INTRUSION ALARM SYSTEM

Case studies reveal most burglars are deterred by the mere presence of an alarm system. Burglars attack unprotected premises considerably more often than ones protected by alarm systems, so an alarm system can greatly minimize your losses.

Though an alarm system is an excellent defense, the best defense is through a combination of efforts:

- Solidly built doors hung on well-fitted door frames.
- Doors properly secured with high quality dead bolt locks.
- Windows that will resist forced entry via auxiliary locking devices.
- Use of proper lighting.
- Use of a quality burglar alarm system.

It is important that you get and maintain a good, reliable system. The type of system that will be best for you depends on many different factors – your security needs, type of valuables, type of premises to be protected, your life-style, and animals in the home, etc.

It is important to select the proper product and supplier. What may appear to be an alarm system “bargain” could actually prove to be a severely compromised or extremely limited alarm system.

Advantages of an Alarm System

- The mere fact that an alarm system exists is often a sufficient deterrent to discourage a burglar even before he tries to force an entry.
- Knowing you and your property are secure increases peace of mind.
- Most insurance companies give a reduction on homeowner’s insurance when an alarm system has been installed.

Be sure to check with your agent for details.

Wired Versus Wireless

“Wired” simply means all components of the system are connected to each other by electrical wire, usually offering more proven reliability.

“Wireless” systems rely on transmitting signals between components, much like radio signals. “Wireless” systems are growing in popularity as the technology improves. A good system costs about the same as a hard wired system. Things to look for in wireless systems are:

- A supervised system. The control panel and sensors are constantly sending each other signals.
- The control panel is in a locked and tamper-proof area.
- The sensor sends two signals to activate the control panel.
- The transmitters are tamper-proof.

How to select an Alarm Company

- Contact more than one alarm companies.
- Are they members of SSSPL organization in Lebanon.
- Have each company appraise your security needs and make suggestions on the system they recommend. Obtain a written proposal that includes the recommendations and all associated cost factors of components, installation, service, etc.
- Contact previous customers of the alarm companies, where possible, to obtain their opinion of the system and service they have received. A member company of the SSSPL will not hesitate to provide you with names of satisfied customers.
- Make sure you understand the system.
Be aware of what it can and cannot do. Receive oral and written instructions covering all circumstances involving the system operation and instructions on testing the system.

- What services are offered, such as a maintenance contract, 24 hour response for repair service…
- Does the company offer a written guarantee? What is guaranteed and for how long? Are parts and labor covered?
- What is the equipment repair policy? What is the policy on service charges after the warranty expires?

**BASIC PARTS OF AN AND ALARM SYSTEM**

There are three basic components to all alarm security systems. Sensors, or detectors, are sophisticated devices that detect unwanted entry. They do this through various kinds of sensing instruments: electronic, electromechanical, radar or microwave, audio and motion/vibration, photoelectric. Detectors work by either breaking an electric current, completing an electric circuit or transmitting a detectable signal to a control unit.

**Control units** are the core of most security alarm systems. They receive information of a disturbance from the sensors, and this triggers an alarm or alarms. Also they provide power supply for all detectors and they are fitted with rechargeable batteries to give continuous functionality for your alarm system if there is a power failure.

**Alarms** are internal or external bells, horns or sirens, designed to make a great noise and scare off the intruder. The noise is continuous or in timed sequences. Some alarm systems include switching devices that can turn on outside and interior lights. Other systems can be connected to an automatic telephone dialing device that calls preselected phone numbers such as a local police station.

Generally, home security alarm systems are classified into two broad categories, perimeter systems and interior space detectors.

**INTERIOR PROTECTION**

**Passive Infrared Detectors**

The passive infrared detector (PIR) is one of the most common detectors found in household and small business. The term passive means the detector is able to function without the need to generate and radiate its own energy. PIRs are able to distinguish if an infrared emitting object is present by first learning the ambient temperature of the monitored space and then detecting a change in the temperature caused by the presence of an object. Using the principle of differentiation, which is a check of presence or non presence, PIRs verify if an intruder or object is actually there.
**Photo-electric Beams**
Photoelectric beam systems detect the presence of an intruder by transmitting visible or infra red light beams across an area, where these beams maybe obstructed. To improve the detection surface area, the beams are often employed in stacks of two or more. The technology can be an effective long-range detection system, if installed in stacks of three or more where the transmitters and receivers are staggered to create a fence-like barrier. Systems are available for both internal and external applications.

**Microwave Detectors**
This device emits microwaves from a transmitter and detects any reflected microwaves or reduction in beam intensity using a receiver. The transmitter and receiver are usually combined inside a single housing for indoor applications, and separate housings for outdoor applications. To reduce false alarms this type of detector is usually combined with a passive infra red detector or “Double Technology” alarm.

**Panic Button**
Panic Button allows you to activate an alarm system manually with push of a button. Either remote (wireless) or fixed station.

