EXPERT PANEL

As part our Security In-Depth Focus, *International Airport Review* asked our Expert Panel the following question:

What challenges do airports face when protecting their critical IT assets and processes from cybersecurity threats?

PARTICIPANTS

ANDY BLACKWELL

Managing Director, Blackwell Security Consulting

RONI TIDHAR

Head of International Consulting - Security & Safety, Ben-Gurion Airport, Israel Airports Authority (IAA)

MICHAEL SCHELLENBERG

Director Integration & Services, SITA

BLACKWELL: Improving staff awareness of cybersecurity risks, enhancing levels of collaboration with key stakeholders and ensuring management systems are robust enough to provide corporate assurance are all challenges that airports face when protecting their critical IT assets and processes from cybersecurity threats. It's important that incident management and business continuity plans are broad enough to cover responses to and recovery from cyber-attacks including those that feature 'insiders'.

There tends to be a lack of understanding within the industry of the risks posed by cyber-attacks and incorporating cybersecurity in security awareness training will help with knowledge transfer. The value of employees reporting suspicious behaviour and events cannot be overstated and is a message that needs to be promulgated by top management.

Collaborative approaches and making use of the advice provided by trusted organisations, including government agencies and representative bodies, will help airports embed best-practices and learn from the experiences of others – good and bad. Information sharing is key. When risk assessments are being undertaken, cybersecurity impacts need to be considered, and the composition of risk assessment groups must include those with comprehensive cybersecurity knowledge and expertise.

Cybersecurity cannot be managed in a silo; it must be fully integrated into the airport's security plan and management system, such as the SeMS.

TIDHAR: Airport safety and security challenges and threats vary in scale from 'simple' bad weather scenarios to the more complex terror attacks or aircraft accidents. The majority of these scenarios show/leave some visible footprints and we may be able to react on the spot or immediately after, in order to reduce damages.

However, a silent monster lurks in the dark – the potential of being cyber-attacked without prior warning. Detecting the mere fact that systems were invaded at all is problematic; this 'Modus Operandi' seems less risky and requires less physical effort from potential terrorists or by other motive-led hackers (tools are available at fairly reasonable prices on-line). Furthermore, disguise is rather easy and the possibility of human error that uncovers the scheme almost doesn't exist – and there is no immediate physical danger posed by airport's law enforcement officers. These kinds of attacks are on the rise. Where? When? Why? For what purpose? By whom? Sadly, these remain mostly unanswered.

Increasing reliance on sophisticated systems and computers exposes our airports to cyber-threats that heavily impacts our degree of control and may cause loss of human lives. We must therefore acknowledge the probability that we've already been hacked, or are due to face it soon, and take necessary precautionary steps such as invest in protective software and develop an accurate redundancy plan and effective CIRT.

SCHELLENBERG: There is little doubt that cybersecurity is fast becoming one of the top global priorities for airlines and airports. The 2016 Airline IT Trends survey revealed that 91% of respondents plan to invest in cybersecurity programmes over the next three years; 63% say cybersecurity is a board-level responsibility at their airline; and 94% of airports are investing in cybersecurity incident response management.

Cyber-attacks are a very real threat, with the potential for huge knock-on effects in an industry as interwoven as the air transport industry. Layers upon layers of infrastructure could be impacted, with the consequences on global travel reverberating across the world. Protection services remain fundamentally important but are no longer enough. The challenge is to build a multi-faceted approach that includes identification, protection, detection and reaction.

Collaboration is really the key. The inter-dependencies built into air transport systems and an accelerating digital transformation in the industry mean the vulnerability to attack is increasing. Cyber-threats cannot be efficiently combated by acting unilaterally. In addition to having a solid cybersecurity strategy and tools in place, we, as an industry, must combine forces and find mutually agreeable ways of dealing with this reality.