International Council For Industrial Security & Safety Management

Newsletter: January 2011

Let's professionalize the professionals...

New dawn awaits new beginning!
New beginning entails new commitments!
New commitments mean new ideas!
New ideas bloom new talents!

The dark night which was pregnant with gory past and gloomy future miraculously heralded the day of promise, progress and prosperity!

Let new initiative bring renewed commitment to profession and let all the Security and Safety Professionals attain satisfaction in whatever they do in their chosen profession!

Let's professionalize the Professionals!

Capt S B Tyagi
For ICISS

Happy New Year!

Happy Republic Day!

FOOD FOR THOUGHT:

After terrorist acts, can the Government work silently with eloquent results!

Reflections on the Security Management Profession

Cynical realism is the intelligent man's best excuse for doing nothing in an intolerable situation - Aldous Huxley

Security professionals in the industrial, financial, retail (loss prevention), consumer products or manufacturing sector remain clustered in their particular iron-clad circles. If you want to see the effects of this isolation just take a closer look at your professional group's local chapter participation. For the most part the membership rosters are far outstripped by attendees at scheduled events, when most information sharing is expected to take place. You'll also notice that lack of interest in direct volunteering and involvement is sometimes affected by a desire to remain independent and guard our play book a bit closer.

For better or worse there appears to me that security as a profession is limited by the protectionist realities of its practitioners. Protection being the bread and butter of our business, it also rules our conscious and subconscious environment and how we must relate to one another in furtherance of our goals on behalf of clients. Let me explain what I mean by this line of thought; we share information related to the protection of people, assets, reputation and brands through a medley of trade groups and networking mediums, but rarely do this information sharing rises to the level of objectivity needed to be applied as a solution to problems confronted by our colleagues. That is because a number of issues come into play; if a colleague happens to be at a competing organization we would be prohibited from sharing material information under non-disclosure agreements and other information protection tools. The same information may not only be leveraged competitively from one organization against another, but also from one professional against another.

I do recognize that there are other overarching forces (mainly client demands, deadlines, or lack of resources) influencing direct participation in trade group events, but little has been said about the more obscure reality of protectionism. With the advent of social media we're now more connected than ever; which means that more information is being shared among professionals, especially from some of the most secretive colleagues among our ranks.

After actively participating in a number of these social media outlets I realize two important facts:

- I know more about my colleagues' past experiences and therefore their expertise than ever before, as well as
- That there is less movement across industry lines than I realized.

For example, there aren't many security professionals with experience in the real estate/facilities industry going over to the large construction or engineering firms, which at face-value may appear to have much in common. Because of our ingrained guarded behavior, we lack the ability to recognize where our mutual professional interests coincide. It is furthermore, representative of the lack of information exchange between security professionals with shared protection interest.

It is also understood that in a tough job market security management candidates would be pitted against one another based on the value of their information resources, but there is much more to be gained by pooling together our collective interests in a way that would not compromise practitioner-client privileges, and would otherwise strengthen our ranks. As we stand today, our realities as security professionals are therefore ruled not by the commonality of our interests, or concerted action for that matter, but more distinctively by our competitive advantages. Information is the commodity that needs to be protected, plied and used to further our objectives in an ever more competitive environment. That stark contrast is more prevalent in the security profession than other such trades and our stature within organizations is hurt by it.

There are no right solutions to this issue, but as a matter of course we can start by sharing our thoughts on this perceived problem. My own view is that we need to reengineer the way our trade groups operate with the aim of offering more meaningful ways to nourish our ranks with coaching, mentoring and organizing a roadmap to fill our leadership pipeline. Perhaps the magic element that is missing in all of this is trust and that, I'm afraid, is not being cultivated enough.

The tragedy caused by the Manila Hostage-taking incident has after all taught us lessons worth remembering

For others, August 23, 2010 was just an ordinary day, but in Manila (Philippines) the day ended with a bloody finish. Lives were lost as a former police personal held a group of Hong Kong tourists' hostage. We understand lives were lost and we would like to extend our condolences to the families of the eight tourists who died in this tragic hostage-taking incident.

