DESIGN AND CULTURE

Stacey Peel *reports on the untapped opportunities for aviation security*

Technology has been the cornerstone of mitigating security risks, particularly terrorism in the aviation industry. The X-Ray and Walk-Through Metal Detector (WTMD) are the traditional examples and drone-disabling software an example relevant to a contemporary threat. Readers will find endless material on the value (and limitations!) of technology and the impact it can have on other aspects of operations such as passenger experience, capital budgets and privacy impositions. I, however, would like to explore two risk mitigation measures that are not often considered but can have an equal, or even better, security outcome to technology: design and culture through Security Management System (SeMS).

Infrastructure projects in airports are typically the domain of project managers, architects, engineers and construction companies with security operations usually engaged just prior to construction, at equipment procurement stage, or worst case security may be considered just at handover stage and only then when it involves the airport perimeter or passenger screening checkpoint. A risk-based approach and early involvement of security, for all infrastructure projects regardless of scope, provides airports with significant benefits – not only for security, but across the business.

SEMS ESTABLISHMENT IS A LONG-TERM PROJECT REQUIRING COMMITMENT FROM THE VERY TOP

Early involvement of security provides an opportunity to design out and reduce security vulnerabilities. The key difference between security and all other risks is that the threat itself has intent. The perpetrator is capable of identifying and exploiting vulnerabilities and circumventing mitigations to carry out an attack. Some of the higher-profile attacks, including attempts on the aviation industry are a direct result of exploitation of vulnerabilities such as the 'underwear' bomber bypassing security screening by carrying explosives on their person through the WTMD. Some of these vulnerabilities relate directly to a security measure itself, for example, the WTMD cannot detect non-metallic threat items, but some vulnerabilities are caused by infrastructure design. An obvious example is where limited space and inefficient processing at the passenger screening checkpoint and check-in/bag drop generates congestion. A crowded space becomes an attractive target. In addition, the environment being such that the introduction of a larger weapon – eg IED in suitcases (as used in the 2016 Brussels Airport attack) – could be more easily introduced into the space than onto an aircraft.

