



International Institute of Security & Safety Management



Let's professionalize the professionals...



Newsletter of NCR Chapter : February 2009



Security Return on Investment: My Experience

Before sanctioning the expenditures on security measures the Managements often ask for "return on investment" as is the vane for other activities of the commercial entities. In most organizations security department is treated as 'cost centre' where there is no linkage with productivity or profitability. But, my recent experience has shown how a smart business often thinks and treats the security function differently and draws benefits.

I patronized Reliance Store in my neighborhood in Gurgaon where I live. Once I bought some groceries and paid for it. There was only one poly bag handed over to me by the cashier handling the counter. After reaching home I realized that against billed amount there were three items short in the poly bag. I immediately returned to the store with the confidence that my matter will be resolved. To my pleasant surprise when I approached Store's 'Loss & Found' counter, the gentleman over there willingly inquired the matter, took me to their CCTV Control room and replayed the archived recording of the camera overlooking the counter. After first play there was nothing abnormal detected. But after second\ld replay with slower speed it became clear that the man at the counter read all the grocery items with his handheld barcode reader and kept them in two poly bags but after receiving the payment handed over only one bag to me. I kept these bags on the shelf in front of this counter and made some inquiry somewhere else. The recording further revealed that the counter man after my leaving the place kept the second bag near my already kept first bag apparently after realizing that he forgot to give me the second bag. This bag was mistakenly picked-up by some other customer! After this archive playing of CCTV recording, store in-charge handed over me the items in question.

Here question is - why did I go back to store driving extra kilometers spending about Rs.200 when items in question were worth Rs.34 only? Because, I trusted that the store like Reliance will listen to my complaint and with the help of CCTV, will try to ensure that no mal-practice was being done by the cashier and no customer would be doing shop-lifting! I was sure that Reliance Store is conscious of its market image and will do it's best for the trust, confidence and satisfaction of the customer.



Suppose, if they failed me! Suppose if they could not find out the real reason behind my complaint!! It surely would have shared my experience with the family members, friends and peers! In my limited circle, I as opinion maker would have changed their perception towards the store, which no sane business entity wants! The expenditure on CCTV in the store with which they could restore the trust and confidence of its customer, it is the investment worth making. It takes long time and hard work to create brand identity, brand equity and brand loyalty but it takes incident like mine to shatter them all in few seconds.

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

Security: Return on Investment

Executive decision-makers don't really care whether firewalls or lawn gnomes protect their company's servers. Rather, they want to know the impact security is having on the bottom line. In order to know how much they should spend on security, they need to know:

- How much is the lack of security costing the business?
- What impact is lack of security having on productivity?
- What impact would a catastrophic security breach have?
- What are the most cost-effective solutions?
- What impact will the solutions have on productivity?

Before spending money on a product or service, decision makers want to know that the investment is financially justified. Security is no different -- it has to make business sense. What Decision makers need is a security metrics that show how security expenditures impact the bottom line. There's no point in implementing a solution if its true cost is greater than the risk-exposure. Every management wants it yet ROI has been very difficult to calculate successfully.

Following attempt is worth understanding and can be applied successfully to any business -

- T is the cost of the intrusion detection tool.
- To determine return on security investment (ROSI) we simply subtract what we expect to lose in a year (ALE) from the annual cost of intrusion. Doing this equation yields the Annual Loss Expectancy.
- E is the savings gained by stopping any number of intrusions through the introduction of an intrusion detection tool.
- R is the cost per year to recover from any number of intrusions.

$$(R-E) + T = ALE$$
$$R - (ALE) = ROSI$$



The above equation will clearly highlight that earlier investment is made on good Security, the greater are the returns! Researchers have found that a business gets a 21% return on security investment at the design phase, a 15% return at the implementation stage and a 12% return at the testing stage.

