



International Institute of Security & Safety Management



Let's professionalize the professionals...



Newsletter of NCR Chapter : March 2009

Third Year on – Going Strong!



We started our Newsletter in March 2006 exactly three years back! When word 'we' is used in present context, it appears to be misnomer as it was 'we' only in exception and mostly it remained a singular effort in bringing out the newsletter. Publishing 36 newsletters of average 10 pages of relevant yet high quality contents drew my attention to many and varied facets of security management. While collecting the information suitable to our readers, my knowledge also got upgraded! It also honed my writing skills which resulted into shaping up a book I am fortunate to co-author with no less than an authority in the field then Shri D C Nath! Does he need any introduction?

I had the good fortune of first interacting with him in 1988 when I started my career in field of industrial security and attended a training program organized by Intelligence Bureau. He was then Special Director in IB and was known for his meticulous approach to all the subjects he handled and penchant for perfection. He was authority on industrial security even then! Now he is a doyen!! I do not know any one more senior or knowledgeable than him in India! There are many senior Army or Police officers now in the field of industrial security but none as senior as him in terms of experience in the field! It is therefore my good fortune that I learned under his tutelage and could find my name alongside his name on the cover of the book titled "Industrial Security: Planning & Strategies".

The book was formally released during the opening ceremony of Security Seminars conducted by IISSM in recently concluded 12th India International Security Expo 2009 on 22nd February 2009. Shri R D Tyagi, IPS, former Director General of National Security Guard did the honor by releasing the book underscoring the need and importance of the book in present context when so much attention is being paid on high quality training, to be imparted to security professionals. An illustrious police officer, Shri R D Tyagi himself is known for his sound knowledge and practice of Industrial Security Management. I hope the readers will benefit from the book.

**Capt S B Tyagi, FISM, CSC
For NCR Chapter, IISSM**



Book Launch - Industrial Security: Management & Strategies





In Pakistan a can of petrol is more dangerous Than a dirty bomb

Intelligence experts reported recently that terrorist groups are taking advantage of the chaos in Pakistan to get radioactive material, and are hoping to use it to make a 'spectacular' attack on the West.

People fear they might explode such a weapon in London or another major city, kill hundreds, if not thousands, trigger widespread panic, and perhaps force an indefinite evacuation.

Much of this fear is unwarranted. Dirty bombs spread radioactivity, and that's bad - but true nuclear weapons, such as the bombs that destroyed Hiroshima and Nagasaki, are much worse because of their enormous release of energy, the equivalent of 18,000 tons of TNT for Nagasaki alone.

Most of the deaths in these nuclear attacks came from blast and fire, and less than two per cent from lingering radioactivity.

Could terrorists make a true nuclear weapon completely on their own? Virtually all experts say no.

To do so requires either the enrichment of uranium, involving expensive high-tech methods, as Iran is doing with its centrifuges, or the tricky implosion of plutonium, the approach taken by North Korea.

Kim Jong Il spent billions on his bomb project, and the result was less than a kiloton of explosion - five per cent of the Nagasaki bomb. It's tough to make a dependable nuclear explosion.

Compared to a real nuclear bomb, a dirty bomb is easy, and certainly within the reach of a well-organised terrorist group. All it needs to do is get some radioactive material and blow it up with dynamite or another conventional explosive.

Terrorists could get radioactive materials from Pakistan, but they could also get them from hospitals, where radioactivity is used for everything from cancer therapy to CAT scans.



Fearful: Right At Your Door
A 2006 film in which dirty bombs are used to attack Western cities



In 1987, scavengers opened a container they found in an abandoned hospital in Goiania, Brazil. They didn't know it was radioactive until days later, and by then they had contaminated themselves and 200 others. Three adults and a child eventually died from radiation illness.



Forty one houses in the neighborhood were evacuated. This was all inadvertent.

Why dirty bomb is really not so dirty?

A full-scale nuclear blast packs vastly more power than dirty bomb could. Imagine what terrorists could do on purpose. Suppose they got a Goiania-type source and spread the radioactivity over a whole city - what would happen?

The answer is surprising. Spread out the radioactivity enough and the deaths from radiation illness disappear completely.

People exposed would have a slight increase in the risk of eventually contracting cancer, but there would be no dead bodies at the scene - except those killed by the dynamite. Diluted radiation loses its potency.

We measure radiation dose in units called Rem. Above 1,000 Rem incapacitation occurs within minutes, followed by extreme fatigue and nausea, then death. For smaller doses, 300 to 500 Rem about half of the victims die within a month.

But reduce the dose a little more - down to 100 Rem and the effects are very mild. At 50 Rem nobody even gets sick!

This 'threshold effect' creates problems for the terrorist. He can put radioactive material into a bomb - but concentrated radioactivity kills fast, so he'll have to protect himself with a ton of lead.

Then he must deliver the bomb, take it out of the lead shield and explode it with dynamite so the radioactive material spreads into the air.

He wants the wind to carry it around the city, but has to hope it doesn't spread too much or it won't kill anyone.

