International Council for Security & Safety Management

Newsletter: October 2013

Let's professionalize the professionals…

http://www.wix.com/sbtyagi/iciss

68 Dead And 175 injured From 14 Nations: Details of Kenya Terrorist Attack Victims begins to emerge…

All security and safety fraternity in the world must feel the pain and anguish felt by the members of ICISS. The pictures above could have been from any country facing the menace of terrorism! Be it 9/11 in USA or 26/11 in India or even 22/9 at Kenya, the fanatics have spread mindless massacre in which victims were innocent and helpless unarmed / unprepared citizens! Kenyan President Uhuru Kenyatta - who has lost relatives in the attack - reiterated his government's determination to continue fighting Al-Shabaab. 'We... went into Somalia to help stabilize the country and most importantly to fight terror that had been unleashed on Kenya and the world,' he said. 'We shall not relent on the war on terror', he said. In ICISS we appreciate the sentiments and commitment indicated in the statement and hope same will reverberate and echo from all the corners of the world wherever the terrorism has played havoc!

At least 68 people killed in attack at Westgate shopping Centre. Somalian terrorist group Al-Shabaab - which has links to Al Qaeda - claims responsibility for attack on Saturday, 22nd Sept.13. 'If they found me, I'm white... so I'm dead': Survivors reveal how gunman executed non-Muslims - after asking them to name Prophet Mohammed's mother. Survivors said they saw fellow shoppers mercilessly executed after being singled out as non-Muslim. Shoppers said people were lined up and gunned down for failing to recite passages from the Koran.

Officials said Tuesday it was possible that a woman from Northern Ireland whose husband blew him up in the July 7, 2005, terror attacks on London's transport system was among the Al-Shabaab militants behind the siege on the Westgate mall in Nairobi, Kenya. On Monday, 24th Sept 13, the Kenyan Foreign Minister Amina Mohamed told PBS that two or three U.S. nationals and one British woman were among the attackers in the siege and hostage drama. Mohamed said the woman involved had, "done this many times before," adding weight to the speculation that Samantha Lewthwaite, who security officials believe did travel to East Africa, and specifically Somalia, several years ago. She is wanted in Kenya for involvement in an alleged terror plot to bomb locations on Kenya's coast last year. Lewthwaite was dubbed the White Widow after her husband blew himself up on July 7 in London. She converted to Islam as a teenager.

S B Tyagi
For ICISS

Security at Malls

Shopping Malls and other soft targets should increase security measures and update emergency response plans in the aftermath of the Kenyan mall massacre that killed at least 72 people.

While overall security at so-called soft targets like sports arenas, hotels, restaurants, movie theatres and housing complexes has increased dramatically in recent years, Saturday 22nd Sept.13 mass shooting in Nairobi should have an immediate impact among those who safeguard such commercial and residential locations.

“They see the attention that this receives and that’s what terrorists want,” said one security expert.. “They want this kind of coverage; that’s why they call it terrorism. They’re getting maximum bang for their buck from a marketing standpoint. That’s kind of a perverse way to look at it, but there’s no stealth involved.”

The primary challenge to secure a shopping mall is to maintain a sense of openness while simultaneously employing a high level of security measures like surveillance cameras, guards, adequate lighting. Utilizing the overall design of the property, particularly near primary access points, is also crucial to the “dynamic discipline”.

Typically, incidents like purse snatchings and flash mobs are the type of crimes on the minds of mall security personnel, but at least three U.S. malls have been the scene of mass shootings since October, most recently in April when an 18-year-old man wounded two at a mall in Christiansburg, Va. The deadliest U.S. mall shooting in history occurred in Dec. 5, 2007, when nine people, including the gunman, died at the Westroads Mall in Omaha, Neb. There have been similar incidents at Noida, India and other parts of the world.