They say let's learn from other people's mistakes so we don't have to experience those ourselves. In line with the hostage-taking that happened in Manila, there are so many lessons we can learn from the said incident.

Media Management

It can be observed that the media coverage by the different networks was very detailed that the public need not know most of them. In addition, it was also aired that the hostage-taker was watching the news the whole time. When he saw his brother being arrested by the police and that was when he got agitated and started firing.

The assault team also had a hard time strategically positioning the team because they were blinded by the heavy lights of these television networks. From the inside, the hostage-taker could easily spot where his enemies are because they were very visible.

I therefore recommend, the authorities should have standard operating procedure-involving the Media for situations like this, especially when security and safety of the majority is as stake.

Crowd Control

During a hostage situation police officials should assign a crowd control unit. If so this should be strictly implemented. During the hostage-taking, the people watching had interfered in the actions of the assault team. They were not able to position themselves strategically because civilians were everywhere. They had to also look after the safety of these bystanders, wasting precious time which could have been allotted to resolve the situation.

Talking about the safety, there was one civilian who was wounded because of the stray bullet that hit his foot. In situations like the said hostage-taking incident, you can never predict what could potentially happen, so instead of risking your life, you would rather opt to stay away from the vicinity.

Avoiding Strangers

To all the tourists and those who are still planning to visit other countries, it is advised to never trust a stranger, especially when this stranger is armed with high-caliber pistols. Yes, it is possible that the passengers trusted this ex-police because he was wearing his uniform. Nevertheless, it is still not recommended to allow him to hitch a ride with you.

With all these lessons, the police unit needs a major role here. Tragic as it may be, we seriously hope that would be the last hostage-taking in the Philippines or anywhere in the world. Let's us all pray for world peace and pray for those people who are having serious problems. May they be able to surpass whatever those challenges, hope that evil works such as this will not even enter their minds?

Source:http://newsflavor.com/world/asia/lessons-learned-from-the-manila-hostage-taking-incident/#ixzz16fXVV3br

This week… Every week….

Don't make Security weak!

Speed guns can help cops detect Suicide Bombers

Researchers say that the wiring in a suicide vest would alter the radar cross section of a 'would-be' bomber enough to allow a radar speed gun to pick.

Radar guns used by police to spot speeding motorists could help identify would-be suicide bomber in a crowd, say researchers.

A radar gun fires microwave pulses at a car and measures the Doppler shift of the reflected signal to calculate its velocity. However, the strength and polarization of the reflected signal - the radar cross section - can provide additional information about the size and shape of the reflecting object and the material it is made from.

Researchers wondered whether the wiring in a suicide vest would alter the radar cross section of a bomber enough to allow a radar gun to pick him or her out in a crowd, reports New Scientist. To find out, William Fox of the Naval Postgraduate School in Monterey; California, and John Vesecky of the University of California, Santa Cruz, used software to simulate how radar signals at 1 gigahertz and 10 gigahertz would be reflected by the most common arrangements of looped wiring typically used by suicide bombers. They found that the clearest reflected signals were in the 10 gigahertz range. Together with colleague Kenneth Laws, they then fired low-power 10 gigahertz radar pulses at groups of volunteers; some wearing vests wired up like suicide vests. About 85% of the time, telltale factors in the polarization of the reflected signals allowed them to correctly identify a "bomber" up to 10m away.

The team now hopes that the US army will fund further development of the system, allowing them to boost the detection rate and include refinements to avoid false alarms being triggered by metal parts ill under-wired bras, jewellery and earphone leads.

The researchers suggest military checkpoints would be major users of such a system - but it could also be installed alongside CCTV cameras in shopping malls, railway stations, airports and high streets.

VIDEO CAMERAS CAN IDENTIFY TERRORISTS

New York: It sounds like something out of science fiction. Researchers at General Electric Co.'s sprawling research centre are creating new "smart video surveillance" systems that can detect explosives by recognizing the electromagnetic waves given off by objects, even under clothing.

Scientist Peter Tu and his team are also developing programs that can recognize faces, pinpoint distress in a crowd by honing in on erratic body movements and synthesizes the views of several cameras into one bird's eye view, as part of growing effort to thwart terrorism.

