



ÆGIS journal

Addressing threats that affect your bottom line

Volume 10 Number 9, September 2007

From the case files of

LUBRINCO

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

1-212-695-1759

and



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

1-480-838-1728

Business in Bogotá or other high-threat areas? Call us!

This month's features:

- **Special Announcement: IP and Critical Information Conference**
- 1. **Asset Location and Due Diligence — Reading the fine print**
- 2. **OPSEC, Economic Espionage, and Competitive Intelligence — Which weighs more: A pound of feathers or a pound of gold?**
- 3. **Executive Protection — When the melting pot stops boiling**
- 4. **Technical Issues — Laptop protection**
- 5. **Real Stories from the Field — Spies for sport**
- 6. **Book and Product Reviews — FileCrypt Desktop 2.0**
- 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 — Backing up data

Recently a friend who has a one-man business realized that his computer's hard drive was full. He purchased an external hard drive, moved all the data to it, and erased all the original data.

Now, it is a good rule of thumb that if a new electronic device is going to fail, it is likely to do so within the first fifty hours. In this case, when he turned on the computer the next day it did not recognize the new drive.

He called the manufacturer, who said it was obviously a Microsoft problem related to the USB driver, and not their problem. He called Microsoft, who spent a substantial amount of time walking him through replacing every driver that could be replaced. Still no joy.

He then connected the drive to someone else's computer, which also couldn't see the drive. This was a clue that it was a drive problem, not a computer problem. At this point he did a query online, and discovered that quite a number of people had been suffering this same problem with this particular model drive.

He ended up taking the drive to a data recovery company. They will attempt to re-build the drive in a clean room, and move the data to a DVD.

If he is lucky enough to recovery all the data, it will cost him a minimum of \$1000, plus of course the cost of the drive he just bought, plus the cost of whatever other drive he gets. If he does not recover the data he is, for all practical purposes, out of business, as he has lost virtually every business record from his entire career.

Our friend's situation is not much different from that of many small businesses, the only difference being that his luck ran out. So what did he do wrong, and what could he have done to minimize this catastrophic – an possibly irrecoverable – loss of information?

Backup

For a start, he needed to back up his data. Backing up data has two parts. First, you need to have at least two copies of all the data, and at least one of those copies needs to be stored far away. Why is this? Well, imagine that you had a business in New Orleans, and kept one copy of your backup data on the bookshelf and the other at your home, neither of which survived Katrina. Fat lot of good the backups would do you.

As an example, we are a small business, and have relatively little data, all of which is stored in encrypted virtual drives. The encrypted virtual drives are regularly copied to an on-line storage facility (we currently use iBackup – see the August 2006 issue of *ÆGIS* or <http://www.ibackup.com>). In addition, these files are copied onto flash drives that we carry with us. In addition, they are regularly copied onto DVDs, with a copy stored in our office and a copy mailed to the other side of the country. An awful lot would have to go wrong to make all our information permanently unavailable.

Computer care

As noted above, if an electronic part is going to fail, it often does so within the first 50 hours. This means that you would be prudent to avoid committing yourself to a new computer or hard drive, getting rid of the old one, until it has been running for a few days. Additionally, you can help assure its continued functioning by using an uninterruptible power supply, better known as a UPS.

A UPS is a device that allows you to run the computer off of a battery, which is constantly being recharged. If power fails, it sounds an alarm, and you can shut down the machine. Or, with most UPS, you can connect it to

the serial port of the computer, and if the power fails it will graciously shut down the computer for you. The advantage of a UPS is that the computer receives consistent power – it is running off a battery – independent of any fluctuations of power coming into your home or office. As it turns out, one of the big causes of mystery computer malfunctions is power fluctuation.

Note that there are also standby power supplies that switch to the battery if the power fails. These are the more common, and less expensive. They do condition the line, and certainly are fine if you can't find a cost effective on-line UPS.

Additionally, hard drives have a tendency to eventually fail: They are, after all filled with rapidly moving parts. Most hard drive vendors provide programs that will allow you to check the functioning of the hard drive. We ourselves use SpinRite (<http://www.grc.com/sr/spinrite.htm> – see the September 2004 issue of *ÆGIS*). In essence, SpinRite reads each sector of data and re-writes it. If there is a problem with the sector, it marks the piece as bad and relocates the data elsewhere. This has saved us on several occasions where a hard disk had gone bad, allowing us to recover the data and keep running at least long enough to back up everything and put in a new drive. If one track is bad, we take note. If more start appearing, we get a new drive.