“We have quietly added different measures to make what was considered a soft target a little harder,” one mall owner said. “We recognized a long time ago that shopping malls are soft targets.” Besides owners, individuals also bear some of the responsibility for their safety at soft targets like malls. Here the importance is stressed of identifying a “safe haven,” or a previously-identified location that can provide protection in the event of an emergency. “Identifying those places to and from work, or during your morning routine, is a great idea," one expert says, "But all too often, people don't have a plan." Restaurants make great safe havens, he said, since they can normally accommodate large crowds, have basic first aid materials and access to food and water.

In what could be a first anywhere in the world, the Mumbai police plan to grade malls across the city by their security-preparedness.

As they receive large crowds, malls have always been considered potential terror targets. Now, with the attack on the Westgate Centre Mall in Nairobi by militants loyal to Somalia's al Shabaab group, the police want to expedite their plans. "The attack… is an unfortunate example of how malls are soft targets. They have multiple entry and exit points and are crowded throughout the day. This makes securing them a mammoth task. Grading them will keep their owners on their toes," a senior police officer told. There are roughly 24 mega-malls in Mumbai. They will be graded from A to F, with category 'A' denoting the best. If the grade is low, the owner will be warned. Consistent breaches in security will result in revocation of license. "This is the first time a government agency is doing such a rating. If a mall is graded poorly, it may lose its patrons. The owner could also lose his license. So we expect that the desire to meet security requirements will be high," said a source in the Mumbai police.

The police will use 25 parameters for grading. These include security at entry and exit points, CCTV coverage, evacuation plans, employee verification, the deployment of a licensed security agency, the ability of police decoys to breach security and the number of mock drills done. Surprise checks by the police have thrown up shocking results.

This year, 145 police decoys were sent to breach security in malls. Of these, 89 managed to enter the premises with explosives or weapons. "Though almost all the malls in the city have metal detectors and frisking mechanisms in place, our success rate in breaching their security has been more than 75 per cent. The figures are shocking. We have time and again written to the malls to upgrade their security but they have failed to do so," said a police source.

"Our mind-set needs to be preventative, not reactionary,"

http://www.thehindu.com/news/national/other-states/mumbai-malls-to-get-security-rating/article5164832.ece

Embracing Global Change and Paradigm Shift – Being an Intelligent and Secure Organization for the Future!

D.C. Nath, IPS (Retd.), PPM, IPM

About the Author:

Mr. DC Nath is Chief Patron of International Council of Security & Safety Management. Superannuated in January, 1995, as the Special Director, Intelligence Bureau, Mr. D.C. Nath (IPS-1960) has been a visiting faculty to a number of Institutes (like the Indian Institute of Public Administration (IIPA), Sardar Vallabhbhai Patel National Police Academy (SVPNPA), Lal Bahadur Shastri National Academy of Administration (LBSNAA) and Academies, including Management Training Institutes, covering different aspects of security and industrial security management.

Winner of both the honors available in the police service, namely, Indian Police Medal for meritorious services and the President's Police Medal for distinguished services, and the Prime Minister's Silver Cup Essay Competition at the National Police Academy in two successive years, Mr. Nath had made a very significant and highly-appreciated presentation at IIM, Lucknow, on "Image Building for IPS Officers" at the Vertical Interaction Program for senior IPS officers.

The author of a highly acclaimed book, "Intelligence Imperatives for India", Mr. Nath earned high plaudits from all around for two of his very significant presentations on: "Revisiting the Future of India" (2005, London) and "Lessons from India for the War On Terrorism" (2007, USA). Known for his professed training ability, he is affectionately addressed as the "Dronacharya" and is considered a security ideologue.

His name figures in the American Police Hall of Fame, a Trust of the US National Association of Chiefs of Police. In December 2010, the International Who's Who Historical Society included his name in the 2010-2011 edition of the "International Who's Who of Professionals". All this indeed speaks volume about Mr. Nath's standing in the field of private security all over the world. Thus, in more than one sense, he is the only one in the field, combining the experiences of a police officer with specialization in intelligence and strategic analysis and an industrial security expert par excellence.