In the absence of actual data on the number of incidents, organizations are often forced to make estimates. Also, the impact of an individual incident can be difficult to assess. In spite of those drawbacks, a common industry security ROI method would deliver several benefits, including the following:

- The contributors to security readiness, the costs to achieve security readiness, and the costs to recover from cyberspace incidents can be better understood.
- The enterprise can reason about its security investment decision with increased precision.
- The public-private collaboration discussion on 'who is responsible for paying for security' can be better informed.
- The relationship between levels of security readiness and recovery costs can contribute to the actuarial basis for underwriting cyberspace insurance.
- The state of security readiness for the nation's critical infrastructure dependent on software can be better assessed.

Security ROI is savings divided by cost. Reasoning about ROI, then, is assisted by evaluating the expression $[ROI: = Savings/Cost]$ where -

- **Savings** is cost avoidance resulting from resistance, recognition, and reconstitution efforts.
- **Cost** includes preparation and incident cost. Incident cost is cleanup, lost opportunity, and critical infrastructure impact.

Methods for computing security ROI are needed to answer questions important to the security investment decision, such as the following:

- If the expected number of incidents is low, will the security readiness investment be recouped?
- For a higher number of cyber attack incidents, what are the minimum factors which are needed to fully recoup security investment?
- Is there an equitable scheme for sharing security readiness costs among the project, the enterprise, and the government?
- What are the guidelines for public-private collaboration and cost sharing?
-

O'Neill, Don, "[Security Return on Investment Interactive Worksheet.](#)"



Hoax Mail in Circulation

IF SOME ONE ASKS YOU TO DIAL #09 or #90, please do not dial this when asked!

New Trick of Jehadi Muslim Terrorists to Frame Innocent People!!

If you receive a phone call on your Mobile from any person saying that they are checking your mobile line, and you have to press #90 or #09 or any other number. End this call immediately without pressing any numbers.

Friends there is a fraud company using a device that once you press #90 or #09 they can access your SIM card and make calls at your expense. Forward this message to as many friends as u can, to stop it. This information has been confirmed by both Motorola and Nokia.

There are over 3 million affected mobile phones. You can check this news at CNN web site.

Please circulate URGENTLY.

<http://rabiabegum.sulekha.com/blog/post/2009/01/09-or-90-please-do-not-dial-this-when-asked.htm>

Authentic Response: McAfee Avert Labs HOAX Notice!!

McAfee Avert Labs would like to inform you of an email HOAX.

This email message is just a HOAX and is a variant of the ACE Mobile Phone Hoax. Currently we know of no call that the user will receive about the HOAX as the initial email states.

McAfee Avert Labs has not received any report of a user's mobile phone being rendered unusable for receiving the call. We are advising users who receive the email to delete it and DO NOT pass it on as this is how an email HOAX propagates.

Below is the actual text from the message that may be received via email:

Dear All,

If you receive a phone call on your mobile from any person, saying that, he or she is a company engineer, or telling that they're checking your mobile line, and you have to press # 90 or #09 or any other number. End this call immediately without pressing any numbers. There is a fraud company using a device that once you press #90 or #09 they can access your "SIM" card and make calls at your expense. Forward this message to as many friends as you can, to stop it.

All mobile users, pay attention. If you receive a phone call and your mobile phone displays (XALAN) on the screen don't answer the call, END THE CALL IMMEDIATELY. If you answer the call, your phone will be infected by a virus. This virus will erase all IMEI and IMSI information from both your phone and your SIM card, which will make your phone unable to connect with the telephone network. You will have to buy a new phone. This information has been confirmed by both Motorola and Nokia. There are over 3 Million mobile phones being infected by this virus in all around the world now. You can also check this news in the CNN web site.

Again, if you receive this email delete it and DO NOT pass it on. Verify at -

http://vil.nai.com/vil/content/v_141392.htm

<http://www.blogcatalog.com/search.frame.php?term=if%20some%20one%20calls%20and%20asks%20you%20to%20dial%20&id=6ddb1ba36f41fc91f93fdcaf59082ec1>



- Is your daughter wasting her time on that no good punk?
- Is your partner cheating on you and making secret calls in the bathroom?
- Are your family members wasting too many unnecessary minutes on your phone contract?
- Are your children texting or talking on the phone when they should be doing their homework or household chores?