How about a brand new drive? The first thing we do, even before we load software, is run SpinRite. If the drive passes, we start loading our software. We then run SpinRite every week. We recommend you do the same.

2. OPSEC, Economic Espionage, and Competitive Intelligence — Which weighs more: A pound of feathers or a pound of gold?

This trick question, much beloved by grade school children, is straightforward. A pound of feathers weighs more. This is because feathers are measured in avoirdupois ounces and gold is measured in troy ounces. A pound of feathers is sixteen avoirdupois ounces, and weighs 453.592 grams. A pound of gold is fourteen troy ounces, and weighs 373.24 grams. And yet, even though lighter, a pound of gold is worth more than a pound of feathers.

A more interesting question relates to dollars saved. Imagine that you wanted to save your company \$100 million. One way to do it is to move all your data processing abroad and fire the 1000 people in your current IT staff. Another way would be to implement an OPSEC program, and cut \$100 million in losses.

Now, which hundred million is more valuable? Which is the pound of gold and which is the pound of feathers? One perspective is that the closing down of the data center is the pound of gold. For a start, it is visible: A thousand people get canned, and a lot of technology gets transferred. It also has the theoretical benefit of knowing that in a finite period of time the info centers will be repatriated, based on a combination of increasing costs abroad and decreasing costs here. This too will be visible, therefore good. This is quite different from loss of intellectual property, which is not directly visible.

The other view – our view, as it happens – is that protection of intellectual property, which makes up 70 percent of the value of most organizations, is the pound of gold. According to Aberdeen Group's Protecting Product Intellectual Property Benchmark Report, 48% of manufacturers report lost market share, 44% experienced lost sales, and 27% disclosed lower margins. All of these go into the \$300 billion lost by American companies each year to competitive intelligence, economic espionage, and theft.

Now, we have a fair idea of the impact of theft of “stuff” at the retail level. This is broken down well by Liz Martinez in *The Retail Manager's Guide to Crime & Loss Prevention* (see the March 2005 issue of *ÆGIS*). She says:

Another way to look at the loss/profit equation is the Rule of 33. The Rule of 33 deals with a hypothetical item of merchandise that sells for \$100. The wholesale cost of this item is approximately \$45, which leaves us \$55 as the amount of gross profit. Subtract another \$28 for uncontrollable expenses, plus \$15 for controllable expenses. The net profit at this point is about \$12. Now, deduct another \$9 for taxes, and the grand total of the net profit on this \$100 item is \$3 (after taxes).

To put this equation into perspective, when you sell one of these \$100 items, you have generated a bottom-line profit of \$3. If someone steals one of these \$100 items, its theft represents a bottom-line loss of \$97 because the stolen item costs the same as the item you sold. So in order to make up the money you lost when the \$100 item was shoplifted, you have to sell another 33 of this same item before you will realize your first penny of bottom-line net profit.

Now \$100 million may not seem like a lot. As one senior manager put it to us, “So I lose \$50 million or \$100 million, and I have to close down a division. So what? I am a 35 billion dollar company: It is simply not material.” Putting aside the SEC's disagreement with this, and the likely disagreement on the part of shareholders and those needlessly laid off, loss of profits is not the same as cost savings. It is even worse than the

replacement cost of loss of merchandise stolen, because you will likely have to re-create a new R&D cycle. Which will in turn be stolen. While we do not *yet* have the figures available for IPCI loss that we have for retail item loss, we can certainly assume the same kind of multiplier effect.

Unfortunately, while the \$100 million loss of IPCI may be the pound of gold, the visibility of the cuts will probably be more attractive to most, as the cost of loss of IPCI will be bourn by those who follow in the future, while the credit for the visible measures will accrue to those who lead in the present. They will choose the pound of feathers.