It is necessary to know and appreciate what is the threat or challenge before us today – both as human beings per se and as security professionals in particular. The concept of a conventional war between two countries is now considered a passé. So has observed John Horgan, Director of the Centre for Science Writings at Stevens Institute of Technology, in a brilliant write-up, "The End of The Age of War", appearing in the Newsweek Special Edition – Issues 2010: "War seems to be a cultural phenomenon, which culture is now helping us eradicate. Some scholars even cautiously speculate that the era of traditional war – fought by two uniformed, state-sponsored armies – might be drawing to a close." "War could be on the verge of ceasing to exist as a substantial phenomenon," said John Mueller, a political scientist at Ohio State University.

The real threat today comprises continued acts of violence, state-sponsored or otherwise in different parts of the world, more popularly described as acts of terrorism. Transnational terrorism is the real threat today before all of us. Notwithstanding the fact that so many advanced countries spend fortunes in military spending, "The past year saw increasing threats to security, stability, and peace in nearly every corner of the globe," the Stockholm International Peace Research Institute recently warned. Many nations and countries are now in fact faced with the phenomenon what can be best described as 'globalization of violence', be that genuine liberation movements or motivated groups practicing terrorism covered by a very thin veil of political pretensions.

Coming down to more specifics - even though unanimity of opinion is still lacking over the definition of terrorism, common refrain in all understanding or analyses of terrorism, veers round to what is described as jihad or jihadi terrorism. Jihad is a war or struggle against unbelievers and is waged by a number of groups owing allegiance to Islam. This was proved most emphatically in the 26/11 massacre at Mumbai (India). Reputed international commentators have described it as the seminal event in the history of international terrorism and particularly in the history of global jihad.

> "It would be a gross error to treat the terrorism facing India — including the terrible recent atrocities — as simply a problem for New Delhi alone. In a very real sense, the outage in Bombay was fundamentally a species of global terrorism not merely because the assailants happened to believe in an obscurantist brand of Islam but, more importantly, because killing Indians turned out to be simply interchangeable with killing citizens of some fifteen different nationalities for no apparent reason whatsoever."
>
> **- Mr. Ashley J Tellis, Senior Associate, Carnegie Endowment of International Peace.**
> **(Indian Express – January 29, 2009)**

There is thus an imperative need to appreciate the precise nature of the threat which marks the major paradigm shift in the history and growth of terrorism. One has to acknowledge this unambiguously. It is now global or universal jihad, which is a threat to all free world countries and it is a war that can be won only if we acknowledge that it is a war against humanity. Unless this is appreciated in the correct manner, the entire approach to handle terrorist threat could be faulted. Perhaps it is this lack of political will, to call a spade a spade is causing such enormous problem today in Pakistan which is at the receiving end from the Talibans. Much of the problem in India also could be attributed to the lack of admission of reality and feeble attempts at taking cover in the name of functioning in a democratic form of government. LeT is now the virtual substitute for Al-Qaeda with Yemen as the latest base station. The United States of America and UK have also been warned of 26/11-like acts of terror. The problem there has become more complex because such threats are no longer posed by non-state actors from outside but are also from home-gown terrorists, a fast emerging phenomenon. Female participation in jihad adds a further and new dimension. "A significant development in women participation in the global jihad has been the dissemination of radical ideologies on-line", writes Mia Bloom in a draft of her forthcoming book, "Bombshell: Women and Terror" (Time, February 1, 2010).

Another major paradigm shift is in the technique of perpetrating acts of terrorism. Apart from perfecting the art of suicidal Fedayeen attacks, there has been tremendous sophistication in the methodology being adopted by the terrorists. There has also been substantial qualitative improvement in the profile of the terrorists involved, as revealed in the analysis of the character and antecedents of those involved in 9/11 or the series of terror attacks in India, involving educated and technically equipped youth representing the Student Islamic Movement of India (SIMI).

Talking about the 9/11 group, Steve Coll, a Pulitzer Prize Winner, has said in an interview, "those guys were not nuclear physicists but they were well-educated, smart, determined, careful and willing to learn." He further added that while AL Qaeda had thus been able to put together really talented people, Lashkar's style of talent is more worrying. Some of the proselytizing networks have been able to recruit and radicalize scientists, doctors and other such talented people from here and there, as seen in 26/11. They can wreak a lot of havoc. (Steve Coll, Pulitzer Prize Winner, The Indian Express, New Delhi, January 26, 2010).

