ecclesiastical

Bulletin

Property Security and Theft Prevention: A Practical Risk Management Guide

Safeguarding property from theft and the damage that often accompanies it is a critical responsibility for any organization or individual. The loss of assets, whether physical goods, equipment, or valuable information, not only creates immediate financial strain but can also disrupt operations, compromise safety, and undermine long-term stability.

Introduction

Theft-related incidents frequently lead to additional property damage, magnifying both the cost and complexity of recovery efforts. By implementing robust preventative measures, strengthening security practices, and promoting awareness among stakeholders, it is possible to significantly reduce these risks. Effective property protection is not simply a reactive measure; it is a proactive commitment to preserving assets, ensuring continuity and fostering a secure environment.

Security

Generally, the more valuable and portable an item, the more attractive it will be to thieves. Deterrence is key to security and can be achieved through a combination of measures, including physical and electronic protection, surveillance, and security marking of items to make them difficult to dispose of. The saying 'out of sight, out of mind' also applies, as limiting access to areas where items are stored or displayed can enhance their security. Theft can result not only in the loss of assets but also in significant property damage from forced entry. To reduce this risk, it is imperative to develop a security plan that safeguards your premises and enables the detection of unauthorized visitors.

Security assessment

- To establish appropriate security measures, a security assessment should be conducted to identify theft risk. This should consider factors such as risk of property damage, as well as the value, portability, location and existing security measures for each asset.
- When conducting the assessment, begin at the site perimeter and work inward, progressively increasing protection measures. This approach makes unauthorized entry more difficult by adding measures such as surveillance systems and intruder alarms.

Perimeter / site security

Surrounding a building with substantial fencing or walls can enhance security and act as a psychological barrier by clearly demarcating the site, making intruders aware they are trespassing. However, this should not compromise external surveillance of the property. Where possible, solid barriers such as brick walls, which provide concealment once scaled, should be avoided. Perimeter fencing should be at least 2.4 metres high to provide effective security.

Common types of perimeter barriers available, from most effective to least, include:

- **Steel palisading** is substantial yet maintains visibility, making it the most effective perimeter barrier.
- **PVC/powder coated expanded metal fencing** is difficult to breach and maintains visibility, but it can be vulnerable at the fixing points to fencing posts.
- **Timber panels** are economical to install but once scaled, provide only a visual screen and offer little resistance to physical attack.
- **Chain link fencing** is readily available, inexpensive, and easy to install. However, it distorts easily and can collapse when cut and is generally unattractive in appearance.

Where perimeter fencing is installed, matching gates should be installed to maintain security. Gates should remain locked outside business hours, preferably using a hardened steel bar and a closed-shackle padlock. Perimeter fencing and walls should be routinely inspected for breaches and promptly repaired or reinforced as necessary.

Barbed and razor wire, broken glass, or any other sharp item should not be used for perimeter protection.

Contractor / visitor controls

There should be clear signs directing contractors and visitors to the reception area, while all unauthorized access points remain locked or supervised. For larger premises, or where contractors are not continuously supervised, identity badges must be issued upon arrival and collected at the end of each day.

Contractors working on-site for multiple days must obtain and return an identity badge each day. Vehicle details, the staff contact person, and arrival and departure times should also be recorded.

For contractors not previously known, official identification must always be requested and verified. Visitors and contractors should use only one designated entry and exit point, and they should not be allowed to leave the site without first signing out which is witnessed by a member of staff.