If radioactivity comparable to that of the Goiania accident were spread over a square mile, the exposure to people - even if they stayed outdoors for a month - would have been only 10 Rem far below the lethal threshold. There would be no radiation illness, no dead bodies.

Low levels of radiation do cause harm, but it is hidden and delayed: tiny mutations in your DNA that increase your risk of cancer by a very small amount.



Why petrol is dirtier than dirty bomb?

Would a terrorist be satisfied with the knowledge that his bomb might cause a small increase in cancer deaths among a small number of people in many years' time? Or would he pick an alternative attack?

Petrol bomb: The jet fuel in the planes that hit the World Trade Centre released the energy of 1.8 kilotons of TNT

Consider Jose Padilla, the Chicago thug who was trained by Al Qaeda and came to America planning to make a dirty bomb.

According to the US Justice Department, Al Qaeda had doubts about the practicability of such an attack, so it directed him to abandon the dirty bomb and blow up two apartment buildings using natural gas.



What worries everyone about this story is that it suggests Al Qaeda understands the limitations of dirty bombs better than government leaders and many scientists.

It is suspected that any well-organised terrorist organization would pick a more reliable weapon, such as petrol or jet fuel. The 120 tons of jet fuel in the planes that hit the World Trade Centre released the energy of 1.8 kilotons of TNT - over twice the energy of the North Korean nuclear test. Have you looked it from this angle?

Aircraft attacks have worked for Al Qaeda in the past. They are far more straightforward to implement than a dirty bomb and the results are more predictable. Buses loaded with passengers and laden with fuel and explosives are another possibility. Hindi films have shown this approach employed by the terrorists and western had originally shown this approach as used by the criminals! But terrorists learn fast and implement faster!!

What your bank should be doing to protect you from ID theft



Identity systems are powerful and profitable business tools, but only takes one broken link in the identity chain to foul the whole works up..."

**James Van Dyke
President, Javelin Strategies & Research**

A person I know suddenly learned that he was a debit-card identity theft victim - while his debit card was locked in a bank safe deposit box!

He immediately informed his debit-card issuer, a major bank, but the branch representative said there was nothing she could do. I directed him quickly to an identity theft hotline, buried on his bank's Web site.



Such a slow response by your bank could lead you to suffer a greater financial loss if an identity thief targets you. So it could pay when you open your bank account to find out exactly what steps your bank takes to curb identity theft.

While many credit and debit-card accounts promise consumers zero liability if their credit or debit card is lost and stolen, that doesn't mean you can't suffer. Your bank may not buy your story and you may be forced to hire an attorney. Many victims don't prosecute because thieves often are family members. So you still could suffer un-reimbursed financial losses, lost wages and legal fees.

Warning: Some 12% of major banks lack a zero-liability policy for debit cards that require access via a personal identification number or PIN, according to 'Javelin Strategy & Research' a marketing research organization based in USA. So learn how your bank protects against identity theft, particularly before opening a PIN-accessed debit card.

In USA, federal law limits card holder's losses on a lost or stolen credit card to \$50. In India there appear to be no such guidelines. Even if there is one, it is not widely publicized. You may have some protection for credit / debit cards - provided that you promptly notify your bank.

Nevertheless, losses when your identity is stolen, according to Javelin's 2008 Identity Fraud Survey Report, can escalate the longer the fraud goes undetected. Victims who detected the fraud within one day spent an average of \$428. But those who took up to five months lost three times as much -- \$1,207, its report says.

Meanwhile, if somebody opens a new account in your name and nobody contacts you, you risk suffering greater losses. You might not hear about it until a debt collector calls or you're suddenly denied credit. This gives thieves a maximum amount of time to do their damage.

Your bank can take precautions

There are certain things your bank can do to nip an identity theft in the bud. It could pay to make sure your bank takes certain precautions, advocated in the Javelin Strategy survey:

- Provides you with the ability to create restrictions - either online, by phone or in-branch - on particular transactions. Don't think you'll ever conduct any wire transfers outside the United States? Bank only with institutions that let you limit those transactions.
- Eliminates distribution of your personal information and limits use of your Social Security number to the last four digits.
- Offers to email or text message you if there's ever a change of personal information, including a change of address, addition of a cardholder or unusually low balance on your account.
- Has a centralized fraud resolution department.
- Lets you quickly freeze your account.



- Requires at least two ways to confirm your identity both by telephone and online banking.
- Regularly educates employees on how to properly secure sensitive information.
- Regularly examines employees for insider collusion.
- Encrypts your personal identification numbers, passwords, Social Security numbers and other private data.
- Uses no hyperlinks in emails. This way, you can determine which emails don't come from your bank.

Meanwhile, Javelin Strategy & Research reports increased theft via mail order or telephone order purchases. It cites a newer tactic, "Vishing," or using the Internet to place phone calls. Internet-placed calls are tougher to trace.

Bottom line: Never provide personal information -- even over the telephone. If you get a communication from your bank, call only the telephone number you already have -- not the one in the communication.

ID theft up or down?

It seems comforting that Javelin Strategy reports a 12% decline in identity theft in 2007. But not everyone agrees with that company's study, sponsored by Visa, Wells Fargo Bank and CheckFree Services Corp.