“We’re definitely on the cutting edge,” said Tu, 39. “If you want to reduce risk, video is the way to do it. The threat is always evolving, so our video is always evolving.”

Scientists at the GE complex, a landscaped, gated campus of laboratories and offices spread out over 525 acres and home to 1,900 scientists and staff, and others in the industry hope to use various technologies to reduce false alarms, cut manpower used on mundane tasks and give first-responders better tools to assess threats. The country’s growing security needs also provide an opportunity to boost business.

The United Sates and its allies now face a new “Iraq generation” of terrorists who have learned how to make explosive devices, assassinate leaders and carry out other mayhem since the U.S. invasion of the country more than three years ago, said Roger Cressey, a former counter-terrorism official in the Bush Administration who now runs his own consulting business in Arlington, Virginia.

“These people are far more adept and capable in many respects than Al-Qaida before 9-11,” he said. “They don’t appear in any no-fly list or terrorism data base.” Since 2002, GE has spent $4 billion buying smaller businesses to take a bigger share of the $160 billion global security industry, a market that includes everything from building security to narcotics detection.

The 7 Best Practices for Network Security

We all face it - the daily barrage of spam, now infested with zero-day malware attacks, not to mention the risks of malicious insiders, infected laptops coming and going behind our deep packet-inspecting firewalls and intrusion-prevention systems. Some even have to worry about how to prove steps of due care and due diligence towards a growing roster of regulatory compliance pressures.

What can you do under so much extreme pressure to make 2007 a better year, not a year loaded with downtime, system cleanup and compliance headaches? I've come up with what I would consider some of the best network security practices.

Best practices are things you do - steps you take - actions and plans. Within those plans, I'm certain you will include which security countermeasures to budget for in 2007. Although I thought about going into details about recent security concepts, such as unified threat management or network admission control, it seems more appropriate to focus on the seven best practices instead of the seven best security tools you might consider deploying. For example, I consider encryption a best practice and not a product or tool. I'm sure you'll find

many commercial and freely available tools out there. You can always evaluate those tools which you find most suited for your own best-practice model.

Here's a best practice list, in order of importance:

- Roll out corporate security policies
- Deliver corporate security awareness and training
- Run frequent information security self-assessments
- Perform regulatory compliance self-assessments
- Deploy corporate-wide encryption
- Value, protect, track and manage all corporate assets
- Test business continuity and disaster recovery planning

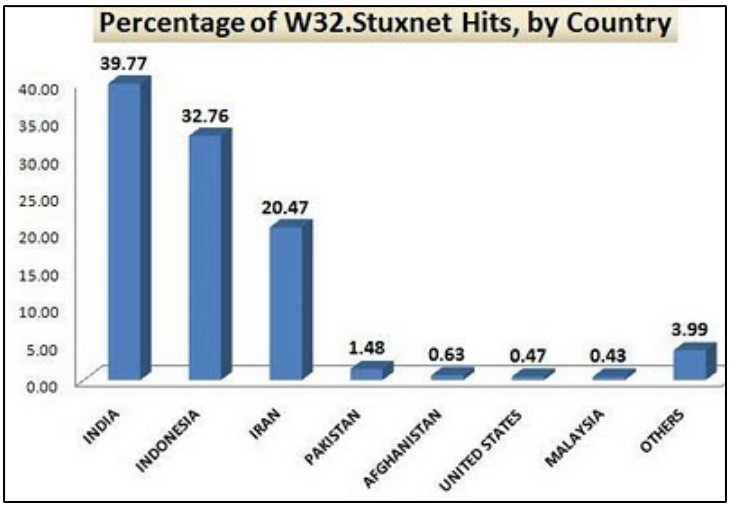
Stuxnet: The Cyber-Weapon Said to Target Iran's Nuclear Infrastructure

