

TIP SHEET



Securing Commercial Buildings

Most people fail to properly develop a security strategy prior to addressing their security needs. This often results in poorly conceived strategies that are restricted to the perimeter of the building. Before you decide on security improvements, there are certain things that you should know.

WHAT YOU NEED TO KNOW

The speed and cost to business of modern day burglaries is shocking. Most computer and electronic burglaries are over in less than 90 seconds, often in less time that it takes for the average alarm company to contact police, yet result in a staggering losses when the loss of information and disruption to business are included.

For this reason you should not rely solely on alarm systems, or other narrowly focused countermeasures such as security bars to protect your valuables. Alarm systems and security bars are not complete security systems.

They are simply options to be considered when developing an effective security strategy that is appropriate for your business.

DEVELOPING YOUR SECURITY STRATEGY

Experience has shown that the most successful security strategies rely on a combination of deterrence, detection and delay strategies applied specifically in this order. Failure to address each of these elements or change their order diminishes your chances of preventing burglaries.

DETERRENCE

The safest property is the one that doesn't attract criminals in the first place.

To avoid attracting burglars make sure that:

- views of your property are as unobscured as possible paying particular attention to landscaping
- facilitate night-time surveillance by using lighting to draw attention to windows and doors that can be observed from the street or other active areas
- "weapons of opportunity" such as small garden rocks or throwable objects are not lying about your property
- participate in the Operation Provident engraving program. Operation Provident informs thieves that all valuables inside the premise are marked with a unique nine digit number that not only reduces the value of the assets to the criminal element but substantially increases the risk to persons found in their possession.



Ask us for information about our Operation Provident program and how you can obtain your free Operation Provident "Stop" sign stickers.

DETECTION

One of the most common reasons why security fails is that there is little chance for detection or detection occurs when its too late.

In those cases where the design of the building or a lack of after hours activity results in limited witness potential, it is important to recognize these shortcomings and take steps to effectively address this problem.



TIP SHEET

Securing Commercial Buildings - Page 2

DETECTION

Many businesses when faced with this challenge will turn to the alarm industry. For alarm systems to be effective it should:

- be encountered at the first and basic level of security (window or door lock)
- detect any perimeter violation as it occurs and not afterward (motion sensors should be used as a back up only)
- eliminate the delay on the alarm condition at ALL entrance points
- draw attention to the burglar through the use of audible sound devices and flashing strobe lights
- be tamper resistant (including external signaling devices and phone lines)
- use technology that effectively manages false alarms without sacrificing security
- be monitored by a remote security station (if required due to low witness potential or other reasons), and must be used in combination with effective delaying tactics.

DELAY

Before you consider adding security to the perimeter of your property, consider these factors first:

- the cost associated with properly securing the perimeter of your property can be great as it is directly proportional to size
- the security of your perimeter is only as good as its weakest point
- windows, doors, locks, frames and even roofs are all common entry points
- bars will only slow down burglars who attack windows and in any event can be readily defeated
- bars can take away from the image of your company
- if bars are used, they should always be applied after the first layer of security (inside the glass) with glass break sensors.

As a result of these shortcomings, we suggest that the best strategy is to develop a "safe" room for your computer hard drives within your office building. This will create a significant barrier in a post alarm environment which can be achieved at reasonable cost.

For further information look for the Crime Prevention Through Environmental Design (CPTED) tip sheet or contact the Rural & Agricultural Crime Team.