



MAKING AN ENTRANCE

Iain Entwistle looks at why advances in technology means that security portals are now better able to complement manned guarding.

Whether it's just one person or several hundred people in a building, they are all vulnerable to criminals who gain unauthorised access. Items being stolen or staff being attacked are the dangers of cutting corners when it comes to physical entry barriers. Traditionally, larger premises have relied on manned reception and security teams, although as criminals become more

sophisticated or simply tailgate their way in by closely following the person in front, specifiers are looking at ways technology can improve security.

One of the most vulnerable times of day, according to a recent police report, is early evening when there are fewer people around. It is relatively easy for a criminal in multi-occupancy buildings to make themselves look like a legitimate office worker and then simply tailgate their way in. Once inside they

are then able to steal valuable property or hack into IT systems where they can cause irreparable damage.

Criminals are very adept at finding a building's weak point in the perimeter security in order to gain entry. For instance, they can sometimes force open magnetic locking doors or tailgate through a security door. Once unauthorised access occurs it is almost impossible to confirm who has the right to be in the building and who does not without rechecking everyone's ID badge or card, biometrics or pin. Criminals often rely on the fact that they are unlikely to be challenged as they move around the building.

As a result, technology is increasingly being used to support manned guarding teams and reception staff, where it can be incorporated into physical entry barriers such as security portals to prevent unauthorised entry. At the same time, any entry barrier needs to be able to withstand a physical attack by determined criminals who are prepared to use tools such as hammers, crowbars and saws to gain entry.

NO MORE COMPROMISES

That meant, until relatively recently, that compromises had to be made between safeguarding building occupants and retaining aesthetics of the entrance area. Security specifiers could specify a low-level security solution that looked aesthetically pleasing, such as a glazed revolving door. However, these aren't designed to resist a forced entry attempt and would not meet LPS 1175, nor be suitable for wheelchair access or specify an LPS 1175-approved doorset that creates a robust physical entrance barrier, but won't prevent tailgating. In addition, they usually have minimal glazing, look imposing and lack aesthetic appeal.

LPS 1175 security portals overcome all these limitations because they have been assessed against a known level of physical attack. In addition, if the security portal incorporates an APD (Anti Piggy Backing Device), which scans the portal with an ultrasonic sensor to ensure that only one person has entered at a time, it will prevent tailgating. If more than one person is present in the portal, an alarm is triggered and the transit is then denied. APD is therefore highly capable of detecting whether there is more than one user in the portal at any one time. In larger portals, a two-zone pressure mat is additionally incorporated to add an extra verification parameter, which requires the person to stand on a specified zone when inside.

Security portals are a good choice where 24/7 unmanned access control is required or can be used in conjunction with a security team and here an alarm is triggered if anyone attempts to make an unauthorised entry. This means the security team does not have to be permanently in the immediate vicinity of the entry point.

Richard Flint, LPCB's Physical Security Certification Scheme Manager, notes: "When assessing the overall level of risk, correctly specified security products are critical in protecting buildings and their users against crime. We encourage the use of LPS 1175-approved products wherever possible because it hardens premises against criminal attack. Specifiers should refer to the LPCB Red Book when looking for LPS 1175-approved security portals and other physical security products. Security portals certified to these standards are able to resist experienced attempts by criminals at forced entry using a wide range of tools."

He adds: "LPCB's LPS 1175 standard sets the bar in providing specifiers with confidence in specifying physical entrance security able to withstand forced attack. Specifying an independently third-party tested LPS 1175 product provides confidence the product will perform as claimed, whereas untested products may not perform as expected."

When it comes to attack from fire, very few portals are able to offer any real kind of resistance. Fires in the workplace can lead to loss of life, serious injury or irretrievable data loss and have a devastating impact on businesses. Some organisations never recover from a fire especially if it spreads quickly. When specifying a fire-rated security portal it should provide fire protection and smoke control from both directions as per the European Fire Resistance norm: EN 13501-2 and EN 1634-1: 2014. Gaining fire rating on both sides of the flat side doors provides specifiers with the assurance that the portals will perform exactly as tested and from both directions.