There has been a distinct trend in exploiting knowledge gathered from information technology, as seen in a spurt in the number of websites, which were earlier hosted for raising funds but now are being used for offering training and dissemination of ideology and other technical know-how. Steganography, that is, sending coded messages through pornographic pictures, was adopted in the December 13-attack on the Indian Parliament. Threat of cyber-attack has indeed pushed the United States to plan for independent Cyber Command. This is nothing but the real case of power of information technology, another paradigm shift!

A new and vital paradigm shift in approach to tackle terrorism should, therefore, lie in spending more time and thought on preventing terrorism to grow or take roots and tackle it with a long term perspective and with societal participation. As it is said, security is business of all, for all and by all. That is why it is recommended that the corporate world should try to educate its employees in the matter of security concerns by way of encapsulating security doctrines in their corporate social responsibility (CSR) policy. Employees will then help build up the national resilience against all forms of security threats including terrorism.

The paradigm shift in approach to tackling terrorism problem today really lies in the concept of public-private partnership. Countering terrorism is not just a job for the security and intelligence services. Yes, there is indeed an imperative need for improving infrastructure and intelligence gathering. The difference between victory and defeat has been rightly described as availability of good intelligence or the absence of it. Such good intelligence could really come up and be built through the module of perfect public-private partnership. Intelligence is the backbone of all political stability which can in other words be put as the by-product of good internal security mechanism. Modules of private-public partnership have been very successfully worked out in the UK through Project Argus and Project Griffin.

Project Argus relates to “resilience planning”. “Responding to a growing concern amongst business for a need to be prepared in the face of terrorism and to bring vast public and private sector expertise together, London First has established a growing Business Security and Resilience Network since 9/11. The Network brings employers, police and government emergency planners together to share expertise and encourage co-ordination of business continuity activities across sectors. Members are also linked up to London-wide fast-time incident alerts as well just launching a quarterly political and fraud intelligence briefing service.”

Project Griffin deals with how police can take advantage of the bulk of private security force available in the country. It is a community outreach program institutionalizing cooperation between the police and private security agencies under three basic formats, within the overall scheme of Counterterrorism measures known as Preventing Extremism Together (PET). These modules are being implemented in many other countries.

It is, in this context, incumbent on the corporate world to undertake security audit and then undertake risk management study, not only to get the Return on Investment (RoM) but also to ensure what is popularly known as business continuity planning. Diligent business continuity planning leads to saving of expenditure. That will also lead to real convergence of both business interests and security interests. If a forward-looking business entity spends money on modernization of its management technology and on methods of improving production technology, why cannot it also think in the present-day security ambience of spending money on modernization of security technology, investment of some money on research relating to security management?

Investment in security will never go waste. Unfortunately, management often forgets that security is amongst its vital tools to increase operational or functional efficiency and thus to increasing production under secure conditions. This paradigm shift is also essentially called for.

The Americans have, therefore, been advised, “By treating terrorism as a hazard to be managed by all Americans, terrorism can also be starved of its ability to generate dread, panic, and paralysis. Terror works only if it convinces people they are vulnerable and powerless. By being candid with the American people, about the threat they face, and by giving Americans ways to address their vulnerabilities – such as providing detailed guidance on what suspicious activities to report and encouraging citizens to get emergency preparedness training – Washington could make terrorism far less terrifying.” (Stephen Flynn, President of the Centre for National Policy in Washington, DC), Newsweek Special Edition, 2010.

It is also worth noting in the same context what has been suggested for the most ticklish terror-ridden country Afghanistan: “The White House says it understands that the solution to the war in Afghanistan is not purely military. Officials have declared a concomitant “civilian surge” of experts to bolster the embattled country’s bureaucracy and economy along with the greater number of troops. But if the U.S. is truly committed to long term security and stability in Afghanistan, it should be investing in the one pivotal sector that has received scant attention from the international community: education.” (Commentary: Learning Curve, Argon Baker, Time, January 25, 2010).