3. Executive Protection — When the melting pot stops boiling

When everything works right, a startling transformation takes place between first generation Americans and second generation Americans. First generation Americans speak with funny accents, eat funny food, wear funny clothing, worship funny invisible creatures, and follow funny customs. Second and third generation Americans talk like us, dress like us, eat like us, and are us, even if their skin color or facial characteristics are different.

When things don't work right, this melding does not take place. Citizens either choose or are forced to stay together, which separates them from the country as a whole.

If ghettoization occurs, or if people are not permitted to integrate into mainstream society, then they may maintain accents and customs for generations, suffer economically and socially, causing civil unrest and potential danger to society at large, which includes those under our care and protection. At the moment, the problems of failure to integrate seem clearest to us when we look at un-integrated Middle Eastern populations in Europe, but this merely distracts us from the American black population that is still not as completely integrated socially or economically into American society as one might hope and expect.

The difference between the two cases, however, is clear: People of color in the United States know they are Americans, and merely want their equal opportunities and rights. In the European case, people seem to be trying to force their home-country customs on the wider community where they now live. This has largely not been the case here, although we have seen some attempts by religious, er, folks to force their particular beliefs on the community as a whole.

One deeply religious, deeply fundamentalist friend of ours explains this as the result of people almost, but not quite, having faith in God.

As an example, he believes that abortion is a mortal sin, and that anyone having anything to do with abortion will be deprived of God's light in eternal perdition. He has, however, no particular interest in making abortion illegal, and no interest whatsoever in picketing hospitals or blowing up clinics. He believes that while it would be reasonable for abortion to be illegal if we had a theocracy, in a democracy it is inappropriate. If people in a democracy choose to involve themselves in mortal sins they will face eternal perdition, which is way worse than any criminal penalty. It is only when one does not quite have confidence in God's power that one feels impelled to act in God's place. Almost (but not quite) having faith, he believes, is more dangerous to society than actual faith or lack of faith.

We are certainly neither theologians no psychologists, but this seems as good an explanation as any of why people commit loony and destructive acts in the name of their god of choice.

Lack of integration is not helped by cultural pride when it serves to separate a citizen from society. This view was clearly expressed by Teddy Roosevelt on 12 October 1915, when he spoke to the Knights of Columbus in New York City. He said:

There is no room in this country for hyphenated Americanism. When I refer to hyphenated Americans, I do not refer to naturalized Americans. Some of the very best Americans I have ever known were naturalized Americans, Americans born abroad. But a hyphenated American is not an American at all.

This is just as true of the man who puts "native" before the hyphen as of the man who puts German or Irish or English or French before the hyphen. Americanism is a matter of the spirit and of the soul. Our allegiance must be purely to the United States. We must unsparingly condemn any man who holds any other allegiance.

But if he is heartily and singly loyal to this Republic, then no matter where he was born, he is just as good an American as any one else.

The one absolutely certain way of bringing this nation to ruin, of preventing all possibility of its continuing to be a nation at all, would be to permit it to become a tangle of squabbling nationalities, an intricate knot of German-Americans, Irish-Americans, English- Americans, French-Americans, Scandinavian- Americans, or Italian-Americans, each preserving its separate nationality, each at heart feeling more sympathy with Europeans of that nationality than with the other citizens of the American Republic.

The men who do not become Americans and nothing else are hyphenated Americans; and there ought to be no room for them in this country. The man who calls himself an American citizen and who yet shows by his actions that he is primarily the citizen of a foreign land, plays a thoroughly mischievous part in the life of our body politic. He has no place here; and the sooner he returns to the land to which he feels his real heart-allegiance, the better it will be for every good American.

4. Technical Issues — Laptop protection

We have seen a recent rash of reports of problems caused by stolen computers. In some cases the computers were laptops, and in others they were desktops. In all cases, the confidential information on the computers was unprotected. This seemed to us to be good reason to again address the issue of data protection on your PC.

For a start, you should ask yourself if there is anything of value on your home or office computer that would cause a problem if the machine fell into the hands of others. If the answer is no, please ask a grownup to take over from here.

Assuming the answer is yes, how can you protect the information? For a start, you need to encrypt any information that you don't want in the hands of others. We use Private Disk (see the November 2006 issue of *ÆGIS*) to create an encrypted virtual disk on our hard drive, and our e-mail client, The Bat! (see the January 2005 and July 2006 issues of *ÆGIS*) stores our e-mail and address book in encrypted form. Some files that are particularly sensitive we encrypt with PGP.

