International Council For Industrial Security & Safety Management

Newsletter: June 2011

Let's professionalize the professionals...

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

The security sense is stronger in the weaker people – it has been said by the wise men! But present word exhibits that stronger the person, stronger is the desire for security!

The expenses on security by cash rich companies is matter of board room debates but the need for security by the poor companies which can ill afford it, has been professional debate for a long time.

Recent trend globally and more specifically in India indicates that preparing themselves for unforeseen security contingencies has eaten-up major share of corporate budget of well-to-do companies. Whereas the cash starved companies are looking at government to provide safe and secure environment conducive for their productive and profitable business activities. Though this is the sovereign responsibility, alas it has not materialized!

As a result there is boom time for economy but bloom time for security service providers. This paradoxical situation needs mid-course correction and balance needs to be maintained only when security preparedness is in commensuration with the threat perception. Let every security professional take note of this principle and their job will be treated as' well-done'!

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)
Reason: I am the author of this document
Date: 2011.06.09 14:24:16 +05'30'

Capt S B Tyagi
For ICISS

Food For Thought:

Like Good Strategy, Good Security begins before first move!

Make sure your Security Strategy addresses physical risks

Physical security starts with a rather simple basic premise: those who do not belong on your institution's property should be excluded from your institution. This may happen in three (often interrelated) ways:

- When those who do not belong are identified, stopped and denied admission by a person.
- When those who do not belong are denied admission by a physical device, such as a locked door.
- When those who do not belong are denied admission because they decide that your institution is too difficult to enter and thus they do not even try.

This section will consider the various methods of excluding those who do not belong:

- Access Control
- Key Control and Locks
- Protective Devices and Alarms
- Windows and Doors
- Fencing and Gates
- Protective Lighting
- General Deterrence

Creating and maintaining a fairly secure workplace can cost a lot of money. Security gadgets and systems don't come cheap! And don't forget about training guards and supervisors on how to operate and configure those systems and others in a secure manner - all the security devices in the world won't help your organization if your administration doesn't know how to properly use them.

But for most companies, the benefits gained in improved productivity, increased public confidence, and the lack of legal fees help maximize the return on investment (ROI) for these costs. However, even with all of these devices and software in place and properly functioning, there are still areas of improvement that can mean an even bigger ROI - specifically, physical security.

Don't overlook physical security

Many organizations spend thousands of dollars on the right devices and software, only to forget about securing the actual building that houses them. Remember: Even if no one can steal or corrupt your data over the network, they may still be able to walk out your front door with it.

Don't neglect physical security in your attempts to lockdown data. For example, many companies have no established policy or defined best practices when it comes to bringing in personal laptops or storage devices, both of which makes it easy to siphon off data from your network. Similarly, it is considered wrong for senior executives to use their cards of Access

Control System for their every ‘in’ or ‘out’ movements. Thus they are creating vulnerabilities for themselves and for others! Let's look at some other areas of physical security that require your attention.

Develop an entrance and exit policy

Take steps to establish a well-defined entrance and exit policy. It should spell out exactly which electronic devices people can bring into the building, exactly where in your building people can use those devices—anywhere they can't.

If your organization doesn't have such a policy, you need to develop one and distribute it to employees and business partners. Make sure it lists permitted devices, and outline how one would gain approval to bring such devices into the building.

Don't worry about being too specific about allowed devices - technology evolves faster than any policy. Rather than putting yourself in the position of having to constantly update the policy, address general types of devices instead. Similar policies need to be put in place about the movements of files and documents inside or outside the premises.

Lock down your equipment - literally

Developing an entrance and exit policy offers a good opportunity to consider how you secure the devices you already have. For example, have you installed locks on workstations and servers to prevent the theft of hard drives? Do you have cable locks for laptops so they don't walkout the building?

Laptops definitely aren't cheap, and they can store an enormous amount of data. Same is the case of pan-drives and external hard-drives.

EMERGING SECURITY TRENDS

The nature of world-wide espionage is currently experiencing a dramatic shift. A recent analysis of trends suggests the need to redefine the problem and to develop new strategies to combat growing threats to national security from economic intelligence gathering and corporate espionage. If left unchecked, analysts estimate losses could grow an additional 50% by the year the next year.

