WHITE PAPER

Warehouse Security and Alarm Responses

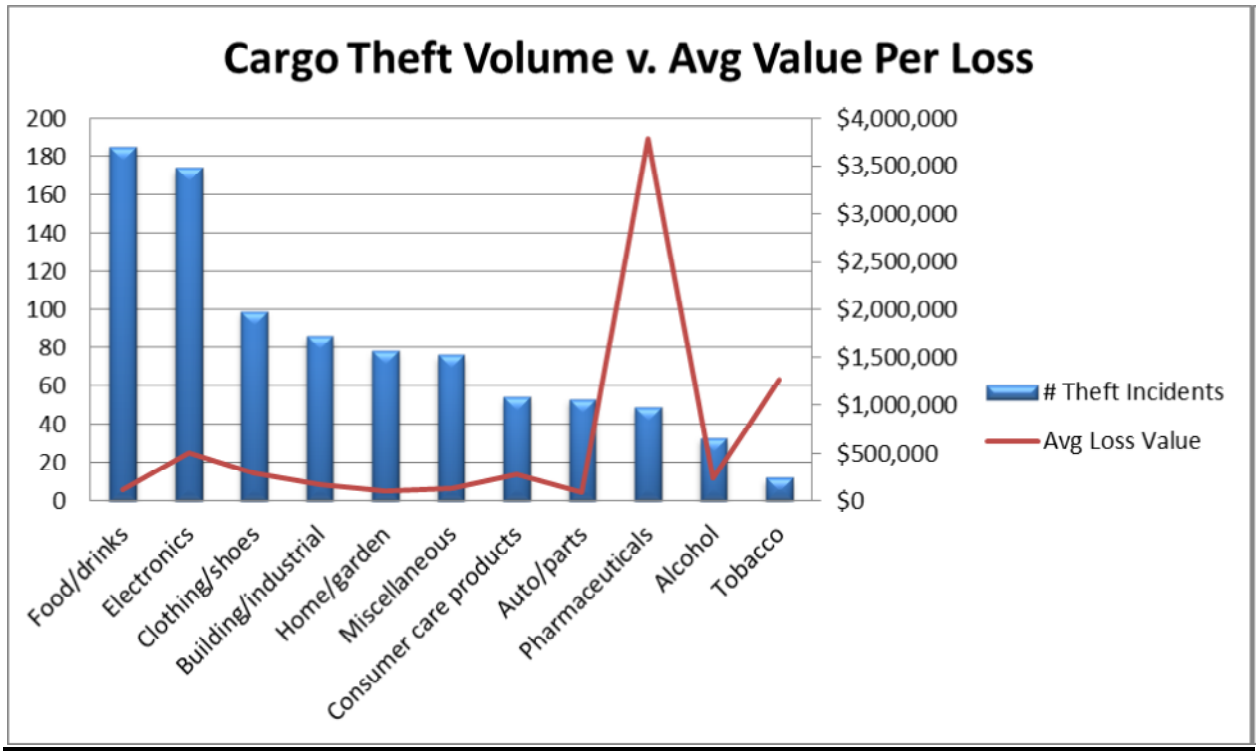
Prepared by AIMU's

Cargo Loss Prevention Committee

OVERVIEW

According to FreightWatch International's Annual Report for 2010 cargo theft rose by 4.1% in 2010, to 899 recorded theft incidents, the highest on record. Of the 899 incidents, 724 (81%) were full truckload or container thefts and 31 were warehouse burglaries (3.4%).

The average loss value per incident in 2010 was recorded at $471,200. This is a decrease of 17% from 2009, when the average loss value per incident was recorded at $572,800. Pharmaceuticals once again measured as the highest per-incident value, averaging $3.78 million, with tobacco second at $1.26 million and electronics third at $512,000. Over the year, FreightWatch recorded 28 losses valued at more than $1 million each; a decrease from 2009, which saw 43 losses valued at more than $1 million. Of the multi-million-dollar losses in 2010, three were valued in excess of $10 million (two pharmaceutical and one tobacco), one of which was a pharmaceutical warehouse burglary in March 2010. Valued at $76 million, it is the largest loss on record.



On March 14, 2010 thieves broke into a warehouse in Enfield, CT. According to published reports they scaled the exterior walls, cut a hole through the roof and rappelled down into the facility using climbing gear. As described in FreightWatch's Annual Report this incident is the largest pharmaceuticals theft loss in history. An article in CCNMoney give details of the incident. The timing of the break-in will come as no surprise; it occurred in the early morning hours and it was done on a weekend. In this case, the thieves were able to drive their truck right up to the loading dock. While security cameras recorded the images of the truck no one was monitoring the cameras. The thieves were able to use the warehouse's own forklifts as the keys had been left with the trucks. At some point during this robbery, which took place over several hours, another alarm went off. At that time staff at the cs monitoring facility called the name listed on the victim's contact sheet and left a message.

A similar incident took place at a GlaxoSmithKline warehouse in Chesterfield, VA where burglars broke through the roof, climbed down a trapeze-style rigging, and hung from it as they disabled the primary and secondary alarm systems. The perpetrator, say two sources familiar with the investigation, exploited wiring shortcuts known to few within the company. Once inside, the burglars stayed for hours, loading two tractor-trailers with $6 million in drugs.

