

Guide to Protecting Property



Guide to Protecting Property

Introduction

Hello and welcome to our guide to protecting property. Protecting your property is not a straightforward thing, the main crimes that most business owners think of are criminal damage, theft and arson, but 30% of business crimes come from within an organisation. This is more concerning especially when considering that most security systems are configured to protect solely against external threats.

We have created this document to provide guidance on protecting your property from both external and internal threats.

We have started with the basics, or baseline security measures; the steps you should take no matter what the level of risk, and then provided further information about how you can build on the basics and achieve extra resilience. Because, unfortunately, it is not a case of **IF** you have a security incident but **WHEN**. Resilience is crucial!

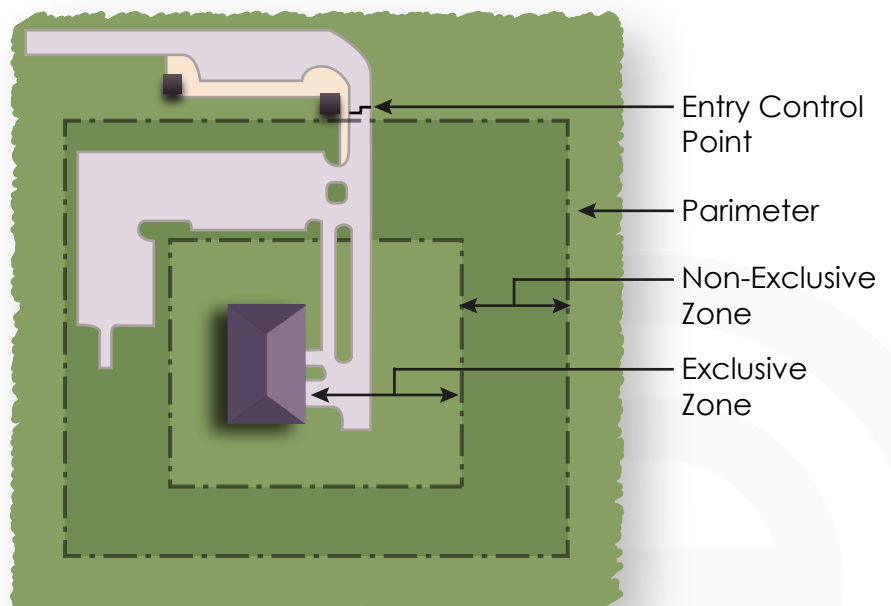
Scope

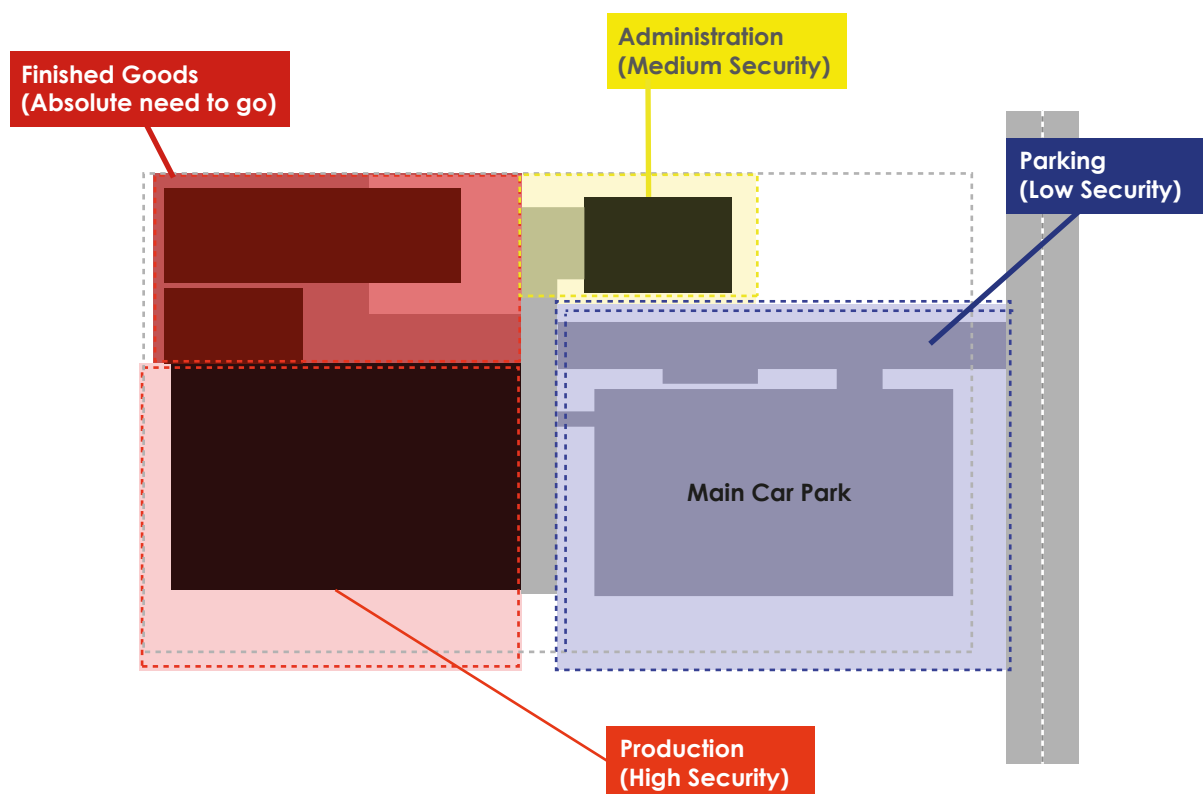
The most effective way of protecting your property is to carry out a full security analysis to highlight what the problems are, how to deal with them and what to do when things go wrong. This document provides only general guidance on property protection.