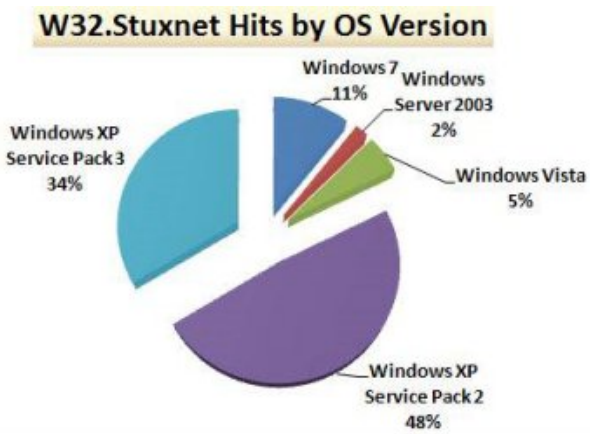
A programmable logic controller (PLC) is a specialized, self-contained computer system used in manufacturing and processing plants around the world.

Most PLCs utilize a diagrammatic programming language called "ladder logic", not dissimilar to traditional flow charts, to allow engineers to schedule activities, turn switches on and off, regulate work-in-process queues and perform many other functions using "code blocks".

For example, a refinery might employ a PLC to control the flow of oil and byproducts between multiple stages of the refining process. It would perform these tasks by opening and closing valves, reading level sensors, etc.

PLCs are often network-attached. The term SCADA (Supervisory Control and Data Acquisition) refers to a network of PLCs and related devices that are supervised by control systems.





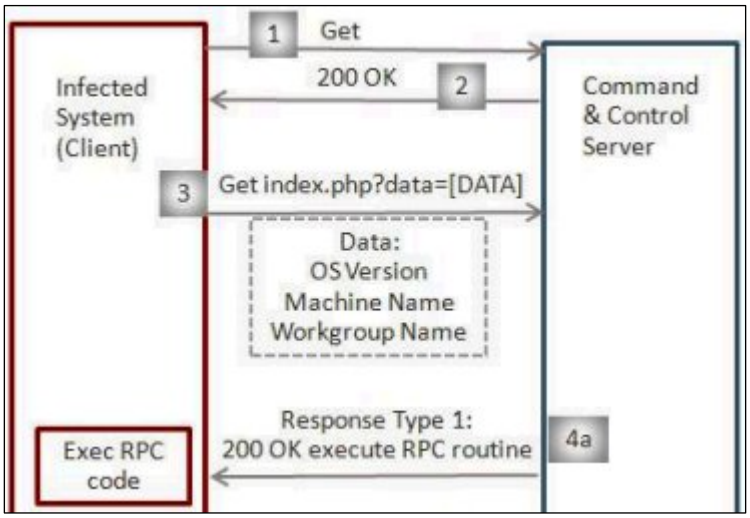
With that as a bit of background, let's rewind to July 2010. That month security vendors began warning of a new type of malware identified as either "Tmphider" or "W32.Stuxnet". The malware used a zero-day Windows vulnerability (involving .lnk or .pif shortcut files) to install both kernel- and user-mode attack software.

Virtually every version of Windows was vulnerable. But, interestingly, the malware had first been spotted infesting Siemens WinCC SCADA systems. Siemens makes one of the world's most popular lines of PLCs and was, as of a few years ago, reported to have a third of the world's market share.

When Stuxnet infects a Windows machine, it reports back to a C&C (command and control) server the following information within an encrypted HTTP request.

- The Windows version information
- The computer name
- The network group name
- Flag for whether SCADA software was installed or not
- IP addresses of all network interfaces

Symantec reports that the malware has some amazing capabilities targeting SCADA directly: "Stuxnet has the ability to take advantage of the programming software to also upload its own code to the PLC in an industrial control system that is typically monitored by SCADA systems. In addition, Stuxnet then hides these code blocks, so when a programmer using an infected machine tries to view all of the code blocks on a PLC, they will not see the code injected by Stuxnet. Thus, Stuxnet isn't just a rootkit that hides itself on Windows, but is the first publicly known rootkit that is able to hide injected code located on a PLC."



A previous historic example includes a reported case of stolen code that impacted a pipeline. Code was secretly "Trojanized" to function properly and only some time after installation instruct the host system to increase the pipeline's pressure beyond its capacity. This resulted in a three kiloton explosion, about 1/5 the size of the Hiroshima bomb.