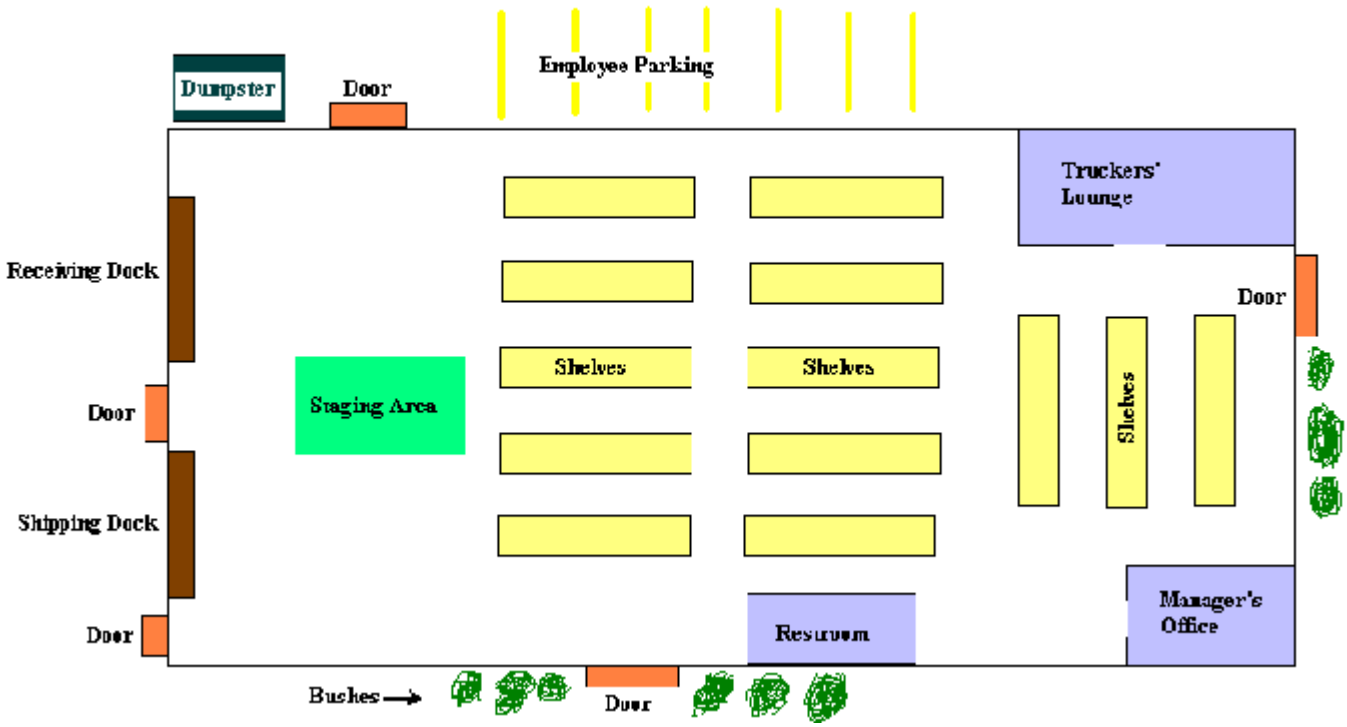
For all their precision, the thieves made two mistakes. Before they disabled the surveillance camera, it captured a grainy image of one of them. An informant identified the man as a 48-year-old Miami Cuban, a convicted burglar and electrician. The man was arrested but then released for lack of evidence. He has since been deported to Cuba, according to Immigration and Customs Enforcement records. The second mistake: one of the burglars left behind a coffee cup.

Meanwhile, as the investigation into the burglary at Lilly's Enfield warehouse continues, the crime scene has yielded a clue: DNA found there matches that found on the coffee cup at the GSK warehouse, suggesting that at least one thief was involved in both burglaries. The genetic material points to a prolific convicted burglar -- a fugitive Miami Cuban, according to sources familiar with the investigation.

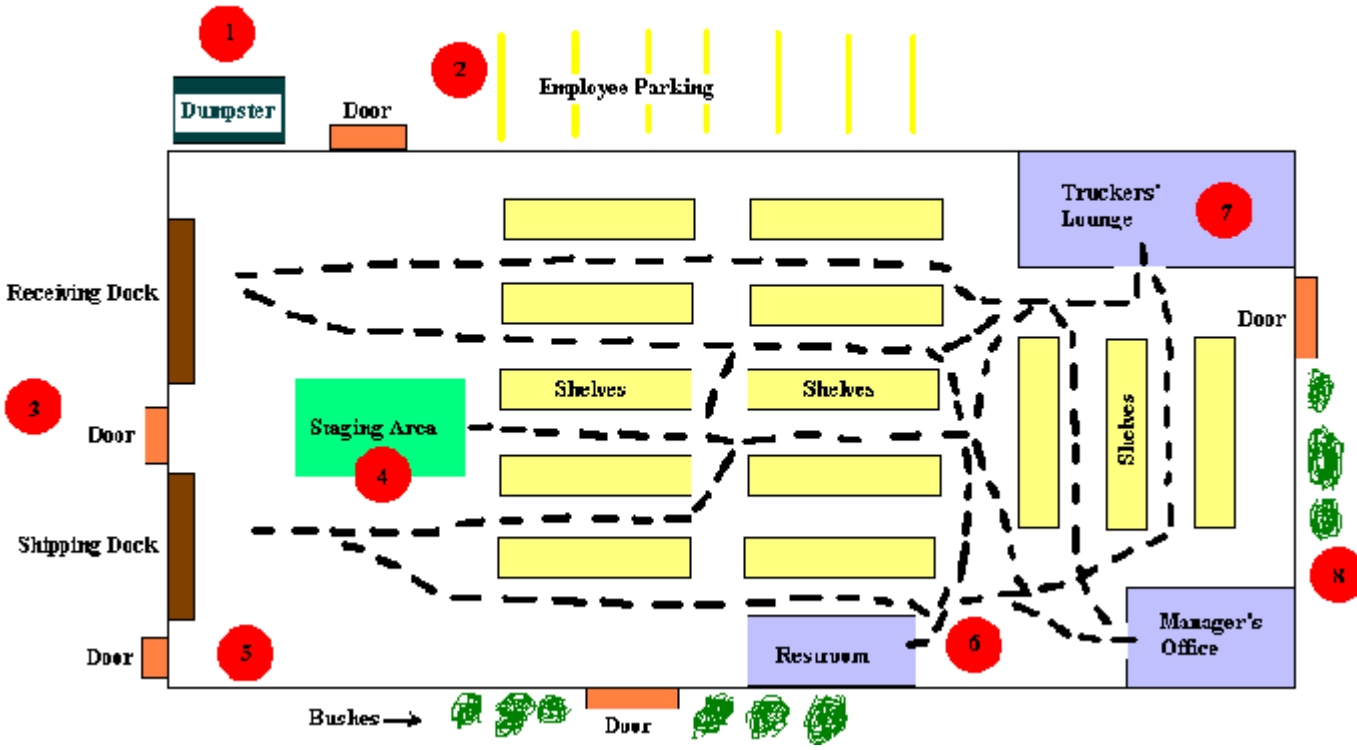
Organized criminal gangs, many of them Cuban-American and operating out of South Florida, according to law enforcement, have dramatically increased both the size and the frequency of their heists.

