INTEGRATED SECURITY

Steve Moody *explains how entrance security solutions can be an effective deterrent with the right approach and processes to back them up*

Traditionally, entrance security solutions have been the reserve of major arenas, airports or offices/organisations that are considered prime targets for terrorists or criminals. However, the threat has changed. Terror attacks are no longer designed purely to make a statement, but to maximise damage. This means that anyone or anything could be a potential target. It's a sad state of affairs, but one we must understand and defend against. Equally, the sheer number of people attending events or other public spaces means a pragmatic approach is also needed, so life can continue as normally as possible. This means entrance and perimeter security measures are critical in protecting the people within the building and its vicinity.

Implementing a basic range of entrance security solutions can drastically improve the safety of your building or assets and how personnel respond and stay protected from a variety of threats. Sadly, those bent on harming us will often pursue their course of action regardless of any preventive measures we take. At this stage, we are initially looking to prevent or slow down the attack so that those in or nearby the target can get to safety.

This is where the strategic placement of bollards, barriers or even trees and art installations can help prevent a direct attack on the building and its occupants. Hostile Vehicle Management (HVM) should be a key part in your strategic risk management, but will not be covered here.

Proper use of perimeter and entrance security also makes the life of security personnel and other employees much easier. Having the right tools for the job and the latest technology allows people to do what people do best – react to situations as and when needed, such as crowd trouble or unauthorised access. To achieve this, security needs to be multi-layered and start from the perimeter of the business, working inwards. This typically means starting with perimeter defences, which could include fencing, cameras and access points. For example, is it possible for a vehicle to drive at high speed towards your venue or building without any form of interruption? It's this type of critical thinking and anticipation of potential threat scenarios that will enable you to step up your entrance security procedures. Simply adding in a few security barriers or new protocols will not cut it – a holistic approach is required.

There are plenty of solutions available, but an ever-changing threat requires more than just hard defences. We need the right processes in place and the right mindset from the start to mitigate these risks. "Integrated security" is a buzzword I am sure you've all heard, but it's a buzzword for a reason – it's only through a holistic approach to security that encompasses the physical, digital and human elements involved that we can truly combat today's threats.

New and innovative technology has made great strides in hindering the progress of potential attackers by obstructing direct and proximity access to the target, but it can have the effect of moving the threat

> **AS WELL AS SLOWING THE PROGRESS OF A THREAT, ENTRANCE SECURITY CAN ALSO PROVIDE SHELTER**

rather than nullifying it. As a result, the target and method of attack will vary – something security personnel will need to be mindful of.

This is why integrated security is so important. It's not enough to simply think about the security of the building – instead, we must consider how people will be travelling and access the asset we want to protect, and even where they might congregate beforehand or afterwards.

Integrated security requires planners, designers, architects, security consultants, contractors and key personnel such as heads of security and HR to be involved at the first stage of any new construction project. Of course, it's possible to retrofit existing assets with an integrated security approach, but it can be more complex than starting from the ground up. Nonetheless, the security benefits are worth it.

An integrated approach also means having the right processes in place, so every person involved in the business or organisation knows his or her role in any threat scenario. Again, this means working closely with other departments such as HR, security, operations and more. Each team must know its role should a security situation arise, and those teams must be able to effectively coordinate and use the tools at their disposal.

For example, what good is it having a state-of-the-art entrance portal with biometric access if those working at the front of the building are unclear how it works or what to do with it in the event of a security threat? Should they shut it off to all personnel? Should they let people in first so they can get to safety? How many do they let in? What if the security threat is hiding among the staff?

Aside from the threat itself, confusion is your biggest enemy. Ensuring people know what they are doing where and when will save lives. Therefore, it's crucial to: identify all potential security risks and which assets are most at risk as well as the likelihood of these scenarios; devise and implement a plan to mitigate those risks; and ensure all departments and personnel involved are clear on their action plan.

