Peder Berg looks at how the latest accreditation system technology can mitigate the risk of a terror attack on stadiums or area events

SMARTER STAD

©Getty Images

In recent years technology has become synonymous with terror threats, whether it is used to detect and combat a potential threat or to actually plan and co-ordinate an attack. A robust and airtight access control system has never been more important than it is today, especially in the case of stadiums and arenas. These venues bring together hundreds of thousands of individuals under one roof, often for high profile events – rendering them susceptible to being a terrorist target.

The challenges faced by stadium and arena venue management, when it comes to terrorist threats, are many and varied. All the standard and expected areas need to be scrutinised, and a lot more besides. Venue management has a legal obligation to know exactly who is in the venue 24/7. Risk management is also high on the agenda, and this is where an accreditation system will play a vital role. Any system will need to support security measures and contingency plans.

One of the biggest risks comes in the form of an insider threat. It is often necessary to give employees and some visitors complete access to a venue, but how do you know they can be trusted? They can 99.9 per cent of the time, of course, but the impact of that undesirable someone slipping through the net can be horrific. Everyone is vulnerable to employing bogus casual staff such as illegal workers, undercover journalists and even extremists. Stadium-style venues tend to have a high turnover of staff and more than their fair share of temporary staff; it is therefore not always easy to build a complete personnel profile on every single employee.

For stadium and arena venues and event management businesses, there is no way of avoiding employing contractors and temporary staff. It makes sense logistically and from a best business practice point of view; the use of contractors is therefore commonplace, providing vital skills and expertise that cannot be developed internally for the same cost or within the same budget. These businesses must necessarily allow information and legitimate access to some of their most sensitive assets to a significant number of workers who are not company employees. The potential damage that can be caused to an organisation from an "insider" within their workforce who uses their legitimate access for unauthorised purposes is well documented. Businesses have suffered significant financial and reputational losses as a direct result of such activity, ranging from fraud and unauthorised disclosures of sensitive company information to malicious sabotage of key sites, systems and equipment.

The use of contractors can result in an increased personnel security risk, as a contractor's primary loyalty may not be to the organisation that engages them and their commitment to the organisation's security culture may be diminished as a consequence. It is therefore essential that companies put in place effective personnel security policies and procedures that manage the insider risks posed by contractors.

Considerable efforts are being undertaken to manage these risks especially against physical and cyber attacks.

DIUM SECURITY

It is widely understood that the implementation of these security measures will help reduce the risks to key sites, systems and equipment. It is, however, equally important to take appropriate and proportionate steps, through the adoption of policies and procedures, to manage the risk of staff and contractors exploiting their legitimate access to sensitive assets, information and people. Stadiums and arenas, like every type of business, should incorporate effective personnel security measures into their management procedures and ensure that the relevant parts of business (human resources, procurement, IT and security) work together to manage and mitigate these risks.

Every year, businesses suffer significant financial and reputational losses as a direct consequence of staff misusing their access and privileges. "Insider" activity ranges from fraud and theft of intellectual property to the sabotage of key sites, systems and equipment. Disaffected individuals, single-issue groups, competitors or those with links to organised crime or terrorism may carry out such unauthorised activities. The potential ramifications of insider activity on the safety and security of the workforce are therefore serious.

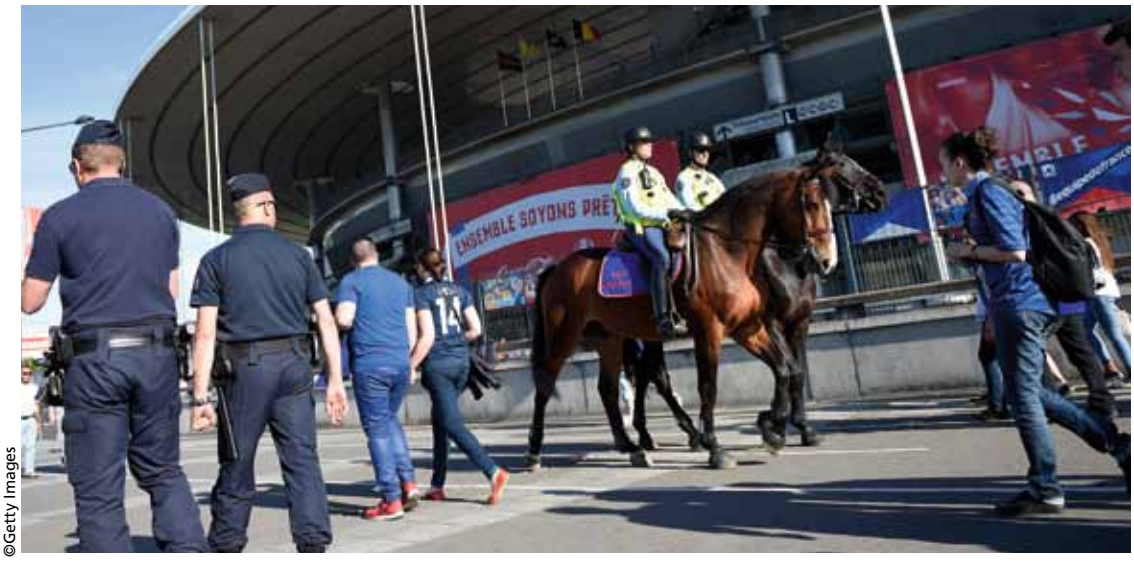
The ramifications of insider activity on the safety and security of the workforce can be serious. Companies owe a duty of care to provide a safe place and system of work, to recruit competent personnel and to take reasonable care not to expose employees or workers to unnecessary risk. A breach of this duty could result in criminal sanctions under health and safety legislation and/or civil proceedings. This can also include penalties for employing illegal workers. The current fine in the UK is up to £20,000 per person for employing illegal workers. Illegal workers include students with expired visas or students working more hours than they're allowed to, as well as people who work on a visitor's visa. This duty arguably extends to the insider risk, and therefore encompasses the engagement and activities of contracting staff. All this goes to prove that a robust and efficient accreditation system is vital to stadium and arena management.