**Glass Break Detectors**
Glass break acoustic detectors are mounted in close proximity to the glass panes and listen for sound frequencies associated with glass breaking. Seismic glass break detectors are different in that they are installed on the glass pane. When glass breaks it produces specific shock frequencies which travel through the glass and often through the window frame and the surrounding walls and ceiling. Typically, the most intense frequencies generated are between 3 and 5 kHz, depending on the type of glass and the presence of a plastic inter layer. Seismic glass break detectors “feel” these shock frequencies and in turn generate an alarm condition.

**Seismic Detectors**
The seismic detector is suitable for monitoring armored cabinets, cash boxes, automatic teller machines, night safes, armored safes, and safe vault walls for all known burglary tools such as diamond-tipped drills, hydraulic rams, oxygen lances and explosives. Mechanical vibrations caused by a burglary attempt are detected and analyzed by the seismic detector sensor, and an alarm is triggered.
Magnetic Contacts
Magnetic contacts most commonly used, electromechanical device that activates when the magnet and contact are separated. Used mainly on doors and windows, most magnetic contacts used in different applications are concealed.

PERIMETER PROTECTION
These types of sensors would be found most of the time mounted on fences or installed on the perimeter of the protected area.

Vibration or Inertia Sensors
These devices are mounted on barriers and are used primarily to detect an attack on the structure itself. The technology relies on an unstable mechanical configuration that forms part of the electrical circuit. When movement or vibration occurs, the unstable portion of the circuit moves and breaks the current flow, which produces an alarm. The technology of the devices varies and can be sensitive to different levels of vibration.

More sophisticated sensors use piezoelectric components rather than mechanical circuits, which can be tuned to be extremely sensitive to vibration. These sensors are more durable and more resistant to tampering.

Passive Magnetic Field Detection
This buried security system is based on the Magnetic Anomaly Detection principle of operation. The system uses an electromagnetic field generator powering with two wires running in parallel. Both wires run along the perimeter and are usually installed about 5 inches apart on top of a wall or about foot buried in the ground. The wires are connected to a signal processor which analyzes any change in the magnetic field.

E-Field
This proximity system can be installed on building perimeters, fences, and walls. It also has the ability to be installed free standing on dedicated poles. The system uses an electromagnetic field generator powering one wire, with another sensing wire running parallel to it. Both wires run along the perimeter and are usually installed about 800 millimeters apart. The sensing wire is connected to a signal processor that analyses:

- Mass of intruder
- Movement of intruder
- Time the intruder is in the pattern

These items define the characteristics of an intruder and when all three are detected simultaneously, an alarm signal is generated.
**Microwave Barriers**
The operation of a microwave barrier is very simple. This type of device produces an electromagnetic beam using high frequency waves that pass from the transmitter to the receiver, creating an invisible but sensitive wall of protection. When the receiver detects a difference of condition within the beam (and hence a possible intrusion), the system begins a detailed analysis of the situation. If the system considers the signal a real intrusion, it provides an alarm signal.

**Micro Phonic Systems**
Micro phonic based systems vary in design but each is generally based on the detection of an intruder attempting to cut or climb over a chain wire fence. Usually the micro phonic detection systems are installed as sensor cables attached to rigid chain wire fences, however some specialised versions of these systems can also be installed as buried systems underground. Depending on the version selected, it can be sensitive to different levels of noise or vibration. The system is based on coaxial or electromagnetic sensor cable with the controller having the ability to differentiate between signals from the cable or chain wire being cut, an intruder climbing the fence, or bad weather conditions.

**Fibre Optic Cable**
A fibre-optic cable can be used to detect intruders by measuring the difference in the amount of light sent through the fibre core. If the cable is disturbed, light will ‘leak’ out and the receiver unit will detect a difference in the amount of light received. The cable can be attached directly to a chain wire fence or bonded into a barbed steel tape that is used to protect the tops of walls and fences. This type of barbed tape provides a good physical deterrent as well as giving an immediate alarm if the tape is cut or severely distorted.

**H-Field**
This system employs an electromagnetic field disturbance principle based on two unshielded (or ‘leaky’) coaxial cables buried about 10–15 cm deep and located at about...
2.1 metres apart. The transmitter emits continuous Radio Frequency (RF) energy along one cable and the energy is received by the other cable. When the change in field strength weakens due to the presence of an object and reaches a pre-set lower threshold, an alarm condition is generated.

We believe that prevention, not paranoia, should guide you to an effective program of home and business security.

When considering the element of risk in the design of an intruder alarm system the structure of the premises to be supervised (protected) will be a major determining factor.

Issues should be considered such as:

- Construction
- Openings

(e.g. doors, windows…)

- Occupancy
- Key holding
- Locality
- Existing security
- Theft history
- Local legislation or regulation
- Security environment

The adoption of a risk assessment approach should lead to better designed system that is commensurate with the risk and meet the customer’s and insurer’s requirements.

Systems and Equipment cannot be reliable unless properly maintained by professionals on a yearly basis.