With these types of losses on record the Cargo Loss Prevention Committee believes it is worth discussing what can be done to make these robberies a little more difficult thereby increasing the odds of detection. We will also take this opportunity to reiterate the types of alarm systems that are available and more particularly describe best practices for response protocols that are used once that alarm does go off.

Warehouse Security Quiz



Check out this floor plan drawing of a warehouse with many security problems.



crimeprevention.rutgers.edu

See Appendix C for a list of security concerns in this scenario

GENERAL WAREHOUSE SECURITY REQUIREMENTS

Warehouses, distribution centers, third party logistics locations. The names may vary but the concept and the issues are the same. In the world of cargo the exposures presented by static warehouse risks are unique and separate in their risk characteristics but provide the same large potential for theft loss as cargo in transit. Warehouses come in all shapes and sizes, from 100 year old brick buildings to brand new, single story distribution facilities. Whatever the construction or configuration a number of general practices should be considered when reviewing security concerns at any location.

- Proper and working alarm system (burglary and fire protection) with back-up alarm system and emergency response plan.
- Advocate the use of company security guards present on site outside of normal operating hours. Preferably security guards on site 24/7.
- Raised barriers/ bollards across entrance gate and any area of perimeter which is accessible to be rammed.
- Dock doors to be adequately secured locked on both sides near base.
- All internal perimeters protected by motion detectors.
- All drivers and visitors to be security cleared prior to being allowed access.
- 3rd party service to perform DOT license validation check on all drivers before releasing load.
- All deliveries and pickups by appointment only.
- All yard jockeys and forklifts to be locked with ignition keys secured.
- All 3rd party cleaners and maintenance companies to be fully vetted.
- Reinforced security cage and/or vault for high value merchandise.
- Theft prone drugs etc. to be stored on high racks.
- No loaded trailers left in yard out of operating hours.
- No empty containers/ trailers to be left at doors out of operating hours.

Please refer to Appendix A for details of TAPA's (Transported Asset Protection Association) Minimum Security Requirements.

EXTERIOR PERIMETER PROTECTION

Exterior perimeter protection is usually provided where part of the premises consists of open storage areas, such as yards or loading areas in which stocks or materials are stored, or where access to these areas would present a severe exposure to the rest of the premises. This protection normally consists of a strong, properly installed chain link fence (or other physical barrier) with pole-mounted or roof-mounted lights that adequately illuminate the area around the fence.

Gates that provide access should be manned or monitored. The number of gates should be kept to the minimum necessary for proper access and safety. They should be secured with locking devices and the distribution of keys should be controlled by management.

In the event additional protection is required, an alarm system suitable for fence or barrier protection can be installed.

One such alarm system that is the taut wire detection system. In this system, an almost invisible, but very strong wire is strung along the top of the fence or barrier. The wire is held at a calibrated tension by a spring mechanism. Either a relaxation of the tension (due to wire cutting, for example) or addition to the tension (pressure from an intruder's hand) will set off an alarm. Even movement of the fence, caused by a careful climber, will activate the system.

Another method for providing outdoor perimeter protection is the electronic fence. In this system, a current-carrying wire radiates an electromagnetic field which when interrupted (the fence is touched or approached) sets off an alarm.

Other systems include seismic alarms which detect the weight of the intruder on the ground surface or photoelectric systems that project invisible rays which when interrupted activate an alarm.

Best practices for perimeter protection should consist of some or all of the following:

1. The storage facility should be completely fenced. The fence should be at least eight (8) feet high with three (3) or more strands of barbed wire. If a barbed wire extension is installed, it should be at a 45-degree angle out from the area to be secured. It is also prudent to bolt or rivet the barbed wire arms to the fence posts. Additional information on security fencing can be obtained from the Chain Link Fence Manufacturers Institute. Their web site (www.chainlinlinfo.org) contains guidelines as well as a product manual.

2. There should be no exposed area beneath the fence; four (4) or more inches of free space under the fence can allow unauthorized access.
3. The fence posts should be well secured in concrete and the fencing properly anchored to the posts.
4. The fence should be at least 25 feet away from any structures or objects like buildings, trucks, intermodal containers and trees that can make it easier either for someone to climb over the fence or camouflage their activities.
5. There should be some method, such as guardrails, to prevent vehicles from backing into the fence line as well as preventing thieves from driving through it.
6. The number of entrances/exits should be limited and all well controlled.
7. All semi-active entrances/exits, such as railroad spurs/sidings, should be locked when not in use.
8. There should be no openings, culverts, tunnels or manholes leading inside the facility that can permit access.

POINT-OF-ENTRY PROTECTION

Complete protection to all perimeter walls of the facility, including the ceiling and floor. These surfaces usually are protected by noise detectors, vibration detectors or by lacing with wall foil or burglar screens. In many cases, this method of protection is cost prohibitive, and protecting the perimeter walls while neglecting the ceiling and floor leaves the building vulnerable to entry through these surfaces. This impracticality of total interior perimeter protection, in most cases, has led to the use of alternate methods to provide somewhat equivalent protection. The two methods that find most frequent application are area protection and point-of-entry protection. Point-of-entry protection consists of the alarming of all windows, doors and other accessible openings into a facility by means of contact devices, switches and/or metallic foil tape. In some instances, a burglar screen instead of metallic foil is used to protect windows, transoms, skylights and similar type openings. These openings may be partially protected to detect only the opening of the door, window or skylight, or fully protected to detect entry through the opening as well as movement of the opening.

The following devices are those most commonly used in point-of-entry protection:

Contact devices - also known as door switches, are designed to detect the opening of a door, window or other perimeter opening. These devices are probably responsible for the detection of the largest number of burglars and are the most maintenance free devices when properly applied. There are basically two types of switches - electromechanical and magnetic - with numerous variations in the design of each.

Metallic foil - is used in the protection of windows and glass doors and consists of strips of foil taped to the glass surface with the intent that the foil will break if the glass breaks. In effect, the foil is like a fuse; breaking the foil breaks an electric circuit. The major disadvantages of metallic foil are that it is easily defeated by the clever intruder and requires frequent maintenance.

Burglar screens - are constructed of easily broken wooden dowels which have a fine wire run either through a hollow center portion or in a grooved slot in the dowel. The dowels are arranged in a cage-like fashion with no more than four inches between each dowel. The screen is placed across the opening, so that an intruder, to gain entry, would have to break the dowels, interrupting the circuit and initiating an alarm. Their use is restricted to areas that are not heavily traveled and is limited to smaller opening like small windows, air conditioning vents or crawl spaces because of their expense of fabrication. Normally the screens are permanently mounted but movable screens are available.

