the lawsuits are going to go away. It is the projection from our insiders in the activist shareholder arena that loss of IPCI is going to be a major issue in shareholder suits, and management shakeups. One is currently underway wherein the shareholders are attempting to reverse management's bonuses of the previous two years and terminate management for cause. The activists are making an aggressive claim that, if IPCI lost were reflected in the balance sheets, the write down would have wiped out the profits on which the bonuses were paid.

In the best of all possible worlds CFOs would insist that OPSEC programs be put into place, but many are still unfamiliar with the problem, even when it is happening to their company. We like to think that as the lawsuit

bandwagon picks up speed and volume this will change, with CFOs finally starting to implement internal controls to eliminate these needless losses.

3. Executive Protection — What level vest do you need?

When looking at ballistic vests, there are more possibilities than may seem immediately obvious to those who don't wear them.

As we discussed in the May issue of *ÆGIS*, you start with the question of what level vest to get. The choices –threat levels – are described in <http://www.nlectc.org/pdffiles/0101.04RevA.pdf>. These are:

Type I (22 LR; 380 ACP)

This armor protects against .22 caliber Long Rifle Lead Round Nose (LR LRN) bullets, with nominal masses of 2.6 g (40 gr) impacting at a minimum velocity of 320 m/s (1050 ft/s) or less, and 380 ACP Full Metal Jacketed Round Nose (FMJ RN) bullets, with nominal masses of 6.2 g (95 gr) impacting at a minimum velocity of 312 m/s (1025 ft/s) or less.

Type IIA (9 mm; 40 S&W)

This armor protects against 9 mm Full Metal Jacketed Round Nose (FMJ RN) bullets, with nominal masses of 8.0 g (124 gr) impacting at a minimum velocity of 332 m/s (1090 ft/s) or less, and 40 S&W caliber Full Metal Jacketed (FMJ) bullets, with nominal masses of 11.7 g (180 gr) impacting at a minimum velocity of 312 m/s (1025 ft/s) or less. It also provides protection against the threats mentioned in section 2.1.

Type II (9 mm; 357 Magnum)

This armor protects against 9 mm Full Metal Jacketed Round Nose (FMJ RN) bullets, with nominal masses of 8.0 g (124 gr) impacting at a minimum velocity of 358 m/s (1175 ft/s) or less, and 357 Magnum Jacketed Soft Point (JSP) bullets, with nominal masses of 10.2 g (158 gr) impacting at a minimum velocity of 427 m/s (1400 ft/s) or less. It also provides protection against the threats mentioned in sections 2.1 and 2.2.

Type IIIA (High Velocity 9 mm; 44 Magnum)

This armor protects against 9 mm Full Metal Jacketed Round Nose (FMJ RN) bullets, with nominal masses of 8.0 g (124 gr) impacting at a minimum velocity of 427 m/s (1400 ft/s) or less, and 44 Magnum Semi Jacketed Hollow Point (SJHP) bullets, with nominal masses of 15.6 g (240 gr) impacting at a minimum velocity of 427 m/s (1400 ft/s) or less. It also

provides protection against most handgun threats, as well as the threats mentioned in sections 2.1, 2.2, and 2.3.

Type III (Rifles)

This armor protects against 7.62 mm Full Metal Jacketed (FMJ) bullets (U.S. Military designation M80), with nominal masses of 9.6 g (148 gr) impacting at a minimum velocity of 838 m/s (2750 ft/s) or less. It also provides protection against the threats mentioned in sections 2.1, 2.2, 2.3, and 2.4.

Type IV (Armor Piercing Rifle)

This armor protects against .30 caliber armor piercing (AP) bullets (U.S. Military designation M2 AP), with nominal masses of 10.8 g (166 gr) impacting at a minimum velocity of 869 m/s (2850 ft/s) or less. It also provides at least single hit protection against the threats mentioned in sections 2.1, 2.2, 2.3, 2.4, and 2.5.

The level you choose is based on the threat you are likely to face. This means, for most of us who are likely to use a vest at all, a threat level that will protect us from our own gun if it is taken away from us, as well as the guns carried by police officers in our region. In this editor's city that would include roughly 36,000 gun-toting city police, plus assorted armed local, state, and federal law enforcement officers.

To add to the mixture, you can get inserts that offer higher levels of protection if you are shot and the bullet hits the insert. We have a number of these, the most protective of which is a Level IV strike plate. This plate is big (9 ¾" wide and 11" high and ¾" thick) and heavy (8.5 pounds) and expensive (it retails for as much as the vest). We have never actually worn it, and hope never to be going into any situation that would require its use.