Given the countries targeted -- Iran appears to be a primary 'beneficiary' of Stuxnet -

researchers speculate that the malware was designed to destroy the Islamic Republic's burgeoning nuclear infrastructure.

Home Security

Threat Assessment by you

If you have just bought your first house you are most likely full of ideas for making it your own. You might want to paint the rooms your favorite colors, hang a huge collection of different artworks and window dressings, and start planting lovely flowers all over the yard. Before spending a dime on such improvements, however, you will want to consider the security that you have in place first.

Before you say that you live in a "safe" neighborhood, and that security is needless, you should know a few valuable things. Firstly, a plan for home security is not only about the relative safety of a neighborhood, but is also about keeping a home safe from disasters such as fire, flooding, and more.

Secondly, robbery statistics indicate that there really are no neighborhoods that are not embattled by would-be criminals. The reasons that one neighborhood remains free of crime as opposed to another tends to be related to the security systems in the homes, and behaviors of the residents.

This doesn't indicate, however, that you have to pour every available dime into a home security system and for the purpose of this discussion we'll look at some effortless and proficient steps that can greatly weaken the appeal of your home to a robber.

The first thing to do is to consider buying window stickers and signs that indicate that a home alarm system is on the property. These are available for sale, even when there is no system installed at all, and these are often a major deterrent to a burglar. In fact, around 70% of convicted burglars say that they totally avoid a home if there is any suggestion of an alarm posted on the exterior of the property.

Second, as an amusing DIY (Do it yourself) project you may want to try to break into your own home. Yes, it may sound odd and like an invitation to be arrested, but only by trying to power your way into the house will you uncover its major weaknesses. For example, you may realize that a window at the back of the house is completely screened from sight, and this might make it a major focal point for a would-be burglar. You can then do everything in your power to make certain that the window is not so tempting. This might mean installing a motion sensor light near the area, or even adding a new lock to the window too.

One thing that most homeowners find out when performing such an assessment is that the entrance from an attached garage is dreadfully vulnerable. Most burglars know this too and will insist that if they can gain access to the garage, they can just walk right into the house. This means double checking that the connecting door is strong and fixed with a good lock. It also means ensuring that you cannot easily hop into the garage from a window or door as well.

None of the things mentioned above are expensive, and all of them are easy. They are sure-fire ways to prevent a burglar from taking the time to break into your home because they make the property very unappetizing as a target.

In Case of Emergency (ICE)

We all carry our mobile phones with names & numbers stored in its memory but nobody, other than ourselves, knows which of these numbers belong to our closest family or friends.

If we were to be involved in an accident or were taken ill, the people attending us would have our mobile phone but wouldn't know who to call. Yes, there are hundreds of numbers stored but which one is the contact person in case of an emergency? Hence this "ICE" (In Case of Emergency) Campaign! The concept of "ICE" is catching on quickly. It is a method of contact during emergency situations.

As cell phones are carried by the majority of the population, ***all you need to do is store the number of a contact person or persons who should be contacted during emergency.***

Store the no with names prefixed by "ICE". E.g.

First name – ICE Akhil
Last name - Pandey

This way all "ICE" (In Case of Emergency) will appear together.

The idea was thought up by a paramedic who found that when he went to the scenes of accidents, there were always mobile phones with patients, but they didn't know which number to call. He therefore thought that it would be a good idea if there was a nationally recognized name for this purpose. In an emergency situation, Emergency Service personnel and hospital Staff would be able to quickly contact the right person by simply dialing the number you have stored as "ICE." For more than one contact name simply enter ICE1, ICE2 and ICE3 etc.

Please share this with others. It won't take too many efforts before everybody will know about this. It really could save your life, or put a loved one's mind at rest.

Remember: ICE will speak for you when you are not able to!

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

Capt S B Tyagi, COAS' CC*, FISM, CSC, CSP

Digitally signed by Capt S B Tyagi, COAS' CC*, FISM, CSC, CSP
DN: CN = Capt S B Tyagi, COAS' CC*, FISM, CSC, CSP, C = IN, O = GAIL (India) Limited, OU = Deputy General Manager (Security)
Date: 2011.01.03 18:25:47 +05'30'