



SECURITY IN DESIGN

When people think about security in buildings or facilities they think of security guards, CCTV, access control cards and ID badges. All of these security measures can be effective in supporting security. However, the level to which these types of measures are relied on can be affected by the level of security offered by the basic design of the building.

IT'S important to take into account that if the design of a building is inherently non-secure, then more reliance is put on additional electronic, physical and procedural security measures. When a building or facility is being designed, security is generally not a consideration, unless the facility is a prison or a bank.

Security is often not considered until the architectural design is completed. Whatever security 'holes' are left by the design are then dealt with, generally with electronic and physical security measures that are 'tacked-on' to patch the problems. In some cases, security holes created by the design aren't recognised until the building is finished, in which case it is generally too late to correct them.

In some cases, add-on security measures can be effective in patching a hole in security. However,

design issues can present on-going problems regardless of the addition of security measures. Adding security measures to support a non-secure design can be an on-going, frustrating and expensive exercise.

SECURITY IN DESIGN

The design of a building or facility can contribute greatly to the security of people and assets in and around it. It can also contribute to the building's occupant's perception of their own safety, freeing them from fear and distraction from their work. Design strategies can mitigate many potential issues including: Break-and-enter, armed hold-up, theft, internal theft, fraud, graffiti, vandalism, workplace violence and assault.

CPTED (Crime Prevention Through Environmental Design) is based on embedding safety/security into the built environment. CPTED suggests that opportunities for crime can be reduced by maximising opportunities for Natural Surveillance, Territorial Reinforcement and Natural Access Control.

Natural Surveillance is about maximising opportunities for surveillance by authorised users of the space. This can have several beneficial effects. It contributes towards authorised user's perceived safety, and increases risk perceived by intruders, because they feel more likely to be seen, challenged or caught. Maximising Natural Surveillance can reduce the necessity for electronic surveillance (CCTV). Maximising Natural Surveillance can also assist electronic surveillance by providing clear, open views.

Territorial Definition is about facilitating ownership of space, ensuring that users of a space



are given clear indicators of what is public space, semi-private space and private space, and providing indicators of what are the desired behaviours permitted in each space.

Natural Access Control is about limiting or deterring admittance to spaces. This can be achieved in numerous ways, for example: channelling users of a space into areas (or thoroughfares) with good Natural Surveillance, using elements of the built environment to act as barriers and limiting the number of entry/exit points.

DEFENSE IN DEPTH

Defense in Depth is another concept that can enhance built-in security. The Defense in Depth concept suggests that security should not rely on any one security barrier/measure. For example, compromising one barrier (or security measure) should not provide an intruder with access to an entire facility. Rather, Defense in Depth suggests that security measures should be layered in succession, and most critical assets should be located centrally to provide maximum protection.

If security is considered early in the design stage, it is possible to identify potential issues that could save a lot of money, time and effort by avoiding on-going security measures to fix problems after a building/facility is established. As a simple example: a door does not require a reed switch

alarm, access control reader, CCTV monitoring, procedural-lock-up by a guard etc, if there is no door in the first place. Further, intruders cannot use a door as a point of entry if it does not exist. Non-essential doors or poorly located doors can create security problems that could be avoided simply by removing or re-locating a door in the design stage of a building or facility.

Significant savings can be made by removing the necessity for (or reducing the numbers of) CCTV cameras and digital-storage space, electronic access control points and numbers of guards or patrols etc, not to mention on-going costs associated with issues like internal theft, robbery, vandalism, graffiti removal, compensation claims or litigation.

An early minor investment to ensure security issues are considered during the design stage of a building or facility can improve the quality of life for a building's occupants, minimise frustration, minimise loss and provide significant savings in the life-cycle cost involved with the management of a facility.

** Simon Hensworth is a senior security professional with global engineering consultancy GHD based in GHD's Defence and Security stream - Asset Protection Group located in the GHD Perth Office. T: 61 8 6222 8640, E: simon.hensworth@ghd.com.au*