WORKS ON ALL CELL PHONES!

Use the software to control electronics devices with your phone!

Use the software to

- View contacts list
- Read text messages (SMS)
- View calls made / calls received
- Set the target phone to call you whenever it makes or receives a call
- View photos
- Many more functions
-

HAVE COMPLETE POWER DOMINATE ANYONE'S PHONE

Control electronics and other people's televisions, radios, mobile phones, security systems with your phone, even traffic lights!

MAKE CALLS VIA THE PHONE YOU HAVE TARGETED

Once the target phone has been remotely set you do not need to be in Bluetooth range to listen into calls. There is no trace or logging of your phone's details on the target phone

That means: they will never know

With our Pro-Edition Software you can now easily find out who your partner, business associates, and friends have been in contact with. Whether you are suspicious of an affair, or would just like information that will help progress your career, you can now do all of the following using your mobile phone, and the person you are targeting will not suspect a thing. Guaranteed!

http://www.spymastertools.com/Ultimate-Bluetooth-Mobile-Phone-Spy_p_0-8.html



Security industry to touch Rs 50,000 crore in 4 yrs



New Delhi: Private security in India will become a Rs 50,000 crore industry in four years as corporate have increased their spending on safeguards after the Mumbai terror strikes, industry chamber ASSOCHAM has said.



Corporates would up their security budgets by 35-40 per cent, the industry chamber said.

The private security business, a Rs 22,000 crore industry now, would touch Rs 50,000 crore as security all of a sudden has become top priority for Indian Inc, it said.

The industry, which has been growing at 25 per cent over the past 5-7 years, would achieve a growth rate of 125 per cent by 2012, it added.

Since a lot of industrial expansion, especially in the infrastructure sector, would take place during the 11th Five-Year Plan, the cost of security gadgets that need to be imported will work out to Rs 20,000 crore in the next two years, it said.



ASSOCHAM further said demand for security gadgets has also increased in educational institutions, hospitals, shopping malls and business centers.

Not only will the manufacturing of security gadgets see voluminous growth, there will more demand for security personnel.

It is expected that over 2 lakhs security professionals would be required in industrial installations in the next few years as no industrial house henceforth can afford to take security lightly, ASSOCHAM General Secretary D S Rawat said.

"Foreign security companies have also started assessing Indian markets for sale of gadgets," he said adding the government should cut import duty on security gadgets by about 50 per cent.

Source: <http://www.financialexpress.com/news/security-industry-to-touch-rs-50-000-cr-in-4-yrs/393783/>

Laugh:

I'd rather laugh with the sinners than cry with the saints!



Software to help Security

With increasing global concerns on terrorism, scientists have devised an e-response to terror by generating tens of thousands of likely behavior patterns of major terrorist organizations, including Hezbollah and Hamas.

Researchers at the University of Maryland's Institute for Advanced Computer Studies (UMIACS) have put these findings on an Internet portal giving access to experts to accurately forecast potential steps of terrorists after analyzing their previous behavior patterns.

Stochastic Opponent Modeling Agents (SOMA) has already prepared likely behavior pattern of several terror outfits, including Hezbollah, Hamas and Hezb-I-Islami. In collaboration with computer experts and political scientists, it has found probability of each of the organizations taking certain actions in different situations.



SOMA Terror Organisation Portal (STOP) will automatically learn the rules that activities of terrorist outfits follow and will set up network to other analysts examining the same subjects, researchers say.

"SOMA is a significant joint computer science and social science achievement that will facilitate learning about and forecasting terrorist group behaviors based on rigorous mathematical and computational models," Professor V S Subrahmanian of UMIACS, who heads the project, said.

The networking ability of the new computing system is considered to be highly conducive to the fight against terror, transcending the national boundaries, say researchers.

"It takes a network to fight a network. Analysts need to learn from other analysts. This system allows multiple users to arrive at a shared understanding of how a terror group operates and what it might do in the future," said Aaron Mannes, a researcher at UMIACS.

