

INDUSTRIAL SECURITY & ASSET PROTECTION

Part 1



For Additional Info <http://www.elitecanada.com/tips.php>

INDUSTRIAL SECURITY

Physical Security, and Sensitive Document, Information Security.

An industrial premise security civil lawsuit often involves a claim against the owner of a property. The plaintiff usually contends that security measures in place at the time of the incident were inadequate and, as a result, did not protect the plaintiff, who is usually classified as an employee, invitee, or business invitee, from a criminal act and resulting injury or damage. Such litigation often follows a tragedy which may have been preventable, and seeks to hold accountable those parties who negligently failed to prevent it. Only too often this negligence represents an environment of opportunity, and a perfect scene for a crime.

Plant-wide Surveillance. Industrial plants are prone to theft of materials and finished goods by people from both outside and inside the facility. To counteract this costly threat, efficient, effective methods of closed circuit television surveillance and materials screening should be in place at all access/egress points.

Access Control. In an environment where time is money, the access control systems for employees and vendors must be designed for the efficient flow of people in and out of the plant. Often, this can be accomplished with a plant-wide system of access control cards combined with package screening systems at major access points.

Safety Management. Whether the threat comes from a disgruntled employee or a natural disaster, such as a tornado, every plant should develop, practice and continuously improve upon their emergency response program. Employees should know what to do and where to go in the event of an emergency

PHYSICAL INDUSTRIAL SECURITY - WHAT IT'S ALL ABOUT

There are various reasons why 'evil forces' are interested in gaining access to your organizations site.

1-Theft of information, product, tooling, etc, or purchase of information from personnel.

2-Theft from records, files documents or related sources....or **SABOTAGE** of facility, equipment, completed work etc

3-Gaining access to working models sample products, processes, or equipment, and making copies.

4-Manipulating personnel for one reason or another to gain information.

5-Using skillful means to obtain information at social events, etc.

6-Gathering information after gaining access to facilities. Searching through discarded records, waste, trash cans, etc. **CAUTION!!!**

7-Using advanced electronic methods. Bugs, phone taps, cell phone taps etc. Making threats, offering bribes, etc.

.

SECURING YOUR FACILITY

The primary objective in developing a security program is to render industrial espionage, Theft, & Sabotage, ineffective by implementing appropriate security measures.

Realistically, it's extremely difficult to reach a level of security that is 100% foolproof. However, proper steps should be taken to reduce every possible security breach. This involves an approach incorporating extensive protective measures--from personnel screening and training to electronic systems applications. (video cameras, DVR Recording, Access Control Systems etc.)

Essentially, security efforts will be a state of mind as much as the application of countermeasures. Every member of the organization has an important role to play in safeguarding company assets--especially those processes that are particularly sensitive and critical.

A well-planned security program will encompass a number of efforts, with special attention paid to many of the following aspects:

- 1- Screening and background checks for personnel;
- 2- Training security professionals and in-house staff; (Changes to the Security Act will soon be in place , and In house security will be obsolete)
- 3- Preventing unauthorized entry and controlling access;
- 4- Classifying, Safeguarding, and Protecting, sensitive and critical materials and information; Documents, Blue Prints, etc.
- 5- Protect tooling cribs, Products, materials, ...anything of value.
- 6- Inspecting security controls and audits periodically; establishing levels of accountability, enforcement, and authorization; Corporate
- 8- Controlling Disposal Efforts;**
- 9- Developing access restrictions and controlling movement in the facility;
- 10- Evaluating and monitoring personnel continuously in sensitive areas;

The Basic Security Planning Checklist on the following page is a practical approach to some of the common aspects of industrial security, theft, sabotage and espionage. It should be considered as a working tool (or as a guide to developing a more comprehensive program) if one isn't already in place. (Information provided should be considered as a basic overview of industrial espionage , asset protection, security planning and not as an exhaustive analysis

PHYSICAL SECURITY CONSIDERATIONS IN BRIEF

Assess overall physical security needs with regard to facility location, layout, design, construction, etc. Assess effectiveness of external/ internal controls with regard to an analysis of barriers, control points, entrances/exits, lighting, authorization levels, hardware, security devices, etc.

Establish effective programs for personnel screening--particularly prior to employment. Establish programs for ongoing evaluation, monitoring, and assessment of personnel, especially those in high risk areas. Control and enforce authorization levels, key usage, access restrictions, sign-in/sign-out, opening/closing procedures, proper use of security systems, vigilance and surveillance, etc.