For more detailed guidance specific to your business, please get in touch.

Baseline Security Measures

To achieve more robust protection for your property you should base your security on the **security in depth** principle. This implies that each layer of defence becomes a delay and if any single layer should fail, the threat should be contained by the subsequent layer. The protection measures below (See Diagrams) overlap each other- where the weakness of one layer are overlapped by the strengths of the next.





Site Perimeter

If your business has a perimeter fence, this may provide an opportunity to temporarily delay any intruder long enough for them to be detected and hopefully disrupted from carry out their intended action.

A fence should be resistant to climbing and breaching, it should be at least 2.4m high with a hostile (think razor wire) topping to extend the fence to 3m overall. Dependent on the size of your business perimeter, it may be necessary to establish a gatehouse to control access.

Inner Perimeter

Larger sites may be compartmentalised into smaller units, or critical areas (especially on petrochemical sites) inside the the main site perimeter. Inner perimeters may also be used for distribution and warehousing, and other areas that require enhanced protection. A specific advantage of an inner perimeter, aside from it adding an additional ring of security, is that its small size allows for the deployment of enhanced security measures that may be too expensive to install around the main perimeter.

Building Exterior

In some cases, the building exterior may be the businesses only perimeter security. Most burglars attempt to enter buildings via either doors or windows, so these should be considered exceptionally vulnerable. If just the doors are strengthened and little attention paid to the windows, the intruder will enter via the window and will most likely be able to release the door from the inside, allowing for easy extraction of stolen items.

a.Doors - All external doors should be equipped with appropriate locking mechanisms which incorporate at least two deadlocking points. As a rule of thumb, external doors should be constructed of steel, solid core wood, or industrial strength glass.

A single door should be designated as the final exit door, with all other exterior doors having internal locking mechanisms. If possible, you should try and avoid using padlocks, unless used internally. In the event of doors needing to be left open for ventilation, a grille gate should be installed.

b.Windows - All ground floor windows, and those within 5 metres of the ground, should have toughened glass, or preferably laminated glass, as a minimum. It may be worth considering installing grilles or bars dependent on the perceived level of risk. If windows are overlooked by public areas, it is advisable to make the windows opaque to make target identification difficult.

c.Roof - You should ensure that all roof doors and hatches are always secured when not in use. If you have skylights, you should secure these using bars or grills, with an alarm fitted to detect any unauthorised opening or breaking. Some buildings have external ladders or fixing that allow access to the roof, these should be secured to stop unauthorised persons accessing the roof.

Building Systems

Buildings should be compartmentalised as to their use within the business. For example, the finance area, the factory floor and the final products area. Each area should be protected by automated access management systems during working hours, and intrusion detections systems during out of hours. CCTV should operate in support.

a.Access Control - All access should be through a designated and controlled access point. You should ensure that only those authorised can enter your business or specific areas. All members of staff and resident contractors should be issued with and wear a company specific identification card. Temporary contracts or visitors should be required to produce evidence of their identity before being issued temporary entry badges.