"Using the queries, analysts can examine the underlying data and then, using the forecasting capabilities, test their theories," he said, underlining the necessity of more than just piles of data for experts.

The unique STOP system, which also allows other experts to comment on any strategy, is being used by four Defence agencies successfully in preparing combat methods against the terrorists. The availability of comments from other experts may sometimes help to find useful data and interesting rules, experts say.

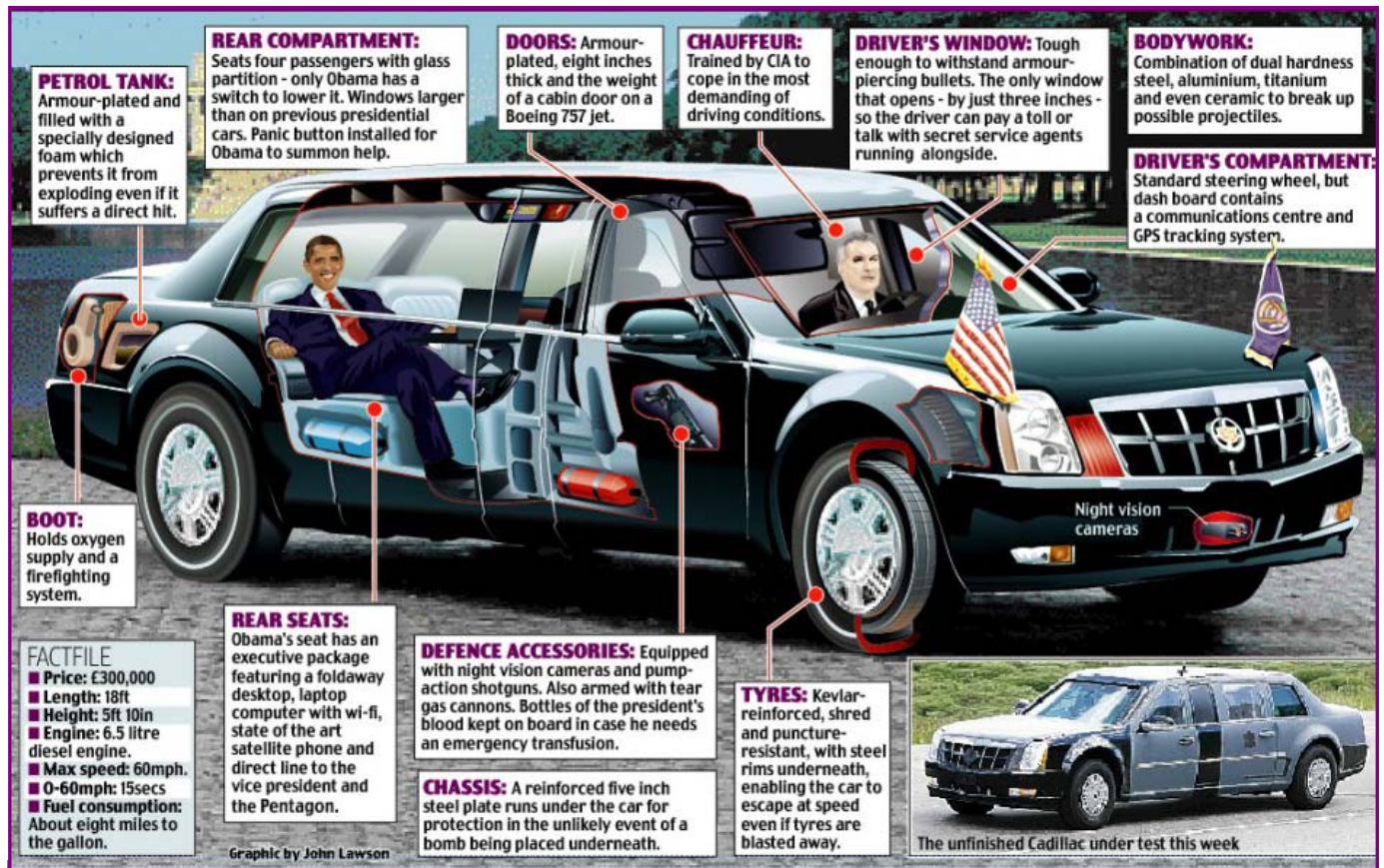
The researchers, however, spoke for a multifaceted approach to find a solution of spiraling terror activities, as often there is a socio-economic background. "But even the best science needs to work hand in hand with social scientists and users," Subrahmanian says.