On the down side, we at present use the challenge and response system ChoiceMail (see the February 2007 issue of *ÆGIS*) to filter spam. This leaves the list of accepted e-mail addresses visible, but we feel this risk is acceptable.

One way to bypass our efforts would be to put in a keylogger. We try to deal with this by having software that should detect keyloggers, by having a lock on the computer to make it difficult to open, and by having our office alarmed. We inspect regularly for tampering of the keyboard.

Finally, we are always concerned with the computer being stolen in spite of all our efforts. To deal with this we have installed PC Phone Home (see the April 2002 issue of *ÆGIS*). This software, available for both PC and MAC, should allow us to locate our computers when they are stolen.

5. Real Stories from the Field — Spies for sport

NFL security confiscated a video camera and its tape from a New England Patriots employee on the team's sideline during a game against the Jets in a suspected spying incident (videotaping of an opponent's offensive or defensive signals on the sidelines is prohibited, though observing them and writing them down seems to be ok). There were also issues about whether radio transmissions had been captured.

We find it interesting that while corporations don't have much interest in actively protecting intellectual property and critical information (even though it makes up 70 percent of their value), sports teams do. We suspect that this is because there are fewer layers to obfuscate cause and effect. A bad decision or lack of care with IPCI can lead to lost points and lost games very quickly and directly.

This is quite different from a corporation. If a corporation suffers a loss it is less obvious. Sure, they may lose \$50 or \$100 million in an incident, but if they are not small enough to be put out of business it goes virtually unnoticed. Sure, they may have to fire 1,000 people or close a division, but in a large corporation that will still have no adverse affect on the remuneration of senior managers, and will largely go unnoticed.

6. Book and Product Reviews

Filecrypt Desktop 2.0

Veridis \$49.00

<http://www.veridis.com/pgp/products/filecrypt-desktop.html> +32 10 88 73 70

As readers know, we are strong proponents on using encryption when appropriate. We store data on encrypted virtual drives, and encrypt individual files if they are sensitive, use encryptors on our telephones when making sensitive calls, and encrypt e-mail that we don't want read by others.

In the October 2005 issue of *ÆGIS* we discussed a number of PGP variants, including *Filecrypt Desktop* from Veridis. This early version lacked integration with Windows. We are now happy to announce the second version of Filecrypt, which *does* integrate well. You can now right click on a file in Windows Explorer and sign, encrypt, sign and encrypt, or delete it.

While Filecrypt Desktop 2 does not integrate with e-mail programs, we consider this to be a non-issue. Simply copy the text, encrypt it to the clipboard, and paste it into your e-mail message.

If you are looking for a straightforward, easy to use Open PGP system, FileCrypt 2 is well worth your consideration.

7. Subscription/Unsubscription/Copyright Information

•• **ÆGIS** is supported and maintained by voluntary efforts. This publication is owned, published, and copyright © 2007 by The **LUBRINCO** Group Ltd, Inc. and Financial Examinations and Evaluations, Inc. It is edited jointly by Richard Isaacs (RBIsaacs@lubrinco.com), L. Burke Files (LBFiles@feeinc.com), and Terry Phillips (TPhillips@aegisjournal.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.

- **Identification, valuation, and protection of intellectual assets and critical information.**
 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, theft, and deliberate disclosure.
 - LUBRINCO is the leading private sector provider of access to OPSEC, the government-standard process for identification, valuation, and protection of intellectual property and critical information from competitive intelligence, economic espionage, theft, and deliberate disclosure.
- **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, anti-money laundering, and anti-corruption program development and training.
- **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.aegisjournal.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, send an email to subscribe@aegisjournal.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, send an e-mail to unsubscribe@aegisjournal.com.

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

If there is a topic that you would like to know more about, send it to editor@aegisjournal.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 editor@aegisjournal.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 **ÆGIS** Web site is included. This should be in the form

Article Title, from the September 2007 **ÆGIS** (© 2007 **LUBRINCO** & FEEINC), to be found at <http://www.aegisjournal.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.