Vehicle access

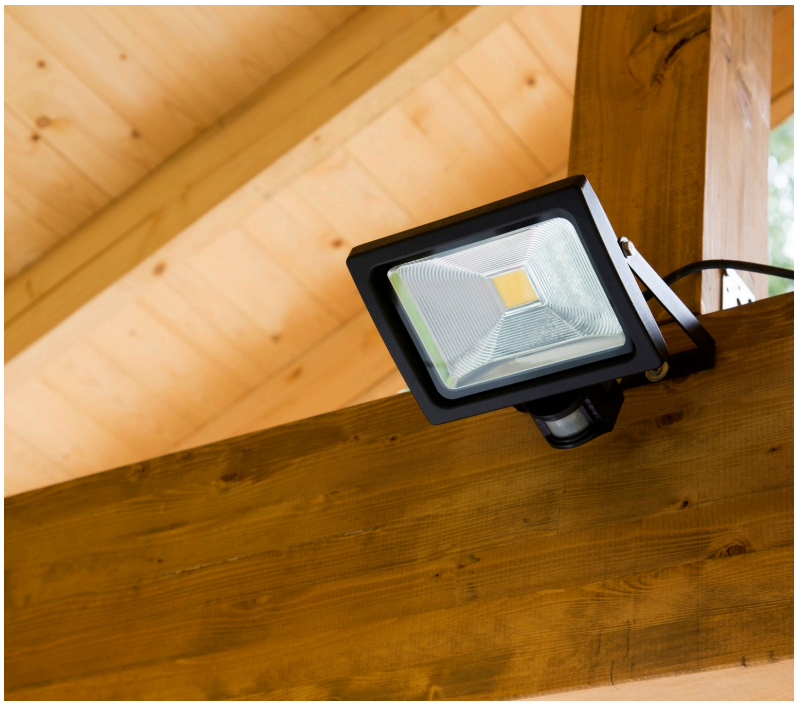
Vehicular access points should be restricted wherever possible. Retractable bollards or one-way plates can provide a more aesthetically pleasing alternative to unsightly barriers. Designated parking areas should be clearly signed, well illuminated, and located outside secure areas of the property. License plate number recognition cameras at vehicular entrances can also serve as an effective theft deterrent.

Security lighting

Security lighting may be operated by timer, photo-electric cell or passive infrared unit. Without adequate surveillance, however, lighting can assist intruders rather than deter them. Security lights must be carefully positioned to provide uniformed lighting and avoid shadows or gaps where intruders could conceal themselves.

Landscaping

Avoid creating accessible hiding places or natural ladders to upper floors. Planting prickly shrubs can help deter trespassers from vulnerable areas.



External metal

Metal items on the exterior of a building are often targets for theft. Roof coverings, lightning conductors, pipework, electrical cabling, statues, and AC fan coils are all at risk. Financial losses extend beyond the value of the stolen metal, encompassing damage to the building during the theft and potential water damage to internal furnishings if roof coverings are removed and rain occurs before discovery.

Access Control

Access to the property should, where possible, be restricted to a manned reception. Unsupervised doors should be self-closing, self-locking and preferably free of external fittings. Additionally, security can be provided through digital keypads or electronic access control locks, which require a known code, authorized swipe card, proximity fob, or biometric verification. The advantage of access control locks is that codes can be easily changed or de-activated if cards or credentials are lost or staff leave your employment. As these locking mechanisms offer limited physical strength and security, they should only be used as a secondary locking mechanism. The number of keys issued should be kept to a minimum, with a key register maintained. Copying of keys by staff must be strictly prohibited. A key numbering system should be used instead of having identifying labels. You should consider using high security, patented key systems where keys cannot be duplicated without authorization, and key blanks are controlled by the locksmith or manufacturer.

For guidance on the appropriate levels of protection and performance of an Electronic Access Control System, refer to CAN/ULC 60839-11-2:2022 – *Electronic Access Control Systems – Application Guidelines.*

Keys kept on site must be stored securely to prevent unauthorized access. Where a significant number of keys are held, install a proprietary key cabinet in a secure, central location, out of sight from visitors.

Physical security

Where possible, external doors should be constructed of solid timber or steel, be at least 45mm thick, and be secured by a mortise or cylinder rim lock. When deciding on which locking system is most suitable for your property, it is recommended to seek the opinion of a locksmith or local crime reduction officer.

Doors not used as final exits or designated fire doors can be strengthened by fitting two mortice rack bolts or two key-operated security bolts in addition to existing fastenings. Outward-opening doors are vulnerable due to exposed hinges; hinge bolts should be installed near the hinges to prevent the door from being lifted off.

The protection of vulnerable doors can be improved by fitting a secondary barrier, such as a roller shutter or gate, provided that fire exit doors are not compromised. Existing doors may also be reinforced with sheet steel or timber linings.

Accessible, opening windows should be secured with proprietary key-operated window locks or restrictors limiting their opening width to no more than 100 mm. In high-risk theft areas, consider installing fixed internal bars or sliding/collapsible grilles to secure windows.

The protection of skylights and roof lights should not be overlooked. In vulnerable or readily accessible areas, these should be secured internally with metal bars or grilles.