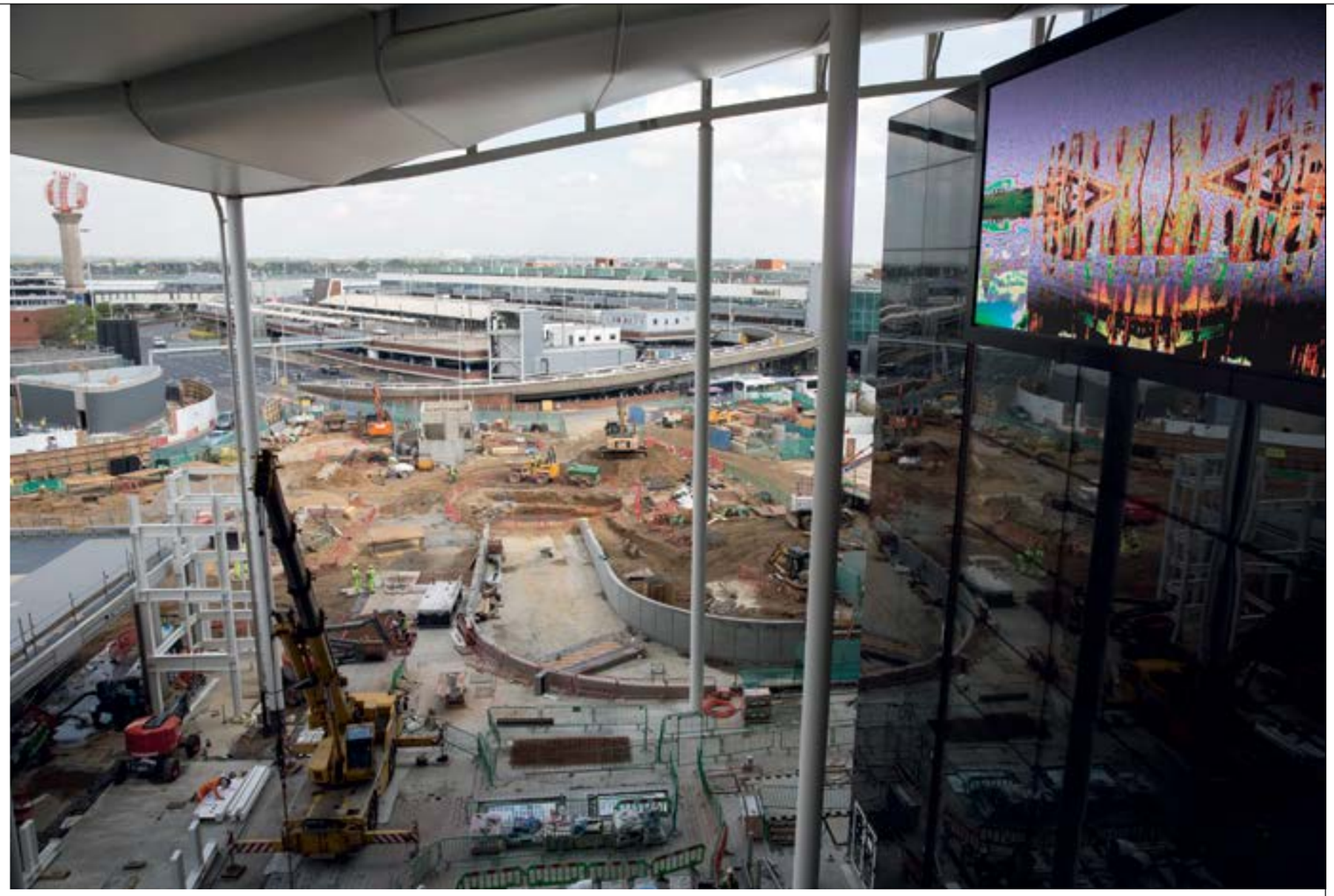
DESIGNING OUT VULNERABILITIES

By designing out vulnerabilities there is a reduced need to overlay security, eg a terminal approach road design that forces a vehicle to reduce speed is likely to lower the specification requirements of the HVM. Also, this may offer the opportunity to exploit different vehicle impact mitigation measures such as street furniture, which may be more aligned with the architectural intent and less visually striking than conventional bollards.

Furthermore, design can take account of potential future needs, eg today's lighting design to take account of facial recognition technology to be used in the future. Consideration of security needs early in a design project results in reduced operating and capital costs. For example, Arup has researched the capital costs and risk reduction benefit of enhancements to a façade against an explosion (see Case Study overleaf).

Determining the security needs must be risk-based. Risk-based design facilitates security responses that are commensurate, avoiding either 'over-engineering' or misdirecting resources and identifies security design needs that may not always be obvious. Additionally, it takes account of different operating environments – business as usual, periods of heightened threat, incident management and recovery. Given these different demands, particularly the latter two situations, engagement with end users and understanding their requirements is critical. What is the critical path into a terminal for ambulance gurneys? What vehicle access do law enforcement and emergency services need during periods of heightened threat and incident response? What data networks do airlines need if check-in has to switch from departures to arrivals during a period of recovery? Design clearly relates to the infrastructure. While it facilitates operations, by its very nature it is typically fixed. In contrast, security culture is much more agile.

Historically, the operational personnel tasked with security duties at airports have been law enforcement agencies, screeners and guards. The nature of their duties mean that they are the last line of defence.



Picture credit: Getty

Involvement of security in the developmental stages of an airport provides an opportunity to design out and reduce security vulnerabilities

Furthermore, the management and investment in resourcing – eg security recruitment and equipment needs – have tended to occur in isolation from the broader management of the airport. This silo approach results in missed opportunities to draw on the presence of a large community of 'eyes and ears', is costlier, less efficient and drives sub-optimal security and business outcomes. This can be addressed by establishing a robust and positive security culture within the entire airport community and is achievable with a Security Management System or SeMS.

REDUCING RISK

When designed and implemented correctly, SeMS is a management mechanism that establishes and maintains mind-set and tools in the airport community and airport management system. It fosters behaviour that identifies and reduces risks and allocates limited resources in a manner that enhances security. Indicators of a successful SeMS include the detection of hostile reconnaissance by a land-side tenant employee that results in the disruption of attack planning; a security audit by a third party is welcomed as an opportunity to independently identify opportunities for improvement; a security risk assessment is undertaken for each and every infrastructure project regardless of its scope; the procurement of security equipment is informed by user requirements, operational requirements, whole of life costs and the impact of its deployment on the business beyond security not solely assessed on purchase price; and personnel/staff competency is assessed in real-time and is based on data.

Furthermore, through improved integration of security management into the business, as compared to a standalone operating unit, the challenges that arise from the perception that security is just a cost-centre are eliminated.

Like all management systems and change processes, SeMS establishment is a long-term project that requires commitment from the top and should be spearheaded by a champion. Without these two commitments, the best an airport can hope for is a tidy library of documentation for the regulators to reference during audits. Additionally, the SeMS must be comprehensive and be subject to a regular quality assurance. Arup's SeMS model comprises seven elements (as illustrated overleaf). The first step in the process of establishing a SeMS is to understand

how ready your airport is for a SeMS: Is there a sense of urgency to implement or not? What is the baseline knowledge of SeMS? The approach to adopting SeMS will be wholly dependent upon the answer to these two important questions.