Perimeter protection is often the most expensive method of protecting a facility as well as the most practical. It is often the most expensive because of the large amount of wiring and labor cost involved in joining each detection device, of which there may be many, into a total system. It is the most practical since this method offers the earliest opportunity to detect any unauthorized entry.

All entrances, exits and other vulnerable areas should be protected by surveillance cameras. See below for best practices for Cameras and CCTV Equipment.

INTERIOR PROTECTION

CAMERAS AND CCTV EQUIPMENT

Perimeter protections and burglar alarm systems are two lines of defense for any warehouse. Their job is to protect and to warn against external threats. However, an overwhelming majority of warehouse thefts in the United States are the result of ‘inside jobs’. In order to counteract this threat the use of video surveillance equipment is becoming more and more widespread. Video surveillance is used to monitor entrances and exits, loading docks and the interior of the warehouse. The images they provide can be accessed via the internet or through a business’s

own computer system. This makes it possible to view these areas immediately when the alarm is activated.

Care should be taken when deciding where to place cameras. Smart criminals are well aware of the limitations of video surveillance systems and may plan their crimes around them. They may commit their crimes just outside of the rage of the cameras.

The goal of most camera systems is to provide recorded evidence when a crime has been committed assisting in the identification and capture of the criminal.

Best practices to protect all points of entry should consist of some or all of the following:

1. All cameras need to be positioned to ensure that it is difficult to manually access them for the purposes of covering or misaligning them.
2. All facility security/ safety personnel should trained for optimum use of CCTV equipment.
3. Camera settings, definition and quality should be confirmed on a daily basis
4. Camera lens' to be periodically cleaned.
5. There should be password protected remote access capability with email electronic alerts triggered by alarm activation.
6. Only digital recording equipment should be used.
7. Recording locations should be secured at all times.
8. The security cameras should have a zoom feature so that drivers, their vehicles and any intruders can be clearly identified. There should be enough light throughout the facility so that any activity can be effectively captured on tape under all ambient conditions.
9. The security cameras should have a pan/tilt feature so that they can reach all vulnerable locations within the facility.
10. The camera monitors should be under the constant supervision of the storage facility management and/or security personnel.
11. The security camera tapes should be labeled and be retained under lock for at least 30 days.
12. All potential entry points of a building should be protected by alarms. Sensors should also be placed high up since some cargo criminals enter the building through roof/skylight.

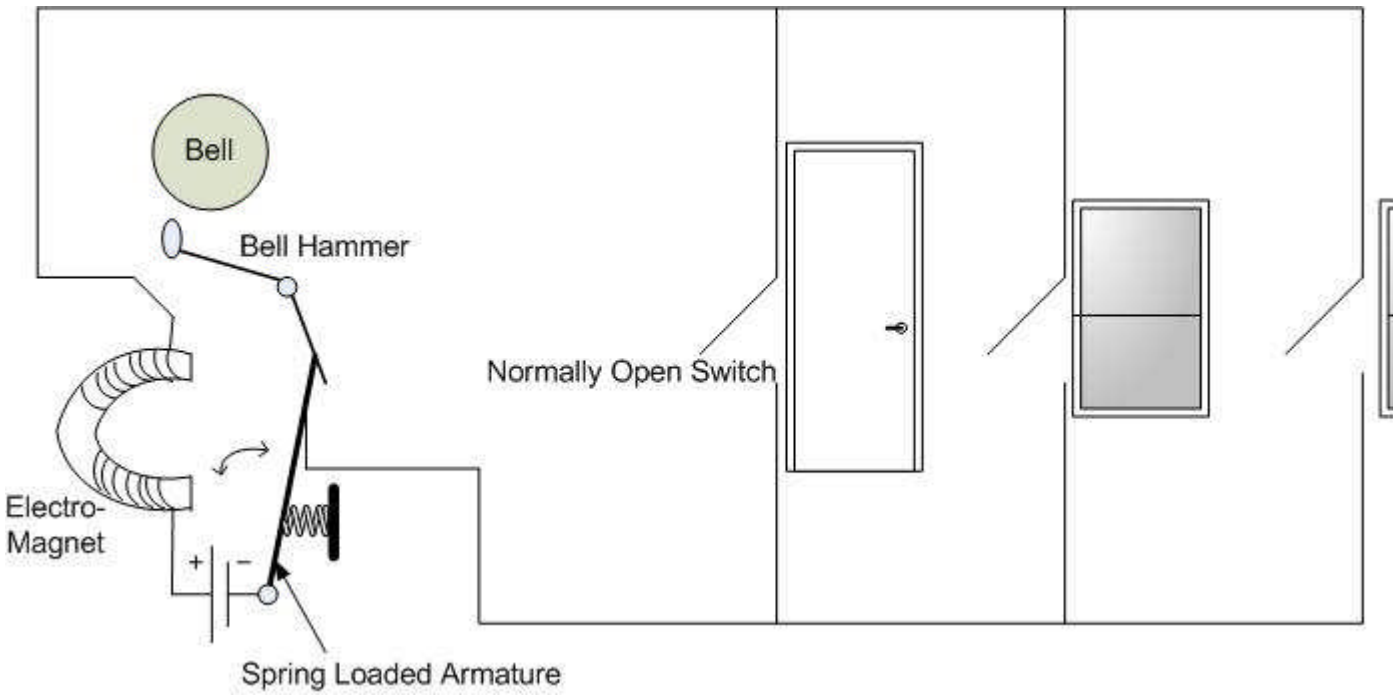
PERSONNEL

Best practices for supervision of all personnel should consist of some or all of the following:

1. All employees of the storage facility should be thoroughly screened prior to employment with the background check including driving, criminal and financial/credit reviews. The storage facility management should verify all the information contained on the employment application such as current address and previous employer (s).
2. No employees should be allowed to park their personal vehicles near the cargo storage/staging areas.
3. Access to certain areas within the facility should be limited to those personnel that should be there.
4. Employees should have limited access to documentation.
5. driver/outsider access to cargo areas should be limited (particularly high value, susceptible product).
6. Conduct Criminal and DMV background checks on all warehouse personnel.
7. Seasonal/temporary workers to be obtained through bona fide employment agency.
8. All employees access to cell phones on site should be restricted to limit communication and photography.