Egress doors must prevent unauthorized access without compromising emergency egress. They must unlock with a single operation, allowing occupants to exit easily, and must open in the direction of travel. Where doors also serve as entry points, locks may be keyed externally for access control.

Any securing and releasing devices used on egress doors must comply with CAN/ULC-S533 — *Egress Door Securing and Releasing Devices.* Reference can also be made to NFPA 101, Life Safety Code

The National Building Code of Canada (NBCC) and National Fire Code of Canada (NFCC) govern many aspects of building construction related to fire and life safety. Each province adopts adjusted versions of the NBCC and NFCC. For clarification, consult your provincial Building and/or Fire Code.

The American National Standards Institute (ANSI) and Builders Hardware Manufacturers Association (BHMA) established performance and durability standards for door hardware products under ANSI/ BHMA A156. This accepted benchmark can be used to ensure you have the appropriate door hardware for varying door applications.

Target areas

Targeted areas including areas containing high-value, easily disposable portable equipment such as laptops and computer tablets should, where possible, not be located on the ground floor. Doors should be constructed of solid timber at least 45 mm thick and secured with mortice deadlocks or cylinder rim locks. Accessible opening windows should be secured using key operated window locks as a minimum, but with internal bars or sliding/ collapsible grilles if possible.

These areas should be kept locked when not in use and access strictly controlled.

Where adequate physical security measures are difficult to implement, intruder alarm protection should be considered for specific vulnerable items. High value portable items should also be security marked and/or electronically tagged to deter theft.

Intruder alarms

In addition to localized sounders, intruder alarm systems should also incorporate remote signaling to inform authorized persons of an intrusion to the premises. Where fitted prior to September 2014, systems should have been installed in accordance with CAN/ULC-S302-M91 (R1999).

From 2014, all systems should be installed in accordance with CAN/ULC-S302-14 - Standard for the Installation, Inspection and Testing of Intrusion Alarm Systems and CAN/ULC-S304:2016 - Standard for Control Units, Accessories and Receiving Equipment for Intrusion Alarm Systems.

Remote signaling systems should contact the alarm company's alarm receiving center, which conforms to CAN/ULC-S301:2018 – Standard for Signal Receiving Centers Configurations and Operation.

You should have your intruder alarm system installed and maintained by a ULC listed company Be aware of your municipality bylaws or local police department procedures as intruder alarm regulations vary by jurisdiction. Some municipalities may require formal registration of intruder alarm systems.

Closed circuit television (CCTV)

Where the size and complexity of your premise and site make effective surveillance difficult, CCTV can be an effective deterrent to intruders. CCTV enables continuous monitoring of areas through cameras linked to digital recording systems or observed by security personnel.

KEY CONSIDERATIONS INCLUDE:

- Camera quality can vary significantly
- Systems can be costly
- Effective monitoring is essential
- Coverage is limited to the camera's field of view
- Data protection, civil liberties, and human rights must be respected

Despite these limitations, CCTV is particularly effective for monitoring car parks and main entrances.

For guidance on design, installation, and performance, refer to CAN/ULC-S316 - *Standard for Performance of Video Surveillance Systems.*

Security guarding

Where theft risk is high, the use of security personnel should be considered. Guards may be employed in-house or contracted from licensed security providers. In-house guards must hold the required license under the applicable legislation in your jurisdiction. In Ontario, guidance is provided by the Private Security and Investigative Services Act, with equivalent regulations in other provinces and territories.

The use of armed security guards requires proof of a legitimate risk to life or property that cannot otherwise be mitigated. In Canada, all armed guards must be employed by a licensed armed security company and must hold both a Possession and Acquisition License (PAL) and an Authorization to Carry (ACT) permit issued by the Royal Canadian Mounted Police (RCMP).

For effective guarding and patrolling, checkpoints should be established at key access points and high-risk areas, including entrances, exits, and important internal locations such as cash storage areas. Incorporating randomized checkpoints in addition to fixed patrol routes enhances oversight and deters predictable patterns.

Conclusion

Effective building security requires a layered approach that combines physical reinforcements, access control measures, detection, surveillance, and personnel oversight. Attention to vulnerable points such as doors, windows, skylights, and high-value asset areas is essential, supported by compliance with relevant codes and standards. Where physical measures are limited, electronic systems and trained security staff provide additional protection. Together, these strategies help deter theft, safeguard property, and ensure the safety of occupants and assets.