The next step is to identify the current maturity of your SeMS. It is likely your airport already has elements of SeMS – eg physical security, internal audit process, airport emergency centre. A maturity assessment will determine the maturity of each SeMS element, in terms of the tools that facilitate and the organisation's mind-set, so you can then target efforts accordingly. For example, you may already have an internal audit system in place that comprises trained auditors, checklists and information management system. Audits, however, are only undertaken immediately prior to the regulator's audit, less than ideal results are suppressed, there is no root cause analysis and individuals are penalised for poor results. In this case, the tools used to ensure compliance are relatively mature, however the mind-set associated with compliance and continual improvement is less mature. In contrast, your airport regularly undertakes desktop exercises using security scenarios and everyone commits to addressing lessons learned. However, there is no link between this and the airport's business continuity system, so issues like media management, clearly defined roles and responsibilities are not available to the security team. In this case, the mind-set for Continual Improvement and Business Continuity is mature, but the tools are immature.

A RISK-BASED APPROACH FOR ALL INFRASTRUCTURE PROJECTS PROVIDES SIGNIFICANT BENEFITS

A MORE HOLISTIC APPROACH

Once your tool and mind-set maturity for each SeMS element is known you can determine what maturity you are seeking to achieve and then target and prioritise enhancement efforts accordingly. Continuing with an example of mature tools, but a less mature mind-set for the Physical Security SeMS element – rather than trying to establish more rigid procurement processes to achieve equipment purchases that better suit the security team's needs – effort could be spent helping the procurement team better understand their needs by establishing a relationship between your security guards, procurement and finance teams to influence a more holistic approach to equipment procurement. The procurement and finance teams are therefore more likely to consider user requirements, human factors (the equipment-human interface and users' needs) and whole of life costs rather than basing investment decisions on purchase price only.

Celebrating success is critical to ongoing support for SeMS. Regularly assessing your SeMS maturity will assist in measuring maturation, but lack of wholesale improvement should not be concluded as a failure – it may be that the time to realise the benefits of efforts is longer term than the frequency of your regular maturity assessment. The other obvious measure of success is where change can be quantified, for example an increase in the reporting of security risks or suspicious activity, reduction in patrol costs through the sharing of resources with safety and reduced insurance premiums as SeMS becomes a recognised risk mitigation measure. Less obvious are the qualitative measures such as seeking out personal stories of success, looking for examples of cross-team interaction not previously seen and identifying new references to security in executives' public statements. These too should be identified and celebrated.

BENEFITS OF SMS

The value of Safety Management System (SMS) is well documented. While SeMS is not as widely adopted as SMS, the benefits are similar in the security context: better security and business outcomes, eg improved passenger perception of security; a framework to measure security performance against investment, (ie return on investment); the opportunity to break down silos and join up airport operations with the business (eg real-time analysis of training needs); and, greater flexibility to respond to changing threats.

The investment in infrastructure will increase as the number of passengers increases. So too will investment in security as the threat changes. It is imperative that we look beyond technology to manage the security risks. The value of security in design and SeMS are realised by those airports that have embraced these opportunities. I therefore pose the challenge to you: is your airport relying on technology alone and what could design and SeMS do for your community, your passengers, bottom line and, of course, security? ●

Stacey Peel - Arup's Global Aviation Security Leader – has worked throughout the Asia-Pacific, Europe, Middle East and North Americas regions across the breadth of the aviation security spectrum: risk based-design, security culture, regulation and government/national policy, risk management, operations and technology.

CASE STUDY:

Cost and casualty benefits of designing in façade blast enhancement

Based on a specific design basis threat of an IED exploding inside an airport terminal, the below compares the cost and casualties (from the blast wave, fixtures and fittings being detached) based on different façade resilience design options:

1. No enhancement
2. Enhancement that is only available if designed-in, ie considered early in the design
3. Anti-shatter film retrofitted to glazing

	No enhancement	Designed-in enhancement	Retrofit
Cost (£/sqm)	800	1,000	1,021
Casualty (internal)	128	0	42

While there could be a 20 percent cost uplift of designing in enhancement compared with no enhancement the value is in the façade's performance and, therefore, the casualties: 128 casualties with no enhancement versus zero with designed-in resilience. Applying industry-standard metrics on the tolerability of risk indicates the cost of designed-in enhancement is proportionate considering the result is such a stark risk reduction.

Retrofitted anti-shatter film performance in terms of protection is inferior to designed-in enhancement and is also costlier on a whole-of-life basis, due to the maintenance and replacement requirements.

Source: Arup

Picture credit: Shutterstock.com