There are a number of approaches to effective accreditation and a plethora of systems on the market, but the challenge lies in identifying the optimum solution. Existing resources will dictate the approach, which is likely to be an upgrade of existing or introduction of new. Every situation will be unique, and any system likely to be bespoke, but let's take a look at what an accreditation system should deliver.

The benefits of robust and efficient access control within stadium environment are many. The two priorities for any accreditation system, in this author's view, are delivering best practice and cost savings. Vetting individuals can be extremely time consuming, so an efficient accreditation system should be built to save time and money though not at the cost of reducing quality standards.

A simple-to-use front end user interface is important. Whether used by the visitors themselves or managed by internal event teams, it ensures an efficient and smooth

SMARTER STADIUM SECURITY



©Getty Images

Smart accreditation systems could help security and police forces to effectively exclude dangerous individuals from stadia and arena events

registration/access control process. The interface should be web based so it can be used on any Internet browser, either on desktops, laptops, tablets or smart phones. The entire application process needs to be easy for the user to access – whether searching and updating individual applicants, running reports or editing the entry.

Password protected unique login portals with varying degrees of access to the system tools and data are key too. Each login should be tracked, providing a full audit trail of data. From a data management perspective, handling many different application categories of personnel, each with its own unique application form, should be possible. For example, stakeholder groups requiring accreditation may include: sporting teams, contractors, production teams, broadcasters, journalists, entertainers, volunteers and VIPs. The system will need to accommodate the uploading of identification documentation such as passport scans, company details or photographs. Applicants should be able to upload files easily with a simple browse and upload function.

Photo badge production, either singularly or in batches, is a must, with each badge assigned a unique barcode in large stadium and arena environments. This allows control and tracking of the contractor members of staff or other type of venue visitor when the badge in use. Ideally, access levels should be able to be easily merged onto badges in colour and text.

Having covered the logistics, we need to drill down to exactly how each individual will be vetted. As with any bespoke system, this is where the individual needs of the business – or in this case venue – should be addressed. The vetting process should have several layers – a visitor accessing public areas will need a completely different vetting process than a contractor who will have daily access to sensitive corporate information.

The actual vetting process is prescribed by the venue and level of security required. The system should include a range of screening elements such as a virtual holding zone for registrations made which allows you to accept, reject or request more information for people applying to access the stadium, this process would typically be carried out by the security department or accreditation team. Communication is pivotal to this process, so the system should automatically generate an email based on accept, reject or more information so the person registering knows what they need to do.

It is likely that an arena or stadium will have a black list of individuals, and the inclusion of a facility to pre-load lists into the system means that if a blacklisted individual applies for access they will automatically be rejected. This goes for individuals or other criteria like country of residence. As part of this it will, of course, need to keep track of who has previously been rejected.

Operating in real time is essential. For example, if an applicant has been accepted and a pass issued and then you receive intelligence on him or her, you can cancel the pass to prevent access to the venue or event. Integration with police systems is also a sensible step in order to obtain this intelligence.

Keeping accurate records of all activity in the system will prove invaluable, especially if an incident or a call for recourse is required. In this instance an audit trail of all communications deployed during the accreditation process will come into its own. Accuracy at all times should be assisted by a facility to set reminders into the system to flag when you need to collect new information such as a security guards' SIA license renewal or a visa for an overseas worker.

Another useful facility to consider is a built-in vehicle access module designed to control which vehicles are brought into the venue. This allows external users to apply for vehicle passes by registering the vehicle details (including brand, licence number and vehicle type). Once an application is made, it can be approved/rejected and assigned correct access levels and load/unload times. Not all systems incorporate this, but it is sensible to incorporate personnel and vehicle movement around a stadium or indeed any large venue or live event.

Ultimately, reliability is non-negotiable. Venues can't afford to deal with system down time. The system needs to be fully operational 24/7, so going offline is not an option. The system supplier needs to be able to offer full technical and customer support service for all users within the stadium or arena at any given time, but especially during large sporting events when the terrorist threat is at its highest.

Peder Berg is Managing Director of Event Advantage Solutions (EAS). Peder is one of the co-founders of EAS and has been with the company for more than 12 years. He is responsible for overseeing EAS's UK business and sales management. Prior to joining EAS, Peder was Vice President of Sales and Marketing for Penton Digital Media and Director of Marketing for Streaming Media.