BURGLAR ALARM SYSTEMS

The burglar as we know it today was first patented by Augustus Russell Pope on June 21, 1853. The design of the Pope patent called for a normally open circuit. Doors and windows were connected in parallel and when physically opened they would close the circuit and activate the alarm. In this first design the alarm did not “latch”, in other words the bell would stop ringing once the violated door or window was physically shut.



Pope sold the rights to the patent in 1858 to Edwin Holmes. Holmes manufactured the device in his factory in Boston, Massachusetts. He began to sell them in 1858. In 1859, in search of a new and bigger market Homes moved his business to New York, which was then perceived as a place where "all the country's burglars made their home". By 1866 he had installed 1200 home alarms. By 1877, he established the first network of alarms monitored by a central station in New York. This was an outgrowth of the municipal fire alarm system in use in New York at the time. The Central Station employed call boxes located throughout the city, which when operated transmitted a signal to a central station from which a messenger or a policeman was dispatched.

Burglar alarm systems are designed to detect the entry or attempted entry of an intruder into a protected facility and signal his presence to others nearby or at a remote location, thus initiating certain procedures intended to prevent or minimize the loss. The three basic components of any alarm system are;

System Types; the methods used to control and monitor the system. They are Local, Police Station connect and Central Station.

Detection Devices; The actual pieces of equipment used to detect an intruder. They are contacts on doors and windows, motion detectors and protection for safes or other objects requiring a high degree of security.

Transmission Systems; The method used to transmit an alarm signal. They are Loop Circuit, Direct Wire and Digital Communicators. These systems should include Line Supervision, the ability to detect and sound an alarm if the line is tampered with, either accidentally or intentionally.

The effectiveness of any alarm system depends on these factors: the reliability of its components; the quality of its installation and maintenance; the promptness of the monitoring company's response.

Underwriters can determine the adequacy of many alarm systems by relying on the burglar alarm certificate program of Underwriters Laboratories (UL). **Underwriters Laboratories Inc.** (**UL**) is an independent product safety certification organization. Established in 1894 the company has its headquarters in Northbrook, IL. UL develops standards and test procedures for products, materials, components, assemblies, tools and equipment, chiefly dealing with product safety. UL has developed standards for alarm system components and installations. The process begins with the testing of alarm system components for compliance with the applicable standard. Follow up tests are critical to make sure that the components remain in compliance. UL also investigates the qualifications of alarm installation and central station monitoring companies. UL categorizes alarm systems as follows:

(1) Local alarm - a signal device such as a loud bell, horn or siren mounted to an outside wall of the premises.

(2) Police station connection - A signal is transmitted to the local police station.

(3) Central station - A signal is transmitted to a central station of the alarm company.

Local Alarm Systems - a local alarm system is one in which the protective circuits and devices are connected to an enclosed and tamper-protected loud sounding device attached to an outside wall of the building in which the property is situated. Disturbance of the protective devices or unauthorized entry through wired portions of the property automatically causes the sounding device to operate until it is stopped by key control in the possession of the owner or by exhaustion of the power supply or by a timing device set for a definite period of time. The activation of the system is usually under the control of the proprietor. UL requires that the contractor inspect the system at intervals of one year or less depending on current and power requirements and maintain and service the equipment.

Local alarm systems are wired to be electrically supervised to deter tampering or defeat of the controls or sounding device. In a supervised circuit a small current is made to flow through the circuit at all times when the system is in the active mode, and the circuitry is arranged so that an alarm will be actuated if conductors of opposite polarity are "crossed" or the circuit is "opened".

Police Station Connected System - a police station connected alarm system is a local system that is direct-connected to a police station so that when an alarm is actuated at the premises a signal is also transmitted to the constantly attended police station. The same requirements for local systems apply to police station connected except that the audible signal may be delayed up to five minutes to allow police to respond to a silent alarm. In the police station connected system, the installing company is responsible for the maintenance of the equipment. In the case where the alarm receiving equipment at the police station is the responsibility of another installer, an agreement is reached between the two companies so that the required maintenance is provided.

Central Station System - a central station alarm system is one in which the burglarious entry is signaled to a facility, called a central station, that is owned and operated by a commercial protective agency for the purpose of providing certain protective services to subscribers. The alarm signal is automatically signaled to the central station where trained operators and guards are in attendance at all times to supervise, record and respond to the signal. The central station itself consists of a physically secure, fire-resistive and guarded structure in which is housed the alarm line circuit terminals, annunciators, recording equipment and associated test and power supply facilities.

The task of turning on and off the alarm system is left in the hands of the owner or proprietor of the premises. He is required to signal the central station (where it is recorded and noted), each time he opens or closes the premises. Any irregularities receive prompt response. The greatest advantage of the central station system is this high degree of supervision afforded.

On receipt of an alarm signal, the central station dispatcher determines whether it is a scheduled opening or closing, a special pre-arranged opening or a bona fide alarm. If the alarm appears valid, the dispatcher refers to the pertinent card file for the name and address of the attached premises. He then telephones the police dispatcher on a direct line giving him the name and address of the premises. Unless otherwise specified on the certificate of classification, the central station holds keys to the premises, and the dispatched guard is given the keys so that he can enter or permit the police to enter with him to search the premises and apprehend any unauthorized persons.

In addition to the central station response, warehouse staff should be trained in alarm response protocols to understand their specific roles and responsibilities thereby allowing them to respond quickly and appropriately in an alarm situation. These response protocols should provide guidance in identifying false alarms, unverified alarms or panic and distress alarms. Warehouse security procedures and central station monitoring companys' instructions should contain clear alarm response protocols. Contact lists must be updated on a regular basis.

Please refer to Appendix B for details of UL Burglar Alarm standards.

WAREHOUSE / FACILITY CONTROL

Insured Owned Buildings and Property

Buildings and property owned by the insured has the ability to install any type of system, device and physical controls within the building and on their property. This includes alarm systems with any type of device, CCTV systems with a choice of cameras taking into account lighting conditions and physical barriers and controls such as fencing and walls inside the building. Exterior controls including fencing, gates and barriers.