A New National Security Perspective

The rapid pace of change in the post-Cold War era demands a new definition of national security issues. The development of the European Community, break up of the Soviet Union, economic and political shifts within the former Warsaw Pact nations, the reunification of Germany, and the brisk economic growth of Pacific Rim countries have led to a new world of opportunity and threat.

The challenge to the intelligence community is to discern and disrupt economic espionage directed towards national companies and interests. A fundamental shift in our understanding and protection of the nation's secrets will require:

- Redefining the concept of national security secrets and moving beyond protection of the defense industry to assisting the entire private sector in combating corporate espionage.
- More explicitly connecting the impact of industrial espionage on the national economy to national security issues.
- Broadening the role of personnel security in non-defense industries, including a new perspective on "clearances," training, and threat awareness.
- Providing more information to the corporate community from the intelligence community regarding espionage threats, source countries, and targets and means.
- Aggressively prosecuting those involved in illegal economic and competitive intelligence.

Emerging Espionage Targets

Every industry and every country has important economic resources which must be protected. Generally, the focus of economic espionage activities can be broken down into two broad categories.

The first is formulae, processes, components, structure, characteristics, and applications of new technologies. Examples include:

- Fifth generation computer architecture; new computer chip designs, conductivity, and biochip research; and software development.
- Biotechnology.
- Supercomputing and superconductivity.
- Holographic and laser research, applications, and modeling.
- Optics and fiber optics technology.
- Aerospace technologies.
- Medical technologies, including pharmaceuticals.
- Advanced communications technologies and processes.
- Electromechanical products and technologies.
- Chemical process technology and research.
- Integrated circuit technologies.
- Advances in satellite usage and space technologies and applications.

The second category is factors associated with the marketing, production, and security of new technologies. Examples include:

- Pricing information.
- Marketing research on demand and consumer profiles.
- Products needed for compatibility and applicability.
- Production timetables and product release dates.
- Production quantities.
- Market targets and schedules and overseas marketing plans.
- Security equipment, sensors, and processes.

- Electronic banking equipment, interfaces, and protocols.
- Technology-upgrade schedules and planned changes in technology.
- Software developments, especially those enhancing new technologies, networking, and technological integration.

Two Vulnerable Targets: Computers and Intellectual Property

Computers provide both a target and a tool for industrial espionage. The new information highways provided by network systems (like Internet, Milnet, and Bitnet) and other advances like Electronic Data Exchange (EDI) and SWIFT (Society for World International Financial Transactions) also can mean increased access for illegitimate purposes. Computer-related crimes can be broken down into four main categories.

Computers as Targets: This relates to unlawful accessing of computers to gain information or to damage programs or hardware. A wide array of crimes fall into this category including: theft of intellectual property or marketing information, blackmail, sabotage of files, accessing and/or changing government records, techno-vandalism (causing internal damage to computer systems) and techno-trespass (violating the privacy of computer files).

- **Computers as Crime Instruments:** Computer processes used as instruments of crime. Examples include: ATM fraud, rounding off monetary entries, credit card fraud, fraudulent computer transactions, and telecommunications fraud.
- **Incidental Criminal Computer Use:** Computers used to increase the efficiency of traditional crimes, for example: money laundering, off-shore banking, pedophile information exchanges, organized crime record keeping, murder (through changing information in hospital records or other control systems), and bookmaking.
- **Crimes Associated With Computer Prevalence:** The advent of microcomputers has opened new crime and espionage targets. These include: software piracy/counterfeiting, copyright violations, counterfeit and black market computer equipment and programs.

Another growing target of economic / industrial espionage is intellectual property. It consists of concepts, ideas, planning documents, designs, formulae, and other materials intended for products or services which have commercial value and represent original thought or work. It may be clearly protected (with copyrights, trade marks, patents, or as trade secrets) or less well defined (in the case of non-protected research, incomplete new concepts or ideas, and public domain information which has been individually modified or refined).

Intellectual property is increasingly sought through industrial espionage because it can reflect a valuable investment involving lengthy research and development efforts. Moreover, it is often stored on computer media which are them-selves an increasing target of espionage.

Methods of Espionage

In addition to unlawful computer access, many of the traditional methods employed in national security and industrial espionage will continue to be prominent.