Members of staff should be encouraged to challenge anyone not wearing a badge. It may be necessary to establish an entry/ exit search procedure. Access points into your business should be kept to a minimum and avoid allowing staff to use shortcuts or designated fire escapes.

b.Alarm Systems – It may be necessary to install an alarm system to cover all external doors, windows and roof access. If budgets are tight, it may be worth considering just monitoring your vulnerable areas, or areas you think are likely to be breached. You should try and place your alarm detection as far away from valuable assets as possible.

Ensure you have implemented a preventative maintenance program, ensuring all repairs are carried out in a timely manner. Sensors employed in intrusion detection systems typically fall into one of three categories:

i.Shell sensors - these are designed to detect break-through of doors, windows and, if necessary, conduits, roofs and walls.

ii.Volumetric sensors - These monitor the internal space of a building, looking for changes against the pre-established background. Some are active, generating a positive detection field; others are passive, looking for changes in heat typically associated with human bodies.

iii.Target sensors - these are installed on specific at-risk or high-value objects, whereby if the object is touched, picked up, or even sometimes approached, they will generate an alarm.

The best systems are those that employ a combination of the various sensor types to provide redundancy and to overcome inherent weaknesses.

c.CCTV Surveillance - It may be necessary to use CCTV surveillance, but this should be decided on a site by site basis. If it is used, it should be used to cover likely routes of entry/ exit and vulnerable points or areas. Where CCTV is installed, signs should be prominently displayed. You should ensure that only authorised persons should have access to recordings, which should be retained for a minimum of 14 days. A preventative maintenance program should be implemented ensuring all repairs are carried out promptly.

d.Lighting - Good illumination coupled with CCTV surveillance will also help deter adversaries. Building facades should be illuminated to at least 5 Lux, and preferably 20 Lux. The decision to increase illumination of doors must be carefully considered as it may alert an adversaries to the existence of a target.

Key Control

Controlling who has use of keys is essential and a procedure should be established to issue keys only to designated and authorised persons upon signature. All keys should be controlled from a central location, if possible, and a register documenting all key issues and returns should be kept. It is also worth thinking about procedures to control duplication of keys and the periodic rotation/ replacement of locks.

High Value Items

Much better security can be achieved by concentrating your high value items or business critical items in one central location. Your strongest physical barrier should be closest to the target, so you should consider using a safe or a strong room. The items should be kept out of sight from anyone not needing to know of their existence and access to them should be strictly controlled. If they are used in day to day operations, they should be securely locked away when not in use.

Shredding

destroying your confidential information at the end of its life cycle is essential to the modern business. Aside from the hefty fines that can be levied, it's just good business sense to keep information secure.