Leased Buildings and Property

Insured's that lease a building(s) or a portion of a building are limited in what they can do to protect their inventory. The lease agreement with the property owner may dictate restrictions on what could be done. In most cases alarm systems and CCTV can be installed at the insured's expense. Physical deterrents such as fencing may be in violation of the lease agreement. In sublet spaces or where there are shared common spaces uncontrolled access may be necessary. Installation of exterior fences and gates may not be possible. In buildings with multiple tenants or a section is sublet, the owner may have an alarm system outside the care a custody of the insured.

Third Party Warehouses

In third party warehouse locations the warehousemen should provide security for their clients. The insured can only ask for security systems, CCTV and physical barriers be installed if not already in place. Changes in pre-existing systems can be asked for by the insured. The economic value of a customer drives the decisions of third party warehouseman on installation and changes to security systems. The security of a third party warehouse must be a major factor on an insured using a third party provider, not the cost.

SUMMARY

In order to be successful a good security system needs to overlap and integrate where possible. No single security layer or system will prevent all intrusions. Unauthorized entry may be made from any direction, including roofs, walls, floors, and adjacent buildings or rooms. Building materials, locking devices, and intrusion detection systems should be designed to protect against these vulnerabilities. A good security design addresses risks with a variety of technologies and barriers that deter, detect, delay, and defend against intrusions. To achieve the best security at the most reasonable cost, the protection plan should not consist of just a high, strong fence or contacts on doors or foil on windows. The plan must be designed so that if the intruder eludes one defense, he will be confronted by a second or third defense that may result in his detection.

It is critical to any security system that audits be conducted on a regular basis to ensure that all security measures, such as fencing, lighting, cameras and alarms are operational and being used to their best advantage.

Security surveys should be conducted with a mandated frequency. Results should be escalated as appropriate. Written action plans should be developed and prioritized for all observations and deficiencies identified to ensure a timely resolution.

Appendix B

The Burglar Alarm Certificate Service of Underwriters Laboratories Inc.

GRADES OF SERVICE

Burglar alarm systems are classified according to the grade of service as Grade AA, Grade A, Grade BB, Grade B, Grade CC, or Grade C. The grade designation establishes the quality of equipment used, the form of signal transmission, and the maximum allowable guard response time. The double grade designation provides for special protection of the connecting line used for transmitting the signal.

1. Local mercantile alarm systems are classified as Grade A or Grade B according to the degree to which the design is electrically supervised against failure without indication to the owner, and to the degree of protection provided against tampering or defeat of the controls or sounding devices.

2. Police station connected systems are classified as Grade AA, Grade A, or Grade B according to the degree to which their design is electrically supervised against failure without indication to the owner and to the degree of protection provided against tampering or defeat of the controls, interconnecting telephone lines and sounding device. The Grade AA designation provides for supervision of the transmitting line between police station and protected premises.

3. Central station systems are graded primarily according to the response time required for central station guards to reach the subscriber premises following receipt of an alarm. Other factors that are considered in establishing grade designation are the quality of the equipment used and the type of signal transmission. Table I summarizes the grades of certificates available from listed central stations and the type of signal transmission required for each grade.

Maximum Response Time	Grade of Service	Type of Signal Transmission System
15 Minutes	AA	Direct wire or multiplex system equipped with UL listed line security devices or systems
	A	Direct wire or multiplex system

Maximum Response Time	Grade of Service	Type of Signal Transmission System
20 Minutes	A	Combination transmitter-local alarm system with outside sounding bell
	BB	Same as for Grade B with line supervision
	B	Transmitter, combination transmitter local alarm with inside sounding bell, direct wire, or multiplex system
30 Minutes	CC	Same as for Grade C with line supervision
	C	Any of the above systems

TABLE I

CLASS OF PROPERTY

Burglar alarm systems are further classified according to the class of property for which they are suitable as bank safes and vaults, mercantile premises and mercantile safes and vaults.

The following definitions apply:

1. Premises - ordinary stores, lofts, warehouses, etc., used for the storage, handling or manufacturing of merchandise.

2. Safe - a movable construction of iron or steel, the doors of which are equipped with a combination lock.

3. Vault - a permanent, non-removable construction of iron, steel, brick, concrete, stone, tile, or similar masonry units permanently built into or assembled on the premises and having an iron or steel door and a combination lock.

EXTENT OF PROTECTION

Premises and Stockrooms - the extent of local and police station connected alarm protection installed on mercantile premises is classified as Installation #2 or 3. The extent of central station alarm protection installed on mercantile premises is classified as Installations #1, 2, or 3 in accordance with the following definition:

a) INSTALLATION No. I - Completely protecting all windows, doors, transoms, skylights, and other openings leading from the premises, all

ceilings, floors, halls, party partitions, and building walls enclosing the premises, except building walls which are exposed to street or public highways, and except that part of any building wall which is at least two stories above the roof of an adjoining building.

b) INSTALLATION No. 2 - Protecting with traps all inaccessible windows; and with screens (or foils and traps) all accessible windows, doors, transoms, skylights and other openings leading from the premises; and protecting all ceilings and floors not constructed of concrete, and all halls, partitions, and party walls enclosing the premises, or

Protecting with supervisory contacts only all movable openings leading from the premises, and providing a system of invisible radiation to all sections of the enclosed area, so as to detect four step movement, or

Protecting with traps all inaccessible windows; with screens (or foils and traps) all accessible windows, doors, transoms, skylights, and other openings leading from the premises and providing a network of invisible beams to subdivide the floor space of each floor or separate section of the protected area into three approximately equal areas, and more where necessary, to provide at least one subdivision per 1000 square feet of floor space.

c) INSTALLMENT No. 3 - Protecting with screens (or foils and traps) all accessible windows, doors, transoms, skylights, and other openings leading from the premises, or

Protecting with contracts only all movable accessible openings leading from the premises and providing one or more invisible rays or channels of radiation with the minimum over-all length of the rays or radiation equivalent to the longest dimensions of the area or areas so as to detect movement through the channel, or

Protecting with contacts all doors leading from the protected area or areas and providing a system of invisible radiation to all sections of the enclosed area so as to detect four-step movement.

Installation #1 provides the most extensive protection of the three. Installation #2 provides more extensive protection than #3.

Installation #1 does not apply to local or police station connected burglar alarm systems. The majority (80%) of protected premises have Installation #3.