Among the many means of obtaining information are:

- Open sources (Right to Information Act requests, published government documents and bidding specifications, opened bids and technical journals).
- Consultants or outsourcing contractors from targeted firms who provide "inside information" to competitors.
- "Moles" working inside a particular industry or company with access to desired information.
- Computer hacking and data transmission interruption.
- Compromising employees through blackmail, set ups, corruption, and bribery.
- The use of student researchers and interns to gain access to research.
- Surveillance of corporate employees.
- Intercepting communications through faxes, telephones, etc.
- Burglary.
- Gaining access to records through janitorial or service personnel.
- New technologies and techniques adapted as detection devices or espionage countermeasures.

Motivations for Espionage

In general, the primary motivation for engaging in espionage is monetary. However, several factors have emerged in recent years that may make it easier for employees or others to participate in economic espionage. As espionage activity has shifted away from a focus on national security, the profitability of spying has increased. In addition, economic espionage (especially when information is divulged to traditional national allies) is less morally repulsive than betraying a national security secret and does not incur the same threat of punishment.

Employers should watch for a number of key characteristics that may indicate a security risk. Security threats may include employees who:

- Are generally unhappy on the job, or unhappy with the location of their assignment.
- Believe they have been overlooked for promotion, salary increases, or commendations and rewards.
- Feel their contributions to the company are ignored and uncompensated.
- Are facing personal financial difficulties.
- Have personal problems.

Prevention

There are a number of measures that employers can take to reduce industrial espionage. The most crucial of these are related to effective personnel policies and procedures.

Selection: Employees should be recruited and screened on the basis of their knowledge, competence, loyalty, and psychological and social stability.

Training: Employee training should include information about security threats and procedures.

Surveillance: Maintaining control over and limiting access to sensitive information will reduce potential losses.

Supervision: Attentive supervisors can both identify security violations as well as intervene before problems occur by remaining alert to warning signals.

Accountability: Ensuring that employees follow procedures, perform efficiently, and adhere to organizational values will help maintain personnel integrity.

Target Hardening: Measures should be taken to protect crucial information and to improve security in order to reduce temptation.

Positive Work Environment: Increasing employees' sense of worth within the organization can increase their sense of obligation and loyalty, thereby decreasing the possibility of espionage.

Realistic Sanctions: Employees must have a realistic sense that security violations will be identified and severely punished.

Positive Rewards: To balance the threat of discipline, positive contributions to the organization must be reinforced and rewarded.

Reinforcement of Ethics and Values: The organization must strengthen its employees' sense of moral obligation through a statement of organizational values, reinforcement of ethical standards, and high standards of professionalism.

In addition to these safeguards, corporations should consider the following precautions:

- De-stigmatizing compromising situations.
- Controlling and supervising the access of janitorial and temporary personnel to sensitive information.
- Accountability and access controls for temporary professional workers.
- Classification systems and model criminal and civil liability legislation for non-defense related intellectual property.
- Limits on outside employee consulting.

Security systems are frequently specified to address a perceived threat, and are commonly employed to protect people, revenues, assets or sensitive information, to

Only our individual faith in freedom can keep us free.

improve productivity, or any combination of these objectives. However, the efficiency and cost effectiveness of security equipment depends not only on its performance in isolation, but upon the programs, policies & procedures, administration and control of the overall security program. When considering equipment needs and options, examine the stated and perceived objectives and how each element of the program will contribute to the achievement of an effective security system.

Needs Assessments

Prior to recommending a physical or electronic solution, work to produce a 'Needs Assessment. This process involves identifying critical assets, reviewing historical security incident data, taking the latest security assessments into account, examining existing security Defence, considering current security operations & practices, and interviewing key personnel. Based on information collected, the consultants will identify the precise needs of the clients and will design and specify the exact equipment required to meet their objectives.

System Design & Specification

The key to providing an effective solution is a complete understanding the requirement. With the requirement clearly identified and agreed upon, design a system incorporating internationally approved standards and utilizing the latest technology taken from supplier database, ensuring maximum cost and efficiency benefits. Whether working with architects on a new construction or within an existing infrastructure, equipment will be designed! Specified to provide an *effective* solution *that* wm be simple to *use and easy* to maintain. "Through life costs" are an important factor in today's rapidly changing markets and all of the designs must take into account the ability to support systems throughout their operational lifecycle.

Tender Preparation & Evaluation

By applying a rigid methodology to tender evaluation, ensure that any system, or supplier, selected, will provide the best technical and financial solution.