While new strategies and considerations must be given to an ever-changing threat, technology undoubtedly forms a major part of the response. There's a huge range of innovative solutions ready to be implemented, but perhaps some of the most viable new technologies include the following:

OPTIMISED FACIAL RECOGNITION

The use of optimised facial recognition in conjunction with extremely high-resolution IP cameras can provide an early detection system particularly if integrated with the access control system. This has the simultaneous effect of a more seamless entry verification process, while images can also be matched against a watched list or blacklist of specific individuals preventing unwarranted access.

This does not only apply to terrorists or criminals, but also to crowd control and to monitor 'known' individuals – this can be useful at public events or other gatherings such as protests. These types of systems also learn, gaining robustness and becoming smarter. For example, hi-res cameras combined with facial recognition could begin to identify and recognise individuals that are liable to cause trouble – perhaps someone who does not warrant being blacklisted, but a person to keep an eye on. This frees up security personnel to get on with their day job, with the system alerting and redeploying staff to deal with a potential situation if required.

BEHAVIOURAL ANALYTICS

Behavioural analytics is a rapidly developing field of research and extremely useful in crowd control situations. The ability for a system to monitor and predict potential threats or crowd unrest is a key tool to help security staff and other personnel respond quickly to real-time data.

Behavioural analytics software and artificial intelligence can quickly identify patterns of behaviour most commonly associated with violence or other activities that could compromise the safety of a crowd. This can be used to alert authorities to a heated situation before it erupts.

Implementing a basic range of entrance security solutions can drastically improve the safety of your building

Analytics software, running off the CCTV system, can learn and recognise the events leading up to any issues occurring. The more scenarios the software reviews, the earlier it can detect the issue, which can then be reviewed, and mitigation can take place.

ACCESS SCANNING EQUIPMENT

We are all aware of the obligatory walk-through metal detectors most commonly found in airports, but the technology has advanced considerably over the past 10 years. Walk-through monitors can now detect a multitude of substances that could pose a threat in an enclosed stadium environment. In fact, the 'sniffing' technology on these monitors can be used to detect anything from excess alcohol through to nuclear material. The access control barriers can then be used to divert the individual into a containment room away from the general public.

PORTALS, CABINS AND REVOLVING DOORS

The solutions mentioned above are mostly preventive and proactive methods aimed at detecting a threat before it arises. However, this does not negate the need for solutions on the 'doorstep'. This is where entrance security portals, cabins, revolving doors and speed lanes are still a highly effective solution. These measures typically only allow one person through at any given time and will detect if more than one individual is present. This prevents tailgating whereby unauthorised personnel simply follow someone else with access to the building, which is why ID badges on their own are

not enough. As well as slowing the progress of a threat, these entrance security solutions also provide an area from which your staff or visitors can shelter.

Staff mental wellbeing may not necessarily be top of your list of concerns when considering security solutions, but the psychological and physical state of employees can be positively affected by well-implemented security measures. Making your staff and visitors feel welcome and secure is an important part of any business or organisation. Ensuring that colleagues and visitors feel safe is integral to this. In fact, it can be crucial to the operation of the business – it would not be a complete surprise to see staff take time off in the aftermath of a security breach, or attack, even if it took place at another location in the vicinity.

Taking the time and implementing the measures to make sure people are not anxious about their safety makes good business sense as well as being the right thing to do. People who feel safe and secure will be more productive than those who are worried about their surroundings.

There is a vast range of entrance security solutions available, ranging from more low-key, but effective, solutions such as speed gates and basic access control to more advanced systems such as revolving doors or portals, which help prevent the risk of tailgating or unauthorised access. It is important to consider the needs of your specific facility or building. Your security needs might be like other businesses, but they won't be identical, so nor should your solutions. Working closely with a security consultant who can assess your security risks and balance recommended solutions with the needs of your business is paramount ●

Steve Moody is High Security Sales Manager at RWS Ltd – security consultants and experts in blast and ballistic protection. Steve has more than 20 years' experience in the security sector, having worked at ATG Access, APT Security Systems and Betafence perimeter security.

Perimeter security measures are critical for protecting the people inside the building

Picture credit: RWS Ltd