The project was funded by the US Air Force Office of Scientific Research. – **PTI**



THIS PRESIDENT IS MORE IMPORTANT THAN ANYBODY IN THE PAST

The Obamamobile: New presidential limo is unveiled - and it can withstand rocket and chemical attacks. Its official call sign is Cadillac One, but it will always be known as the Obamamobile.



His Secret Service agents have already been familiarizing themselves with the machine they call 'The Beast', built by General Motors in Detroit and based on a Cadillac chassis.

Bulletproof glass and armor-plating are standard throughout and the car is hermetically-sealed to withstand chemical

weapons. As with previous presidential limos it is packed with electronic communication systems to allow Mr Obama to keep in contact with the outside world. One personal touch will be the remote-controlled ten-CD changer on which he can play his favorite artists, said to include Stevie Wonder and Bob Dylan.

Despite the protection afforded by Cadillac One, the Secret Service will be taking no chances when Mr Obama is sworn in as the 44th president. A three-mile security perimeter will be thrown around the U.S. Capital, with no vehicles allowed inside, to prevent a car bomb attack.

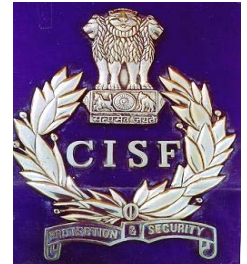


12th INDIA INTERNATIONAL SECURITY EXPO 2009

February 22-25, 2009, Pragati Maidan, New Delhi.



Security systems have become an integral part of virtually every facets of life. Aviation security, cyber security and disaster management along with fire protection and prevention in industrial, urban/rural and public places are also assuming increasing relevance.



With the change in the trend and character of crime besides its element of growing sophistication, it becomes imperative that counter measures be reviewed and upgraded from time to time. Another factor that warrants this periodic review is the fast changing security technology scenario.

The 12th India International Security Expo 2009 of the India Trade Promotion Organization (ITPO), in which IISSM is collaborating along with the Central Industrial Security Force (CISF), is scheduled at Pragati Maidan, New Delhi, on February 22-25, 2009. IISSM is organizing four ½ day's Security Seminars on all the four days of the event at the venue itself on "Security – The Way Forward". We do hope to meet some of you there.

Module Day	Date	Timings	Break	Subject	Fee (Rs. / \$)
1	22.02.09	1400 hrs - 1730 hrs	1500 hrs - 1530 hrs	Terrorism in the wake of 26/11, Mumbai Threat Analysis and Countermeasures	2000 / 45
2	23.02.09	1400 hrs - 1730 hrs	1500 hrs - 1530 hrs	Information Security – Risk Management Hotel Security	2000 / 45
3	24.02.09	1400 hrs - 1730 hrs	1500 hrs - 1530 hrs	Security Audit Retail Security	2000 / 45
4	25.02.09	1400 hrs - 1730 hrs	1500 hrs - 1530 hrs	Women Security Standardization of Equipments	2000 / 45

More Details at: www.iissm.com

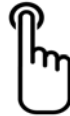
Contact for registration - Email: premsagar@iism.com

"Life is what happens to you while you're busy making other plans."

- John Lennon



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 (4) such Courses in 2009, all in New Delhi for the present, as per the schedule below.

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.

- i) March 18-21, 2009.
 - ii) May 20-23, 2009.
 - iii) July 15-18, 2009.
 - iv) October 28-31, 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: captstbyagi@yahoo.co.in