The FPJ140 2SF and FPJ140 1AF security portals provide fire protection and smoke control on both sides of the flat side doors for up to 60 minutes,

ACCORDING TO POLICE ONE OF THE MOST VULNERABLE TIMES FOR ENTRY IS EARLY EVENING

conforming to EI60. At the same time they are available with attack-resistant glass, making them an ideal entrance control solution for any secure area. The FPJ140 1AF fire-rated security portal features a manual swing door with automatic sliding curved doors and provides resistance to fire for up to 120 minutes to EI120. Both can be customised to suit individual client requirements with different types of finish options available as well as the integration of third-party devices. Battery backup is also provided, so in the event of power loss the units will remain operational for up to six to eight hours.

FIRE-RATED SECURITY

Fire-rated security portals are an effective way of maintaining the integrity of the fire line and slowing down the spread of fire, while keeping the premises or sensitive areas within, such as data centres and server rooms, secure from unauthorised personnel. Unlike fire doors, which generally don't offer any form of tailgating detection, security portals will only allow the transit of authorised users. Any attempt at tailgating behind an authorised user will be detected and the secure side doors will remain locked preventing the transit. The FPJ140 1AF and FPJ140 2SF provide standalone solutions combining both attack and fire resistance along with tailgating detection in a single unit.

It's worth bearing in mind that it is much more cost effective and less disruptive to prevent unauthorised access by criminals in the first place. An effective way of doing this is to specify a security portal that incorporates anti-tailgating measures or, where forced attack is a possibility achieves LPS 1175-approval and Secured by Design requirements.

Once illegal access has been gained, it's pretty much impossible to spot an intruder

It's one of the reasons why specifying products that are approved to this standard is a requirement on projects in many different sectors including education, finance, healthcare, manufacturing, the public sector, residential, retail and utilities.

Although often caused unwittingly by staff, unauthorised entry through tailgating can lead to serious issues for businesses. It's worth remembering that you can install the most advanced CCTV, alarm and IT security system available, yet all of it will be rendered pointless unless you tackle this simple issue first. Often it is only technology that can do this because it allows single-person verification.

The consequences of not taking action could have wider reaching results. Conversely, taking steps to address the issue with an LPS 1175 or Secured by Design security portal that is capable of preventing unauthorised entry can create a sense of enhanced safety and wellbeing with staff. Irrespective of how many people are in the building, if a risk assessment identifies that a person could gain unauthorised access, it is your responsibility to ensure that they are stopped in their tracks ●

SECURED BY DESIGN

Secured by Design (SBD), the national police crime prevention initiative, seeks to improve both the security of buildings with security-related products, like doors and windows that meet its Police Preferred Specification standard and incorporate crime prevention techniques and measures into the layout and landscaping of the immediate surroundings.

SBD's Police Preferred Specification accreditation requires products to be tested independently against rigorous physical attack under United Kingdom

LPS 1175 SECURITY STANDARD

LPS 1175, or to give it its full reference – Loss Prevention Standard 1175, is an important security standard. It relates to requirements and testing procedures for the Loss Prevention Certification Board (LPCB) approval and listing of intruder-resistant building components, strong point, security enclosures and free-standing barriers. LPS 1175 covers a broad range of physical security products and services, including, for the first time, security portals.

Within the LPS 1175 certification standard there are a number of different ratings associated with the level of security provided by the approved products. For instance, security portals that achieve a Security Rating of SR3 provide resistance to determined attempts of forced entry using a range of techniques and tools such as drills, chisels and crowbars, including those that involve the creation of noise. LPS 1175 security portals are also available with bullet-resistant glazing – BR3/S EN1063 – where extreme levels of force may be used. For some buildings and facilities it may be necessary to incorporate metal detectors into the portal.

Accreditation Service laboratory conditions using a variety of tools – and re-tested regularly along with inspections of the manufacturer's production facilities to ensure that quality has been maintained over time. SBD accreditation requires products not only to have been tested to relevant security standards, but also fully certified by an independent third-party certification body accredited by UKAS. It's worth verifying that the security portal you specify for high-risk areas meets both LPS 1175 approval and SBD accreditations.

Iain Entwistle, Product Marketing Manager at Meesons A.I. Ltd, has a background in security and product development. He has been active in the design, patenting and development of a range of innovative security portals, speed gates and supporting safety technology for the UK and European markets.

Security portals not only create a robust physical entrance barrier, they also prevent tailgating



Picture credit: Meesons