Thus, in order to build up an intelligent and secure organization for the future, it is not enough to revitalize the internal security mechanism or even reforming the entire criminal justice system in a country. Equally, if not more, important will be to help develop the spirit of national resilience through a carefully structured public-private partnership, educating the people at large and thus leading to the creation of what we would like to call “good citizens.” The concept of ‘good citizen’ has to take root in the manner envisaged in Article 51-A of the Constitution of India, spelling out the fundamental duties of the people. All of us need to embrace and imbibe that culture and the spirit in toto and that is the mantra for success and survival.

Invest In Security Today For Stress Free Tomorrow

Making of Security Force More Effective to Protect Industrial Installations

Security is a vital function of fostering an appropriate environment conducive for development and growth. In the wake of growing security concern at national and international levels, it has become imperative for all the establishments including industrial entities to upgrade and modernize the security systems for effectively meeting the growing challenges.

Security is not any more regarded as peripheral function entailing additional expenditure to the organization but is considered as a critical and integral part of the organization for the prevention of loss that the organization might suffer in absence of effective security system. This is contrast departure from traditional approach which management uses to have only few years back. Any forward looking management with sincere concern for the security of plant and personnel has either changed their approach or is in the process of changing it with the understanding that security is no more side function but it is main line function with bearing on organization’s productivity and profitability.

Why management must invest in Security

It is the duty of management to protect the personnel and property of the installations by having necessary security infrastructure. It is erroneous impression that security is responsibility of the security officers and not of the management. Security officer is to advise the management on security matters and implement their directives and instructions. Thus management will be well advised to appreciate security related proposals in earnestness and lay importance to best security practices. The security measures need to be constantly upgraded and this must be taken as investment and not expenditure, for secure work environment today will be harbinger of stress free tomorrow full of prosperity.

Industrial Security not only increases the profitability and productivity or the organization, it also increases the trust and confidence of investors and the common people at large. Market perceptions and credibility is known to have changed drastically soon after major breach of security or industrial accidents. Prudent management, therefore, lays emphasis on cost -effective yet un-breach able security plans. Industry needs to be ready to not only handle disaster in any form but should also needs to be capable of foreseeing them and keep such eventualities as part of their planning. The rapid pace of progress allows less opportunity for learning by trial, making it necessary to get design and operating procedure right from the first time. With this philosophy, the industries must also plan for the faster recovery, should at all a disaster occur.

Public concern at multiple injuries and deaths from spectacular events such as a major explosion invariably leads to calls for additional control. It is therefore important particularly for projects involving the storage and use of hazardous chemicals to address both on-site and off-site security when deciding on security measures to be applied. Rapid growth in industrial field has brought a significant increase in number of people both workers and members of general public whose life could endanger at any point of time by accident involving hazardous materials and processes.

“Security Preparedness is war-like exercise and like war, it decides not who is right, but, who is left!”

Website scams

Click fraud

The latest scam to hit the headlines is the multi-million dollar Clickfraud which occurs when advertising network affiliates force paid views or clicks to ads on their own websites via Spyware, the affiliate is then paid a commission on the cost-per-click that was artificially generated. Affiliate programs such as Google's Adsense capability pay high commissions that drive the generation of bogus clicks. With paid clicks costing as much as $100 and an online advertising industry worth more than $10 Billion, this form of Internet fraud is on the increase.

International modem dialing

Many consumers connect to the Internet using a modem calling a local telephone number. Some web sites, normally containing adult content, use international dialing to trick consumers into paying to view content on their web site. Often these sites purport to be free and advertise that no credit card is needed. They then prompt the user to download a "viewer" or "dialer" to allow them to view the content. Once the program is downloaded it disconnects the computer from the Internet and proceeds to dial an international long distance or premium rate number, charging anything up to US$7-8 per minute. An international block is recommended to prevent this, but in the U.S. and Canada, calls to the Caribbean (except Haiti) can be dialed with a "1" and a three-digit area code, so such numbers, as well as "10-10 dial-round" phone company prefixes, can circumvent an international block.

