OMNIRISC
REDEFINING SECURITY

Security Newsletter

APRIL 2018 I ISSUE 8

The various physical security processes are designed to **deter, detect and delay** unauthorized entry to or wrongful actions within a facility. In this issue we will continue to examine the physical security element of access control that is used to keep ourselves and our properties safe.

The various elements of physical security systems include:

- Overall and continuing threat and risk assessments.
- External perimeter and building security including locks and alarms.
- Security of internal sub-spaces
- Staff, visitor and vehicle access controls.
- Electronic surveillance.
- Human guarding
- Security control and management services.
- Security lighting
- Security incident response.
- Close protection of key staff
- Security, crowd control and safety of large-scale events and gatherings

Access Control

All buildings and facilities have a number of entry points for pedestrian access and usually have a larger number of other exits for emergency evacuation purposes. In addition, many have access for vehicles. These various access points are secured and managed in a variety of ways.

The following types of access to a building or facility need to be considered, as each one requires differing security management strategies.

- Employee access.
- Visitor access.
- Employee vehicle access.
- Visitor vehicle access and
- Delivery vehicle access.

Generally, the different security management strategies required to deal with these can be described as either closed or open, although sometimes a combination of both are used. **A closed access control system** will control all access to the building/facility at its physical boundary. **An open access control system** will allow initial access to the building/facility with subsequent internal control being exercised by the internal space holder.

A Closed Access Control System

Example 1

An example of a closed system would be an office complex that possibly includes:

Companies in the gaming and integrated resorts (IRs), financial services industry and Companies seeking high-end security services

This complex would ensure that various perimeter control points are operated to ensure that employee access is controlled. That authorized visitors are channeled, controlled and properly escorted. That if appropriate, authorized vehicles are permitted to park and their occupants checked through the full access control processes and that only authorized delivery vehicles are permitted to enter the building or facility.

With a closed system, the following types of access generally require differing security management procedures.

Employee access: Authorized employee access is often [but not always] by way of a separate employee entrance to the facility. This access is usually controlled by manned security services with a variety of identification methods used. It is sometimes also augmented by a number of physical barriers. [See examples below]

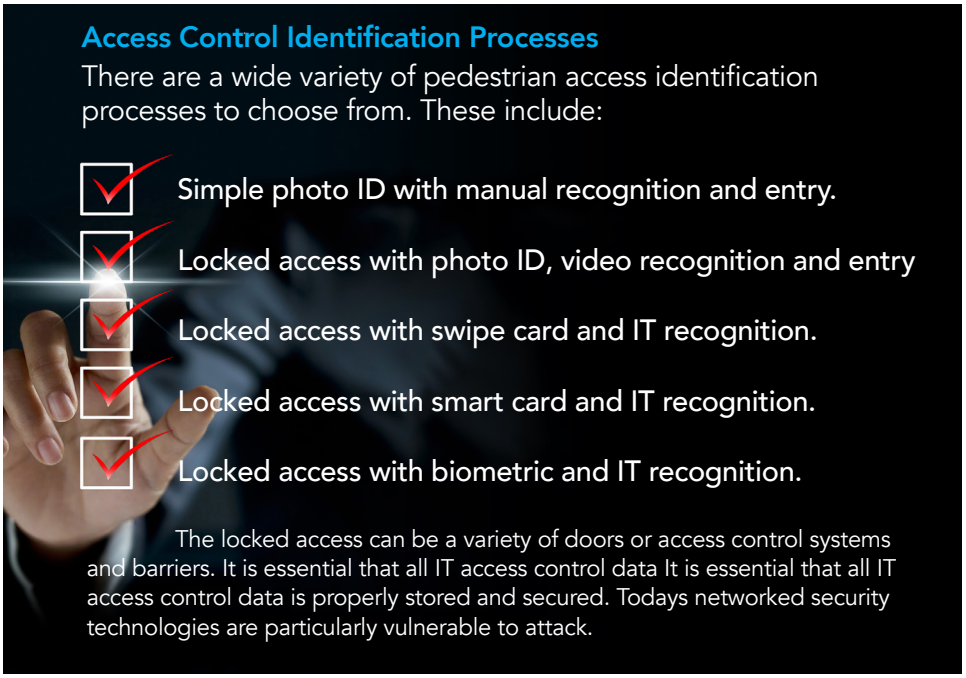
Visitor access. Authorized visitors should be channeled to, checked and managed at a single point e.g. the main entrance. Once their identity is confirmed, they should be issued with clear visitor identification and directed to the area they wish to visit. If necessary they should be escorted to that area and handed over to a responsible person.