Global Capability

The consultants come from a variety of backgrounds including Intelligence Services, Military and Police Forces and from Commercial Security organizations. Their sector expertise would cover Mining, Oil & Gas, Embassies, Banks, Commercial Premises and Key Points such as Airports, Ports and Refineries. Such consultants must have designed and specified systems such as:

- **CCTV -** both overt and covert surveillance platforms and including facial recognition
- **Access Control -** including proximity readers and biometrics
- **Perimeter protection -** including sensors, fences (electrified and or alarmed), lights and barriers
- **Alarms -** intruder and fire detection, panic systems and central monitoring
- **Explosive Detection Systems -** X-Ray machines, vapor and trace element detectors
- **Physical Security -** safe havens, vaults, high resistance doors and windows, turnstiles
- **Asset Management -** Building Management Systems, vehicle and guard tracking systems

rape escape Women's Self-Defense

Self-defense principles

- **Stay aware of people in your surroundings**
- **Stay with people, go to people**
- **Keep a barrier between you and the bad guy**
- **Attract attention**
- **Control his hips and his control his hands**
- **Use your strongest weapons against his weakest targets**

1. Stay aware of people in your surroundings.

Not surprisingly, criminals exhibit predatory behavior in preparing to attack. They will try to pick a casual location to look for their prey. They will look at their intended victim far more and for longer periods of time than social norms. They will move when the prey moves. They will stop and look around for witnesses. They will often make several passes by the prey in a sort of 'dry run', seeing if the victim will react or to get a sense of how the attack might work. Pay attention! Who is looking at you? Has the same person or car passed by you twice? Does someone appear to be moving with you?

2. Stay with people, go to people.

Do not ever let yourself be taken somewhere. Cops call it the "secondary crime scene" and most of the time it will be where your worst nightmare resides. If you are approached in a public place do not get in a vehicle with him. Do not walk around the building to the alley -- STAY where others can see you. His worst fear is the fear of getting caught, so you should drop to the ground if you need to in order to prevent him from carrying you away. On the other hand, if you are in your house or another location that is private, you need to GO to people. His worst fear is the fear of getting caught -- run out the door to a neighbor's. Crawl out a window onto the roof. Drive your car up to a diner or convenience store. Go where there are lights and others.

3. Keep a barrier between you and the bad guy.

Use a barrier to block him or use distance to gain time. Keep your doors locked. Stay in your car! Force him to get through a barrier before he can get to you. Use a barrier of pepper spray. The more difficult you make it, the more time it takes him and that means he might be discovered.

4. Attract attention.

The first thing he will say to you is "don't scream or I'll kill you". He's telling you exactly what will ruin his plan. Go ahead, ruin his plan -- create a disturbance, scream, throw things, blow the horn. If you think you should yell "fire" go right ahead. You can't count on others coming to

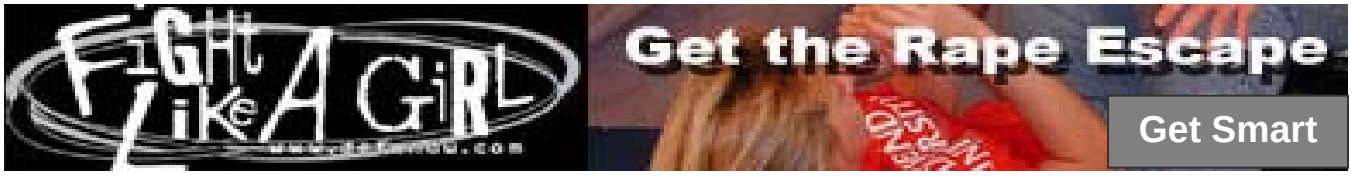
your aid, but you want to appeal to his fear of getting caught and make him think that someone could hear you and be coming.

5. Control his hips and his hands.

This might sound strange if you've not gone through the Rape Escape course, but the concept works. Control his hips to prevent penetration. If you can get your feet on his hips you can control the distance between the two of you. His hands are the weapons he will use against you. He will hit you, slap you, stab you or shoot you, but he has to use his hands to do the damage.

6. Use your strongest weapons against his weakest targets.

His weakest targets are those that are most valuable, yet ironically, cannot be entirely strengthened. His eyes, throat, groin and knees are your primary targets. Your secondary targets are his face and his abdomen. Strong weapons that you can employ are your kicks using the bottom of your feet, your elbows, hammer-fists and palm heel strikes.



Life is very precious, about security be serious!
Be aware of security, to save life & property !!

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

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!