Picture credit: ATG Access Ltd.

URBAN SECURITY

Lucy Ketley *explains the importance of having a focus on access control for public safety*

It has been nearly 50 years since the famous psychologist from Stanford - Philip Zimbardo – launched one of the most influential theories of criminology; the 'Broken Windows Theory'. In his field study, Zimbardo abandoned two identical cars in two very different neighbourhoods. One within a notoriously crime-ridden area of New York City and the other in an affluent neighbourhood – Palo Alto in California. Both cars were parked with their number plates removed and the bonnets open.

Within ten minutes of the cars being placed within New York City, the first was gradually stripped of its spare parts and vandalised; meanwhile the second remained untouched for over a week. Eventually, Zimbardo took a sledgehammer to the car located in California and only then did passers-by give the car the same treatment as in New York City. This theory demonstrated how something which is clearly neglected can quickly become a target for criminality; this became the 'Broken Windows Theory'.

This same theory can be applied to the wider community and urban areas. In a study of over 400 convenience store robberies, one significant difference between stores which had been targeted and those which had remained untouched was the distance from the nearest graffiti.

Whatever the security expertise; be it physical security, surveillance or cyber security, one of the most important factors of ensuring an urban area or community is safe for pedestrians and residents is crime prevention through environmental design. The three questions you need to consider when assessing the environmental design of an area from the perspective of a criminal: will I be seen (surveillance); can I get in and out easily (access) and, does anyone care what happens to the area/target (territoriality)?

If criminality won't be detected, it is easy to conduct. If no-one really cares about criminality happening, the target will be significantly more vulnerable than an area which utilises surveillance, security measures (if appropriate) and presents as being an area where care is taken. Not only can security products such as physical access control barriers help to provide a visual deterrent, but they can also add to the aesthetics and demonstrate the care taken within an area.

Access control barriers are a critical aspect of urban security and play a fundamental role in providing a visual deterrent as well as a working, proven and tested vehicle barrier – protecting against vehicle as a weapon and vehicle-borne improvised explosive device attacks. Behind a physical access control barrier, you will find software, an access control methodology, surveillance protocols and other visual accessories such as traffic lights and signage to inform system interaction.

Having the right combination of physical products, supporting access control software and hardware as well as the 'know-how' to use them correctly will augment the security system and provide the best level of protection for any urban area. Understanding the different pieces and knowing how they come together in a coherent security plan is the best way to ensure that an area has adequate and proportional protection.

Understanding the different pieces and knowing how they come together in a coherent security plan is the best way to ensure area has adequate protection

As with any other aspect of urban security, the first stage is always careful planning. Before knowing how to implement an effective plan, an all-inclusive site assessment will need to be conducted, involving all relevant stakeholders and identifying potential access points and vulnerabilities needing to be addressed. This site assessment should look at every potential vulnerability including the uses and potential future uses of the urban zone in question, as well as the surrounding areas. This of course from the perspective of an attacker – ignoring sentiments such as one-way streets for example.

One of the main reasons for performing a thorough site assessment early in the process is to design plans that work effectively. By identifying every potential weak point and vulnerability being addressed by physical access control systems (and ascertaining how they integrate into a wider urban security plan), a project is less likely to require later adaptations and therefore likely to stay on budget and be more effective long-term.

Security objectives must be clear, areas can be protected using a layered approach. For instance, areas which are constantly subjected to high pedestrian footfall and have a heightened risk of attack are likely to require a permanent protection strategy. Areas used for events might only require protection measures for a short duration. If these events are rare, temporary security measures may be more appropriate. If events happen regularly and within the same urban spaces, a semi-permanent security strategy might be advisable.

Behind each physical access control system is an operating methodology. Without secure protocols to make sure that the physical security solution works as well as it can, the whole thing falls apart and exposes vulnerabilities. After all, any security system is only as strong as its weakest link.