Employee vehicle access. If employee's private vehicles are permitted within the complex. Their access to the complex perimeter should be checked or controlled by smart card access. The occupants should then join the normal employee entrance procedures.

Visitor vehicle access. Similarly, authorized visitor vehicle access should be controlled and the visitor directed to the normal visitor access location.

Delivery vehicle access. All delivery vehicles should be expected and authorized before access is permitted and their deliveries should be checked by the recipient department. All vehicles should be checked by security before departure.

OMNIRISC SECURITY SERVICE (MACAO) LTD. 26 Avenida De Marciano Baptista, Chong Fok Comercial Centre, 12/H, Macau
Office: +853 28558964 Email: info@omnirisc.com
www.omnirisc.com



Access Control Identification Processes

There are a wide variety of pedestrian access identification processes to choose from. These include:

- Simple photo ID with manual recognition and entry.
- Locked access with photo ID, video recognition and entry
- Locked access with swipe card and IT recognition.
- Locked access with smart card and IT recognition.
- Locked access with biometric and IT recognition.

The locked access can be a variety of doors or access control systems and barriers. It is essential that all IT access control data It is essential that all IT access control data is properly stored and secured. Todays networked security technologies are particularly vulnerable to attack.

An Open Access Control System

Example 2

An example of an open system would be a casino complex that includes:

Integrated Resorts (IRs)
Gaming floors
Cash holding areas
Convention and Exhibitions
Food and beverage outlets
Retail outlets
Jewelry outlets
and Sporting facilities

Most of these areas operate under an open access control system with general public access and less obtrusive security oversight. While some, such as gaming floors and cash holding areas operate under much greater security scrutiny.

In an open system, the Individual outlets are generally responsible for their own security based on their own threats and risks. Although the facility is usually covered by the casinos security services it is likely that a jewelry outlet would require additional security coverage.

Emergency Exit Points

All facilities/buildings have a number of additional emergency exit points for fire and evacuation purposes. These are usually kept closed and locked and are not generally used for entry. [although some organizations do use them as entry points]

There can be a tendency amongst employees to wedge open emergency exit doors for convenient movement. This defeats an access control plan and should be discouraged by regular security patrols and by the fitting of door opening sensors and alarms.

Emergency exit doors should be outward opening and fitted with push bar [panic] locks for ease of exit. Where doors are secured with code, combination, swipe or proximity card locks they should be capable of being overridden by the push bar type.

Evacuation routes and door locking mechanisms need to be checked regularly to ensure the routes are free of obstruction and that the emergency door locks function properly and efficiently.

The Threat From Within

The effective use of a well-designed and managed access control system can ensure that any external threat to your organization is minimized if not prevented. But what of the internal threat from authorized entrants? This needs to be taken into account.

To guard against insider misconduct or criminal activity, organizations need to establish multiple layers or concentric circles of physical security. These should provide additional access controls to ensure that only authorized and necessary individuals are admitted to the particular area. The access control systems described above are an initial step. These then need to be multiplied and deployed again to protect vulnerable facilities, equipment and data.

Effective Security Training

Even in the best run organizations with highly developed security systems, humans can be the weakest link. Through laziness, mistake or misconduct, employees can jeopardize an access control system in an instant.

To counter this, an organization needs to have effective security policies that are known to and fully accepted by all employees. Staff need to be fully trained in the system and adhere to the policies therein and security departments need to be proactive in seeking out and resolving breaches of the access control protections.

Access Control Audits

All organizations with access control processes need to regularly check and audit these to ensure continued compliance.

Violations of access control can include:

- Loaning of keys/cards to third parties
- Transfer of keys/cards without authorization
- Unauthorized duplication of key/card information
- Failure to report missing keys/cards
- Propping doors open
- Admitting unauthorized persons into the building
- Admitting unauthorized vehicles into the building
- Failure to report damaged locks or doors
- Leaving IT passwords in view
- Misusing IT passwords
- Downloading excessive amounts of data
- Failure of security staff to properly manage the access control system

Any violations should be reported by staff and need to be picked-up and resolved in a timely manner by security personnel.

Regular auditing by the security department and the occasional independent audit of all access control practices and procedures by an independent organization will ensure that the access control procedures continue to be effective and fit for purpose.

In subsequent issues we will continue to examine further aspects of physical security and security auditing such as electronic surveillance, human guarding and security control and management.

About the Author

James Langton, is an advisor to "OMNIRISC SECURITY" with over 40 years' experience in the security and law enforcement industries.