Phishing

"Phishing" is the act of attempting to fraudulently acquire sensitive information, such as passwords and credit card details, by masquerading as a trustworthy person or business with a real need for such information in a seemingly official electronic notification or message (most often an email, or an instant message). It is a form of social engineering attack.

The term was coined in the mid-1990s by crackers attempting to steal AOL accounts. An attacker would pose as an AOL staff member and send an instant message to a potential victim. The message would ask the victim to reveal his or her password, for instance to "verify your account" or to "confirm billing information". Once the victim gave over the password, the attacker could access the victim's account and use it for criminal purposes, such as spamming. Phishing has been widely used by fraudsters using spam messages masquerading as large banks (Citibank, Bank of America) or PayPal. These fraudsters can copy the code and graphics from legitimate websites and use them on their own sites to create legitimate-looking scam web pages.

They can also link to the graphics on the legitimate sites to use on their own scam site. These pages are so well done that most people cannot tell that they have navigated to a scam site. Fraudsters will also put the text of a link to a legitimate site in an e-mail but use the source code to links to own fake site. This can be revealed by using the "view source" feature in the e-mail application to look at the destination of the link or putting the cursor over the link and looking at the code in the status bar of the browser. Although many people don't fall for it, the small percentage of people that do fall for it, multiplied by the sheer numbers of spam messages sent, presents the fraudster with a substantial incentive to keep doing it.

Pharming

Pharming is the exploitation of vulnerability in the DNS server software that allows a hacker to acquire the domain name for a site, and to redirect that website's traffic to another web site. DNS servers are the machines responsible for resolving internet names into their real addresses - the "signposts" of the internet.

If the web site receiving the traffic is a fake web site, such as a copy of a bank's website, it can be used to "phish" or steal a computer user's passwords, PIN or account number. Note that this is only possible when the original site was not SSL protected, or when the user is ignoring warnings about invalid server certificates.

For example, in January 2005, the domain name for a large New York ISP, Panix, was hijacked to a site in Australia. In 2004 a German teenager hijacked the eBay.de domain name.
Secure e-mail provider Hushmail was also caught by this attack on 24th of April 2005 when the attacker rang up the domain registrar and gained enough information to redirect users to a defaced webpage.

Auction and retail schemes online

Fraudsters launch auctions on eBay or TradeMe with very low prices and no reservations especially for high priced items like watches, computers or high value collectibles. They received payment but never deliver, or deliver an item that is less valuable than the one offered, such as counterfeit, refurbished or used. Some fraudsters also create complete ‘web stores’ that appear to be legitimate, but they never deliver the goods. In some cases, some stores or auctioneers are legitimate but eventually they stopped shipping after cashing the customers' payments.

Sometimes fraudsters will combine phishing to hijacking legitimate member accounts on eBay, typically with very high numbers of positive feedback, and then set up a phony online store. They received payment usually via check, money-order, cash or wire transfer but never deliver the goods; then they leave the poor, unknowing eBay member to sort out the mess. In this case the fraudster collects the money while ruining the reputation of the conned eBay member and leaving a large number of people without the goods they thought they purchased.

Stock market manipulation schemes

These are also called investment schemes online. Criminals use these to try to manipulate securities prices on the market, for their personal profit. According to enforcement officials of the Securities and Exchange Commission, the 2 main methods used by these criminals are:

Avoiding Internet investment scams

The Internet allows individuals or companies to communicate with a large audience without spending a lot of time, effort, or money. Anyone can reach tens of thousands of people by building an Internet web site, posting a message on an online bulletin board, entering a discussion in a live "chat" room, or sending mass e-mails. If you want to invest wisely and steer clear of frauds, you must get the facts. The types of investment fraud seen online mirror the frauds perpetrated over the phone or through the mail. Consider all offers with skepticism.