Ensure full documentation of all security problems and violations. Develop levels of classification and restrictions (including written policies) on all sensitive material, etc.

Establish procedures for handling/ safeguarding sensitive materials, tooling, equipment etc.. Develop and enforce restrictions for employee access within the facility and around sensitive/high risk areas.

Promote an ongoing program of monitoring and evaluation for the potential exploitation of persons with personal problems who work in sensitive and high risk areas. (Security level may not be applicable to Valiant Tool)

Establish effective ongoing security education training programs. Evaluate and plan for the possibility of electronic eavesdropping and ensure proper countermeasures. Use appropriate security systems, safes/vaults, and other anti-intrusion and theft devices. Develop a comprehensive business security planning program with ongoing evaluation and upgrade efforts.

BASIC SECURITY PLANNING CHECKLIST

Access controls and facility surveillance aspects
Identification and assessment of access controls, point of entry limitations, personnel vigilance, etc.

Types of controls

- a. Security personnel, patrols and inspections (SIGNAGE)
- b. Alarm systems and anti-intrusion devices.
- C Closed circuit television and electronic monitoring
- d. **Key control** management and accountability
- e. Levels of access and authorization
- f. I.D. badges and recognition systems (if required)
- g. Pre-employment screening and on-the-job monitoring
- h. Security education and emphasis on enforcement
- i. Other types of access controls

Perimeter and barrier protection

- a. Natural barriers: landscape and terrain
- b. Fencing: type and construction
- c. Walls and ceiling construction: high risk areas
- d. Gate facilities: security checkpoints
- e. Frequency of patrols and security checks
- f. Door and window locations and security devices used
- g. Reception areas: location and control of entry
- h. Employee surveillance and vigilance
- i. Parking areas: entrance/exit, access to facility

How effective are the current security aspects of the following areas?

1.
 - a. Barrier controls, fencing, building design, etc.
 - b. Lighting conditions for security illumination
 - c. Obstructions to security patrols and surveillance visibility
 - d. Exterior doors, access points, entrances, etc.
 - e. Exterior windows and other openings
 - f. Possible points of concealment and climbing aids
 - g. Trash collection areas and disposal of documents, papers,
 - h. Alarm systems and related security devices
 - i. Personnel, visitors, and others: control of movement, etc.

How effective are current procedures with regard to:

1.
 - a. Access controls
 - b. Opening and closing
 - c. Control of documents
 - d. Supervision/monitoring
 - e. Property control
 - f. Check-in and check-out
 - g. **Control of contractors**, vendors, repairmen, janitors etc
 - h. Disposal/removal of records, papers, etc.
 - i. Key control and key usage
 - j. Locking and unlocking
 - k. Shipping/receiving controls
 - l. Storage of materials, etc.
 - m. Employee vigilance/surveillance
 - n. Security systems/devices
 - o. Other procedures and controls

General Recommendations

Security protection, and prevention is not only effective for asset, and access control, but also in the event of potential lawsuits. It can be shown that preventative security planning has been implemented for the security, and safety of employees, visitors, suppliers, vendors etc.

1- An effective methods of closed circuit television surveillance and materials screening should be in place at all access/egress points. FENCING

2- Plan for Access Control to manufacturing plants. (Locks can be picked or manipulated)during working hours, and especially on weekends or off shifts.

3- Control your access to documents, blueprints , client contacts, bids etc. with control of who has access and when they have access , with sign in, and out procedures, for control. A safe room should be considered.

4- Screen your employees thoroughly, they will have access to your assets, equipment, tooling, documents, and sensitive information.

5- Random property, and plant location, security patrol spot checks. Who controls keys, access, etc. Who has keys ?? Duplication!!

6- Control WSIB and insurance claims with investigations, And follow ups.

7- Special attention should be dedicated.... in control of suppliers, vendors, trades entering your plants, and controlling their access to the specific area of business. Possible solution...proximity readers.

8 Time Theftwhat precautions are in place? Employees leaving plants prior to shift end, or managers/ sales personnel not on the job as required.

9- DO NOT ALLOW INDIVIDUAL LOCATIONS TO CONTROL THEIR OWN SECURITY. THIS IS INEFFECTIVE & IS EASILY BREACHED !

CORPORATE MUST CONTROL SECURITY....INTERNALLY & EXTERNALLY.