For one thing, the Federal Trade Commission reports a 32% rise in identity theft complaints to 258,427 during the 2008 calendar year. Chris Jay Hoofnagle, senior fellow at the University of California-Berkeley law school, complains that consumers, regulators and businesses have no reliable way to assess identity fraud at major financial institutions.

"Lending institutions should publicly report basic statistical information about identity theft events," he says. Information they should disclose: The number of identity theft events suffered or avoided; the form of identity theft attempted; the targeted product, such as a mortgage loan or credit card; and the amount of loss suffered.

Information Security

"Shoulder surfing" – it means that someone is trying to glean information off a computer screen by looking over the user's shoulder. "All covered entities should be looking at this closely,"

Violations of patient confidentiality by definition may put patients at risk of identity theft. For example, a computer belonging to Hospital in Houston was stolen from the office of one of its vendors earlier this year. The vendor had possession of the computer to convert paper records to electronic files, according to news reports.



The computer appears to have been stolen for its own value, news reports say, but it contained patients' medical records and Social Security numbers. It was also noted that the vendor lacked bars on its windows, unlike other companies in the same building. The hospital fired the. The magnitude of this debacle became clear when, in April, the hospital sent 16,000 letters to patients saying that their Social Security numbers and medical records may be on a computer stolen from a hospital vendor.

This hospital has aggressively cracked down on identity theft since its own first-hand experience in 2002, when an employee of the hospitals stole 32 patient Social Security numbers and gave them to her boyfriend, a gang member, who sold them for \$100 each. To get the Social Security numbers, the wayward employee had confiscated inpatients' "blue cards," which were used to label their medical records and contain their names, addresses, birth dates and Social Security numbers. The buyers used the private data to obtain credit cards in the patients' names.

When a patient realized his identity had been stolen, he contacted the hospital in May 2002 to see if it had been the source. The theft was confirmed. Ultimately, the employee pleaded guilty in the case and testified against other perpetrators. The hospital stopped using blue cards.

The ID Theft Risk Assessment

Because of this experience, hospital initiated an identity theft risk assessment, examining:

- The identity theft risks it faces;
- Existing processes for responding to an identity theft incident;
- Methods other organizations have used to minimize the threat of identity thefts; and
- The strategies one could pursue to minimize the risk to identity theft.

Terrorist tactics that will show up on this side of the ocean could employ weapons of mass disruption rather than mass destruction.

And as we've seen since 26/11 Mumbai Attack, the psychological and economic effects of an attack can linger as a powerful force. This enemy is patient and smart. If we assume anything else, we stand into danger.

At the other end of the day, our job as the security profession's leader comes down to a process of Domain Awareness - what's going on out there - followed by Prevention-Protection, Response-Restoration, and Consequence Management. Creating the framework is the easy part ... filling it out with meaningful public-private activities is our ongoing challenge.

There is often a frustrating reality in our 'post-26/11 Mumbai attacks' normalcy that involves security checks, inspections, going through the standard operating procedures etc. But the other reality is that we don't want to hamstring business either. It's a balancing act - much like the teeter-totter with security on one side and customer service on the other ... all of it resting on a foundation of economic stability.



The responsibility of keeping awake, and Resisting complacency Falls on every one of us!

A corrupt country cannot fight terrorism

Swapping ministers is not change. Change your leaders in 2009.

Our country needs an aggressive anti-terror plan like the one below

- 2. Get latest arms and technology** for coastal and inland policing, upgrading anti-terror forces
- 3. Make the police independent - remove political control.** (the department can be placed under an independent commission. this will also reduce abuse of the police force as body guards for VIPs, for providing political intelligence to the ruling party, for collecting money for a corrupt establishment etc.)
- 4. Provide identity cards to the population before the next election.**
- 5. Announce a reward for good information given regarding terrorists.**
- 6. Punish ministers,** officials who delayed calling the army and let the communal killings continue in Delhi (1984), Gujarat, Mumbai and Orissa (Riot survivors who saw their friends and family abused or murdered need to be given justice. Lack of justice breeds young terrorists).

Thank you
Sincerely

Arun Bhatia
arun@arunbhatiaelect.com
<http://www.arunbhatiaelect.com>

"If at first you don't succeed, failure may be your style."

- Quentin Crisp



Dates to Remember!



The Certification Courses conducted by IISSM are widely known and acknowledged. In order to meet the increasing demand from practicing executives, it is proposed to organize four such Courses in 2009, all in New Delhi for the present.

The venue is the Conference Room of IISSM Office complex. Suitable number of participants will be accommodated in each batch on the basis of first come first serve. The first such program is organized on March 18-21, 2009.

- Mr. D C Nath, Executive President & CEO, IISSM at nathdc@iissm.com
Mobile: 9811995693
- Lt. Gen. Prem Sagar, Executive President (C&F), IISSM at premsagar@iissm.com
Mobile: 9899078687



Suggestions & feedback may be sent to us on e-mail: captsbtyagi@yahoo.co.in