Internet Crimes: Stealing band-width

There are many "don't steal my bandwidth" pages on the web. They are often long winded and hard for the novice or even the experienced web designer to understand. "Don't Even Think About It" is short and to the point. You will know what stealing bandwidth is in the 3 short minutes it takes you to read this page that is written without any sugar-coating at all.

What is Stealing Bandwidth?

There are many forms of bandwidth stealing on the web today. However, the bandwidth theft focusing on here is image/graphic stealing, and is the bandwidth theft that occurs most. That is when you find an image you like and you are:

1. Too cheap to have server space of your own to use -and/or-
2. Too lazy to upload the image to your own server -and/or-
3. Uneducated about the crime you are committing -or all of the above-Crime?

Yes, it is a crime. The person whose site the image is on that you are linking to for the source of the image is paying to display their image on your site.

First of all, the image belongs to them, not you. What right do you have to say; "Oh, wouldn't this look great on my site?" and just copy the image URL and use it on your site. You have no right at all. It is not your graphic. Even if it is a very common graphic, for example a bullet or an arrow, and you have seen it on many sites. The operative word here is "on." Get it? It is on a site.

That site owner is paying one way or another to have that graphic displayed on the web. Perhaps they pay a monthly fee. Perhaps, they use a 'free' web service, however, they have limits on the amount of bandwidth they are allowed to use. By linking to the graphic, YOU have STOLEN from them one way or another. Secondly, if it is an original graphic that the site owner designed them self, and you link to the source of the graphic to be displayed on your site, you are not only stealing the bandwidth, you are now plagiarizing their work too.

It seems a big culprit these days are the "community" type websites (MSN Groups & Yahoo groups are a fine examples). A person can easily set up a little web site lickety-split - and it's even faster when you link to the source of the graphics you have seen on the web & like rather than uploading them in YOUR space. Not to mention writing to the owner of the graphic and asking their permission first. People do this because it is a fast and cheap way to put something up quickly. In doing this, you are stealing!