U.L. LINE SECURITY SYSTEMS

Burglar alarm systems are classified as to type or principle of operation as local, police-connect, or central station. Regardless of the type, however, all burglar alarm systems consist of three basic components. The first component is the alarm sensors or detection devices that are intended to detect the burglarious entry. These are connected through the alarm system's electrical circuit to the second component, the control cabinet, by which the system is turned on and off, and tested. The third component in the system is the reporting device to which the detection signal is transmitted. This can be a bell outside the protected premises, or an alarm

panel at a police or central station office. It is this third component that categorizes the system as local, police-connect~ or central station.

In a central station system, the control unit transmits the alarm signal to a central station office where it is monitored. The medium over which the signal is normally transmitted is a telephone circuit. It is at this point, the telephone lines, that the system is most vulnerable to defeat or compromise. A compromise is defined as the disconnection of the protected premises from the connecting line or communication link in a manner that does not cause a signal at the central station and allows entry into the protected premises without causing a signal at the central station. (However, it should be noted, that there are other methods of defeating a central station burglar alarm system besides attacking the telephone line.)

In an attempt to reduce the vulnerability of these systems to compromise, line security equipment was developed which, when added to the conventional central station system, provides additional protection against telephone alarm line compromise attacks.

UL STANDARD FOR LINE SECURITY

Central station burglar alarm systems are rated by UL as Grade A, B or C depending upon guard response time and the type of equipment used to provide the service. To indicate the addition of line security to the system, UL applies the designation Grade AA, BB or CC. The double letter designation signifies only the difference in response times since the same line security equipment is used to provide each grade of service.

TRANSMISSION OF ALARM SIGNALS

All burglar alarm systems, whether simple or sophisticated, consist of three basic components: sensor(s), control unit and reporting device. The sensor(s) detects the presence of the intruder, usually through a change in sensor status, and generates a signal to the control unit. The control unit processes this signal and, assuming it constitutes an alarm condition, relays or transmits an alarm signal to activate the reporting device. In a local alarm system, the reporting device would be a bell or siren installed at the protected premises. In a police connect or central station alarm system, the alarm signal is transmitted silently over some medium, such as an electrical circuit (or radio), to alarm indicating equipment (the reporting device) at a remote monitoring location.

In general, most police-connect and central station alarm systems rely upon telephone lines as the transmission medium for the alarm signal. Four signaling methods or systems are currently recognized by Underwriters Laboratories Inc. (UL) as suitable for transmitting the alarm signal over telephone lines in a central station burglar alarm system. They are: direct wire, transmitter, multiplex and digital communicator. The first three systems require dedicated telephone lines, ie., a pair of copper conductors that are leased from the telephone company and used solely for signal transmission; digital communicators operate over the public switched telephone network (the same circuits over which ordinary telephones operate).

In a direct wire system each protected property is connected directly over an exclusive circuit to the central station. The transmitter system, more commonly known as a McCulloh system, is essentially a "party line" in which several protected properties are connected in series over a single loop or circuit to the central station, with each protected property identified by a unique code. As defined by UL, multiplexing is a method of signaling characterized by the simultaneous and/or sequential transmission and reception of multiple signals over a communication channel (in this case, telephone lines) with means for positively identifying each signal. A McCulloh system is technically a simplified form of multiplexing. The fourth method of signaling is the digital communicator which is discussed next.

DIGITAL COMMUNICATORS

Originally introduced in the mid 1960's, the digital communicator gained an unfavorable reputation because of the proliferation and subsequent unsatisfactory performance of a device that operates on a similar principle, the tape dialer. Operating over the existing telephone lines (they are like telephone extensions that plug into the phone lines), the tape dialer upon activation sends a recorded voice message to any telephone number preprogrammed into the machine.

Although the tape dialer afforded a cost-effective alternative to the other signaling methods, a number of factors limited their acceptance. First, burglar alarm systems utilizing tape dialers experienced a high rate of false alarm, and since often the dialers were programmed to call the police (or fire) department, a number of municipalities soon

adopted ordinance that controlled or prohibited their use. Second, a significant disadvantage to the use of the tape dialer is that the device has no means for verifying that its message has been received. And finally, since the public telephone network cannot be provided with line supervision, tape dialers were limited to low security applications.

Unlike the tape dialer which consists only of a sending unit, the digital communicator is comprised of a digital transmitter at the protected premises and a digital receiver at the remote monitoring location. On activation, the transmitter seizes the telephone line, preempting any incoming or outgoing calls, and simulates the dialing of the telephone number at which a receiver is located. The transmitter first looks for a "handshake" signal to verify that the receiver has been contacted and then proceeds to transmit a digital coded message which the receiver is capable of deciphering. Before disconnecting it awaits a signal that the message has been received. The transmitter can be programmed to dial any telephone number, but this number must be at a location where there is an active receiver. One receiver, normally, can monitor many (usually up to 1,000) transmitters.

The digital communicator is far more reliable than the tape dialer primarily because there is a verification of signal reception. However, a major drawback to their use as a high security device is that they operate over the public telephone network which, as stated earlier, cannot be adequately supervised. Consequently, the telephone lines in a digital communicator system remain vulnerable to compromise. In the Standard for Safety ANSI/UL 611, Central Station Burglar Alarm Units and Systems, UL attempts to address this inherent weakness of the digital communicator.

UL REQUIREMENTS FOR DIGITAL COMMUNICATORS

Digital communicators have only recently been recognized by UL as an acceptable means for transmitting burglar alarm signals. Prior to this recognition, all UL listed signaling equipment required dedicated telephone lines which provide for continual supervision. However, because of maintenance problems associated with dedicated lines and partly as a result of their unavailability in some areas, UL has instituted a listing service for digital communicators.

The following are the UL requirements for digital communicators used for central station burglar alarm service:

a. All information exchanged between the transmitter and receiver shall be by digital code or the equivalent. A voice message may be used to transmit supplemental information.

b. The transmitter shall be capable of seizing the telephone line at the protected premises, cutting off an outgoing telephone call, and preventing its use for outgoing telephone calls until signal transmission has been completed.

c. The equipment shall be able to disconnect an incoming call and free the telephone line for signal transmission.

d. After the receiver has been contacted:

(1) The transmitter and receiver shall verify that contact has been made;

(2) The transmitter shall send its signal;

(3) The receiver shall verify that the signal is valid, and

(4) The contact shall be disconnected as soon as verification is received.

e. The equipment shall provide for the following:

(1) If the transmitter does not get a signal verifying contact with the receiver, it shall go on-hook (disconnect from the network) after waiting no more than 45 seconds and then try again.

