



International Institute of Security & Safety Management



Let's professionalize the professionals...



Newsletter of NCR Chapter : October 2008

PSAR Act & Workplace Violence



The dramatic growth of the industrial security sector over the past twenty years has largely modified the way security is organized, distributed and controlled. These changes asked in turn for accommodation by the state and the police, among other things through the regulatory sphere. There are yet many dark areas in 'The Private Security Agencies (Regulation) Act', 2005. Many states are yet to finalize the rules and it seems that even in the midst of what terrorism has done to India, we are yet to take stock of situation and gear-up to give more authority and sanctity to private security!

Closer home, we have noted with concern the rise in work-place violence! In Noida, the dastardly act of killing of CEO by the sacked employees was still being discussed that another CEO became target of work place violence.

The most common industrial threat, workplace violence includes cases of disgruntled employees causing harm to a facility, its assets or other employees, and domestic issues that carry over to the workplace. The term "going postal" has entered our language due to a rash of violent outbreaks at U.S. postal facilities. School killings also fall into the category, underscoring the fact that no workplace is immune to the problem. Industrial facilities become more susceptible to violence in times of economic downturns when layoffs increase.

"Most industrial facilities have a workforce that is a microcosm of the world in general". "This means they include different types of people, with various personalities, who may be under stress and duress both at home and in the workplace. Some may have anger and violence issues that can carry over into the workplace. This can be lethal if it's not properly identified and handled early on."

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

Security Mantra

**"The biggest guru-mantra is:
Never share your secrets with anybody. It will destroy you."**

Chanakya Quotes (Indian politician, strategist and writer, 350 BC-275 BC)



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.
- Advances in satellite usage and space technologies and applications.
- Electromechanical products and technologies.
- Chemical process technology and research.
- Integrated circuit technologies.



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 themselves 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.

Webcams can be hijacked by Trojan Technique!!

By: Jo Best, News.com; Posted on [ZDNet News](#)

A new worm has been discovered in the wild that's not just settling for invading users' PCs--it wants to invade their homes, too.



The Rbot-GR virus follows a fairly traditional malware route of exploiting Microsoft security vulnerabilities and installing a Trojan horse on infected machines. However, the worm also spies on users by taking control of their Webcam and microphone, then sending images and soundtracks back to the hackers, according to antivirus firm Sophos.

As well as getting an insight into homes and businesses across the world, the worm allows the malware writer to take a look at information on the infected machine's hard drive, steal passwords and launch denial-of-service attacks.

Graham Cluley, senior technology consultant at Sophos, said the virus could be used for industrial espionage--or simply by a nosy hacker to take a look into people's bedrooms. "Whether this worm is the work of professional snoopers or lusty teenagers--it's hard to say for certain," Cluley said. "What we do know is that there have been a few hundred different versions of the Rbot worm, all of which have been designed to gain some kind of remote access to innocent users' data. This one goes further by also specifically collecting Webcam footage. It seems more and more hackers are building a cocktail of different functionality into their creations."

Those who have the virus may be unaware that their every move could be being tracked by remote hackers. An infected Webcam may show an "active light" when it's being used, but Webcams without such light would offer no giveaway the hacker is watching.

There is, however, one simple way to dodge the prying eyes of the malware merchants--just unplug or switch the Webcam off when it's not in use.



Now that's just plain spooky...

Throws towel over webcam





Going Out? Check list for Safety & Security

House Security:

- Keep close watch on modus operandi of thefts occurring in your area and take corrective action at your home.
- Use maximum locking device at home. Delay is important factor in theft. As much as hurdles you will put, more it will be inconvenient to thieves.
- Keep friendship with your neighbors. Keep them informed about your long absence. Give them the task of watching your house and give them phone numbers to contact you in emergency.
- Contact regularly your neighbors during absence and remind them the task given.
- Do not disclose exact time or period of your absence to servants, newspaper vendor, hawkers etc.
- Must not tell milkman or newspaper vendor about your intended absence. Let them guessing about your date of return.
- Piling-up of newspaper in front of entrance is telltale sign of your absence. Ask your neighbor to remove them everyday.
- Do not tell your children or maidservant exact travel plans. They spread the news far and wide.

While Driving:

- Be sure that you have all documents with you while driving. It will increase your confidence.
- Plan your journey in advance and start your journey with sufficient time for reaching at a destination.
- Do not use alcoholic drink.
- Use safety belt. Majority of lives lost in accidents is due to non-use of safety belt.
- Children should be asked to sit in rear seats. Or separate them because they divert attention on petty issues.
- A torch, fan belt, first aid box, extra wheel, headlamp, toolbox, water etc. are some of the essential items in long journeys.
- Do not drive continuously for a long period. Even five minutes engine stop is enough for rest.
- If possible follow a vehicle of ideal speed with ideal distance when road is unknown to you.
- Do not talk on interesting issues while traveling with family and friends.
- Inspect vehicle after every 3 to 4 hours of journey.

If you find this information important, you may send it to your friends. Points are based on common sense but some time we forget to remember them before moving out of house. Readers may add other essential points as per their experience.



Dates to Remember!



IISSM Annual Seminar 2008

The annual seminar of IISSM is being from 12th to 14th November 2008 at Hotel Cidade de Goa. Readers are requested to please contact following if booking is not already done -

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

Details of these courses and fees can also be obtained from home page of IISSM at <http://www.iissm.com>

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