REGULAR SERVICE AND MAINTENANCE ENSURES SECURITY EQUIPMENT FUNCTIONS AS IT SHOULD

When it comes to designing operating methodology, considerations include, establishing parameters for entering and exiting an area; implementing strict procedures to ensure correct system use; the implementation of authorisation mechanisms, such as cards, biometrics or PIN codes – proportionate to the level of security necessary and finally, creating a hierarchy of access privileges based on roles and responsibilities of different stakeholder groups. The final step, but far from least important in access control strategies is continuous monitoring and surveillance.

Deploying surveillance cameras at access points not only assists stakeholders such as the emergency services, but also provides supporting evidence for any unauthorised access attempts, adding to security surveillance strategies. Having adequate and proportionate surveillance systems in place will assist in keeping an audit trail if necessary and provide real-time evidence should it be needed in the event of security breaches.

It is important to consider the regulations and standards that are needed when designing and specifying a physical access control system. If the system is being utilised for hostile vehicle mitigation, the physical barrier chosen will need to comply with internationally recognised impact test standards (ISO 22343, IWA 14-1 or BSI PAS 68). The relevant risk profile should be highlighted during site assessment stage, which in turn will inform the security rating required on any mitigation products being planned. Manufacturers should be able to share all relevant testing results and criteria for any products proposed.

In addition to the physical barrier being appropriately rated, the operating systems/protocol behind the barrier should also meet the relevant standards. This applies when placing an automatic system into a public highway and is also applicable to any monitoring systems to ensure the right security credentials are in place to prevent perpetrators from accessing software to circumvent physical security systems.

When specifying physical access control equipment, it is often the case that additional physical

components which are fundamental to operation are forgotten about or overlooked. In addition to the physical barrier (certainly when placing such systems within a public highway), a cabinet to house the hydraulic pump unit (HPU) and the system PLC is required and should be placed (ideally) within 25 meters of the physical access control system. Traffic lights and warning signs are also required to ensure safe system transactions. These additional elements require thought, careful placement and possibly some security as standalone items (LPS 1175 for example) to ensure systems are not able to be compromised.

ACCESS CONTROL BARRIERS PLAY A VITAL ROLE IN PROVIDING A VISUAL DETERRENT

Following the completion of specification and system design, plans that have been developed can be implemented which involves planned execution and installation. Once installed, it's important to think about maintenance. Developing a strict maintenance and inspection schedule is crucial for keeping physical access control systems running smoothly, especially as they contain a multitude of moving parts. A regular service and maintenance regime ensures that security equipment is functioning as it should. Bollards, for example, need to raise and lower properly; regular checks can therefore identify any issues that might affect this, such as mechanical failure or corrosion.

Malfunctioning equipment can seriously compromise security. For instance, if a bollard does not deploy when needed due to poor or non-existent servicing, unauthorised vehicles could gain access to areas that are supposed to be secure. This can, potentially, highlight site / area vulnerabilities and put people at risk. By contrast, well-maintained physical access control equipment enhances security and ensures greater effectiveness. Guaranteeing that bollards and other security measures are in optimal condition heightens the visual deterrent to threats and the care being put into an area (going back to the preluding 'Broken Windows Theory).

Training is a key part of correct system use. Physical access control systems rely on making sure that the stakeholders using the equipment are familiar with the products and the systems to an intimate degree, and part of that is educating the users to ensure operating protocols are followed. Again, a physical access control system is only as secure as its weakest link and sometimes, sadly, this is the user itself. Invariably, you cannot completely design out 'human error.'

Urban security plays a proactive role within the care and consideration of an area, positively contributing to a public realm that the community and residents can be proud of. Measures implemented should be layered and plans should be designed to prevent criminality, further enhance the aesthetics of an area and provide a safe place for people to live, visit and work without fear ●

Lucy Ketley is Sales & Marketing Director at ATG Access Ltd.

It is important to consider the regulations and standards that are needed when designing and specifying a physical access control system

Picture credit: ATG Access Ltd.