We also have smaller and lighter drop-in standard size (5" by 8") inserts, which vary from the soft insert that came with our vest to a 0.2" thick Level IIIA metal insert weighing 1.38 pounds.

Why would you add one of these inserts? Well, if you are shot, the bullet can push the vest into your body, causing some level of trauma. If this happens, it would be nicer if it were pushing on a big plate rather than concentrating all the force on one tiny, bullet-sized area. In addition, woven ballistic vests aren't generally swell at stopping knives, so an insert can be desirable if you happened to be being stabbed in the chest where you are wearing the insert. Most important of all, if you are in an automobile accident – which is much

more likely than being shot – having the insert hit the steering wheel is better than your chest hitting the steering wheel, though that is less of an issue today, with most cars having air bags.

The bottom line is that we do not, in our normal daily lives, wear a ballistic vest: We face no more danger than anyone else, so it is not necessary. If we are in a situation where there is some higher probability of risk we will wear a vest, but will only use the soft insert. If we are doing something where we envision a higher probability of being actually shot at we will use one of the more visible inserts. While we do not imagine ever needing the level IV plate, we haven't thrown it out.

4. Technical Issues — Satcom on the train

For us, communications is a constant preoccupation. When we travel we tend to have local-country and U.S. mobile phones with us, as well as variety of satellite phones, including both laptop-sized Inmarsat phones (we have, by the bye, an extra O'Gara Compact M device for sale. It uses full M coverage, not spot-M coverage. We would be delighted to let someone have it at a bargain price...), as well as handheld devices (we try for one per person) including Iridium, Globalstar or Thuraya handsets, depending on where we are going. We also, of course, have personal locator beacons.

Even with all this, communications can be iffy, depending on where you are. In the Grand Canyon, for example, we are given to understand that you may have a few hours of Globalstar coverage each day, depending on the whim of the moving satellites, with no other options available if you feel chatty. At the Poles, Iridium is your *only* choice. And, of course, you need to be able to see a satellite, so satcom doesn't help you indoors unless there is a satellite within view out the window.

This led us to wonder whether we could acquire and maintain a satellite connection from a train. So, on a recent transcontinental train trip we brought an Inmarsat device into the observation car to give it a try. We figured this would be a best-case opportunity, as the train tends to run in a pretty straight line across the prairie. If we could acquire the satellite we should have a good shot at maintaining it.

In fact, this was the case. We easily picked up the Atlantic Ocean Region-West satellite as we sped across the Great Plains. We maintained a strong signal, and were able to continue talking even when cell phone coverage disappeared. We could not have done this with our various collections of handheld satellite phones.

On the other hand, we have been in situations where we did not have a clear shot at an Inmarsat satellite, but did have line of site to other satellites, so you pay your money, take your choice, and hope you know where your satellites are located!

5. Real Stories from the Field — Preventing theft from checked baggage

It is widely rumored that theft in checked baggage has skyrocketed now that air travelers can no longer lock bags. While our request to airlines for statistics on this have gone unanswered, we certainly know that on our last trip we were robbed of two knives, a small impact weapon, and a flashlight. While all of these are more or less replaceable (the flashlight was given to us at the SureFire 2006 Anti-Terrorism Symposium, and was so engraved), it is still over \$600 that we have had to spend out of pocket, with no clear knowledge of when – or if – the cost of replacement will be taken care of by either TSA or the airline.

After the theft, the question we had to ask ourselves was how we could best avoid being robbed in the future. After much back and forth with TSA and law enforcement, the answer was simple: We needed to lock our bags.

How could we do this? Carry a firearm. Bags containing firearms must, according to TSA, be locked. Indeed, if you take a look at the instructions at http://www.tsa.gov/travelers/airtravel/assistant/editorial_1666.shtm, you will read that:

- The firearm must be in a hard-sided container.
- The container must be locked.

In their correspondence with us, TSA said that “if your suitcase also serves as your hard-sided, locked gun case, it may not be left unlocked.” Both operational editors of *ÆGIS* travel with hard-sided aluminum Zero Halliburton cases (<http://www.zerohalliburton.com/> - see the June 2006 issue of *ÆGIS*). This means that all we will need to do is to toss in a firearm, declare and tag it at the airport, lock it (possibly after TSA inspects the bag), and be on our way.

There is, of course, the minor issue that many states will not allow us to possess a firearm. Our first thought was to get a *starter pistol*. A starter pistol has the advantage of being considered a firearm, thus requiring being declared and checked in a locked bag. Plus, not being an actual weapon, we thought would generally be legal to possess. As it turns out, it is flat-out illegal to own a starter pistol in this editor’s hometown of New York City.