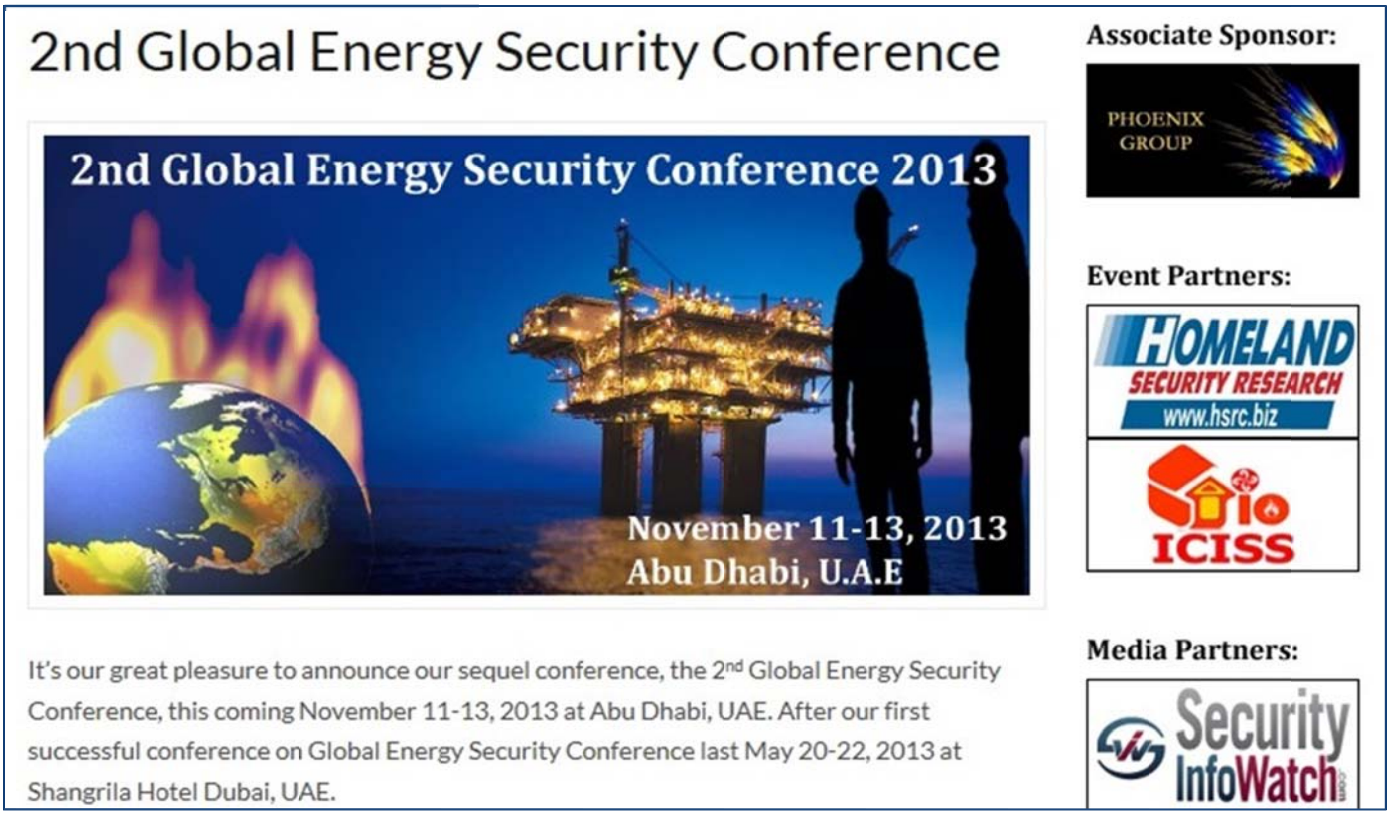
One other area that is festering boil for bandwidth stealing are the Bulletin Boards that offer the members an ability to have a cutesy little icon next to their name. People remember that cute little picture of a dancing potato they saw on a web site and link to the image source for their member icon. Now, the site owner who's dancing potato graphic you are linking to is looking through their server logs and see 15,048 hits to this one little graphic. "What the heck," they say in disbelief! Or, they get a notice from their 'free' web site host telling them that they have exceeded their allowable bandwidth for the month and their site will be shut off OR they have to pay extra money to keep it up.

Bottom line, if you want to use a graphic on your site, you must do these things: write to the site owner of the graphic that you would like to use on your site. •>ASK<•, repeat ASK them if you can use that graphic on your site. If they say yes, then thank them and be certain to thank them in the credits of your site. If they say no, swear a bit under your breath but under no circumstances do you link to the graphic thinking that "I'm not really using it on my site, since it is not on my server. Leave it alone and go find something else instead.

Does this text make you angry or are you grinning ear to ear? If you are feeling angry, you are one of those snatch and grab people who take what they want and say the heck with the rules. If you are smiling ear to ear, you are a site owner who is glad to see the text you have just read. It is in plain English and not sugar coated in any way. PhenomenalWomen.com understands this because so many images on this site are linked to and bandwidth stolen daily.

A warning: many site owners can track down and pinpoint exactly where their images are being used on other sites. When that happens, you will be in trouble. If you are new to the web, take the advice of this page as your first lesson and don't forget it.

Upcoming Event


2nd Global Energy Security Conference 2013
November 11-13, 2013
Abu Dhabi, U.A.E
PHOENIX GROUP
HOMELAND SECURITY RESEARCH www.hsrc.biz
ICISS
Security InfoWatch.com

2nd Global Energy Security Conference

It's our great pleasure to announce our sequel conference, the 2nd Global Energy Security Conference, this coming November 11-13, 2013 at Abu Dhabi, UAE. After our first successful conference on Global Energy Security Conference last May 20-22, 2013 at Shangrila Hotel Dubai, UAE.

Associate Sponsor:

Event Partners:

Media Partners:

For more details, please visit - http://www.pcstconsultant.com/2nd-global-energy-security-conference/

P.S. - If you don't like to receive our newsletter, we apologize for bothering you. Please let us know your mail address and we will move it out from our contact list, thank you!