(2) If the transmitter has received the contact verification signal and has transmitted its message, but then does not receive a sign-off (verification) signal indicating that a valid message has been received and accepted, the transmitter shall go on hook, recontact the receiver and repeat the process. The transmitter may send the message a second time before going on-hook, but shall not wait more than 5 seconds for the sign-off signal in any case.

f. Supervision of the telephone line(s) at the protected premises shall be provided in one of the following ways:

(1) Two telephones lines shall be used and the transmitter shall be able to switch from one to the other. Both telephone lines shall be monitored so that if a fault develops on either one, the transmitter will contact the receiver through the remaining line to report the problem and identify it as telephone line trouble.

(2) The transmitter shall contact the receiver with an identifiable signal at least once every 24 hours. The regular opening signal, closing signal or a special signal may be used for the purpose.

g. If the telephone line supervision is provided as described in paragraph 6a, the transmitter shall be capable of switching to the secondary telephone line after two attempts to make contact with the receiver on the primary telephone line. After making two attempts on the secondary telephone line, the transmitter shall switch back to the primary line. This sequence shall continue until the transmitter has made at least eight but not more than fifteen attempts to deliver the message.

h. If supervision is provided using paragraph 6b, the same number of attempts to transmit the signal is required.

i. The transmitter shall be designed so that when the user places the system into the secure (night) mode, an indicator will show whether or not the telephone

line(s) is in operating condition. The indicator may be visible, audible or both. The indication of the receipt of the sign-off signal will provide the check for the telephone line used to transmit the closing signal.

j. The transmitter shall be powered from alternating current and shall be provided with a standby battery having 24 hour capacity under maximum load.

k. The receiving equipment at the central station shall accommodate a minimum of two incoming telephone lines. Incoming transmissions shall go to the first available line.

l. Each incoming signal shall initiate an audible alarm that shall remain established until manually reset.

APPLICATION

With the high rental cost of dedicated telephone lines and their diminishing availability, central station operators have sought other means for transmitting burglar alarm signals. Digital communicators provide a reasonable alternative. But, since digital communicators cannot be provided with continuous line supervision, they do not afford the same degree of high security as can be obtained from a direct wire or multiplex system. In general, they provide a level of security more consistent with that of a McCulloh system.

UL acknowledges that digital communicators perform at a different level in comparison to the other signaling systems and this is reflected in the grades of service that they have been assigned under the UL Burglar Alarm Certificate Service. A burglar alarm system with a digital communicator alone can be certificated as Grade C; with a listed sounding device, a Grade B certificate can be issued.

Burglar alarm systems utilizing digital communicators provide a type of central station service that is suitable to many small businesses and homes. Since they operate over the public telephone network, normal daily usage of the telephone, in a sense, does verify the integrity of the network. This may not compare with the degree of supervision provided by dedicated telephone lines but, when other factors are taken into account, digital communicators installed and operated according to UL requirements do afford an alternative to the other signaling systems. The important considerations here is application. Digital communicators are not high security devices; they are intended more for the low risk application. When applied in such manner they provide a cost-effective and acceptable method of alarm signal transmission.

SUMMARY

Table II provides a summary of the factors which affect the certification of burglar alarm systems.

Type of System	Grade of Service	Class of Property	Extent of Protection

Local Alarm	A or B	Safes and Vaults	Complete or Partial
		Premises and Stockrooms	Installation #2 or 3
Police Station Connected	AA, A or B	Safes and Vaults	Complete or Partial
		Premises and Stockrooms	Installation #2 or 3
Central Station	AA,A,BB,B,CC or C	Safes and Vaults	Complete or Partial
		Premises and Stockrooms	Installation #2 or 3

TABLE II

Table III has been prepared by Underwriters Laboratories Inc. to help explain their certificate service and its various classifications. The chart does not include Holdup Alarms, Bullet Resisting Enclosures or Tear Gas Systems. At the present time, there are no companies listed for tear gas protection.

According to UL, the alarm systems which cause the greatest amount of misunderstanding to users and the insurance industry are the local alarms having remote connections to the police or a central station. This type of alarm does not record opening and closing signals or have guard response. Therefore, it should not be considered as equivalent to a central station alarm.

There are two separate classifications for Bank Safe and Vault Alarms which require bells. There are only ten companies listed in these categories and not all are listed for both types of alarms.

A safe or vault alarm certificate issued to a bank by a Local Mercantile or Police Station Connected alarm company will be a mercantile type. This certificate should not be confused with a Local Bank certificate since requirements for bank alarm equipment are much more stringent due to the higher values involved.

Appendix C

Warehouse Security Quiz
Answers

1. **Never put a dumpster or other garbage containers by a door. This dumpster is in an ideal spot for employees to hide stolen things and move them to their cars later on. If your dumpster is in a bad spot and can't be moved, let everyone know you search it often for merchandise.**
2. **The closeness of this parking area, plus the fact that it is right by a door, makes it easier for employees to take things from the warehouse and put them in their cars. The further people park from the warehouse, the better. If possible, have a fence separating the warehouse from the parking lot.**
3. **The receiving dock and the shipping dock are too close together, and there is no barrier between them. It would be easy to take things from one truck and put them into another.**
4. **This staging area may be too close to the loading docks. If no one is around to keep an eye out, it would be easy to take something and put it in a truck.**
5. **This warehouse has far too many doors. There should only be one that is open, and there should be a guard or other employee in charge of watching this door. If fire regulations require more than one door, use bars that set off an alarm if the doors are opened.**
6. **This is a bad spot for the restroom. To reach it, the truckers have to walk through the warehouse. This puts your goods at risk of being stolen. Just because people are dropping off or picking up shipments doesn't mean they are free to wander around. It's best to keep unauthorized people out of the warehouse.**
7. **To get to this lounge area, the truckers have to walk all through the warehouse. Look at the tracks to see where they might walk. Everything along these routes is at risk. It is important to restrict movement in your warehouse. Don't let people just go wherever they want.**
8. **These bushes are a good hiding spot for things stolen out of the warehouse, especially because they are right by the door. So either get rid of the bushes, or lock the doors.**