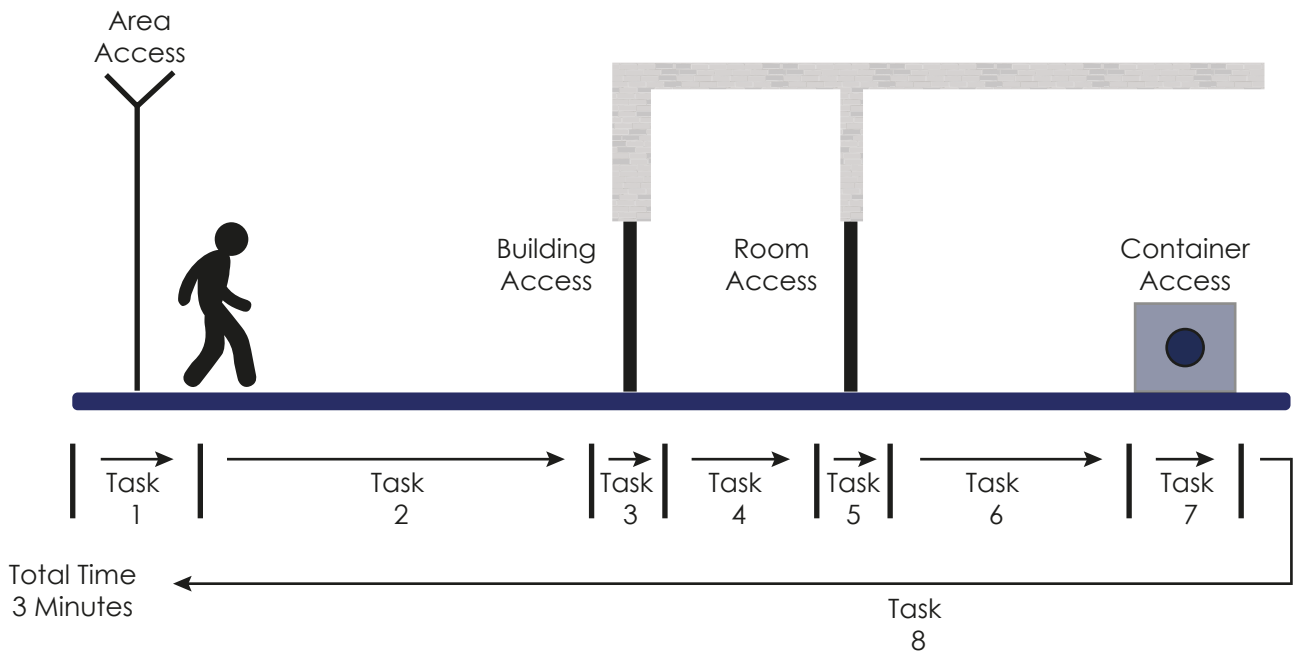
Day and Night

Unless you run a 24 hour operation, it is important to note that there are two regimes to consider when protecting property- working hours and outside working hours. Each has their own security challenges. The table below highlights some common challenges and solutions.

Regime	Challenges	Solutions
Working Hours	<ul style="list-style-type: none"> • More access points in use • Intruders can infiltrate in the guise of employees, contractors or customers • Employees can be the source of criminality 	<ul style="list-style-type: none"> • Emphasis on deterrence • Layered access management • Monitoring for deviations • Security awareness programme
Outside Working Hours	<ul style="list-style-type: none"> • Employees routinely forget to lock buildings and filing cabinets correctly • Valuable company property, including cash, is often left out overnight • Keys are left hanging out in full view • Employees are often not aware of the value of information put in bins • Out of hours cleaners have access to sensitive areas 	<ul style="list-style-type: none"> • Emphasis on barriers, locks, intrusion detection and response • Compartmentalise areas of the business • Assign responsibility for locking up routine • Carry out an after hour's inspections • Remove cash from site at the end of the day.

Beyond Baseline

The baseline protection measures will go a long way to protecting your assets, particularly against opportune criminals or those with little or no tools. However, organised criminals will be more prepared, so you need to be able to detect when your protection measures are being breached.



Task	Mean Time (Minutes)	Cumulative Time (Minutes)	Task description
1	0.1		Climb over fence
2	0.3	0.4	Run 25M
3	0.8	1.2	Force Door
4	0.4	1.6	Walk 15M
5	0.2	1.8	Cut lock
6	0.1	1.9	Walk to container
7	0.2	2.1	Open container and gather materials
8	0.9	3.0	Escape
			Total (3 minutes)

Alarm & CCTV Monitoring

Going beyond the baseline security measures, should give you the earliest possible notifications that something is not right. Alarm and CCTV monitoring can be extremely effective if used correctly. Any alert generated from your systems must be identified, confirmed and a proportionate response initiated in the quickest time possible.

Keyholding & Alarm Response

The main reason for placing your security detection as far away from a possible target as possible is to give you the maximum amount of time to intercept an intruder and stop him carrying out his act. The picture above illustrates the speed an intruder can gain access to a target.

A keyholding and alarm response service can respond in a timely manner day or night and prevent a criminal carry out his act. The service will also mean that you are not putting a member of your staff into harm's way. But remember, the key to a successful alarm response service is getting to the alarm before the criminal has time to complete his act and escape.

Security patrols

Security patrols can be a very useful service in high risk areas that are known to be targeted by criminals, such as large industrial estates. The role of the security patrol is to disrupt any likely criminal act. By either preventing the criminal starting his act or disrupt him early in the act. Security patrols can also be used to ensure the premises is locked up at the end of the working day and opened in the morning. It can also be doubled up with a keyholding service.

Security Guarding

Overreliance on security guards can be a mistake; they are expensive and sometimes they cannot be relied upon. However, security guarding can be very effective if used correctly. Integrating them with your security systems becomes a force multiplier and combining the role with other tasks onsite soon adds value. However, the role and the guards should be reviewed on a regular basis.

Summary

I hope you have found this document of use. Remember, this document starts with the basic of security, the things you should do irrespective of the level of risk, and then goes onto further information about building resilience into your security plan. However, the most effective way of protecting property and equipment is a balance of **Physical, Operational, Technical** and **Educational** measures.

If you would like to discuss ways we can help build an effective and balanced security plan, then please get in touch.