

AIRLINES

INTERNATIONAL DAILY

27 OCTOBER 2016

AVSEC WORLD

brought to you by ACI, IATA and ICAO

25-27 October 2016 | Kuala Lumpur



Airlines International Daily is sponsored by:



Change throughout the organization

Creating a culture of security in an organization and educating people on how to deal with a crisis situation is of the utmost importance.

Francis Morgan, Director of Security for the Council of the European Union, speaking on yesterday's *Landside Security* panel, said that, during the Brussels Airport bombings, his organization learnt some valuable lessons, including the importance of keeping staff regularly updated during a crisis.

He said that when the bombings occurred, his organization worked hard to get information from the authorities on the situation. "But there were gaps in our dealings with the Belgium Government. We encountered difficulties finding out what was going on, and that then created gaps in our communication with staff.

"We wanted to communicate regularly, but then we decided that if we didn't have anything new to say, we wouldn't say it," he added. "But that proved to be a mistake. It meant staff inside the EU building felt unsettled and uncertain about what was going on. So, a key learning was to keep the

communication going regularly, even if you don't have any news to report."

Morgan noted that staff empowerment was equally vital. "What we encountered around our building was a few people who were confident, who got their staff together to check they were okay. They knew who was in the building, who was where, and these managers showed initiative to address the situation."

A larger group of people just waited for instructions and were not so proactive. "That meant the people working in their teams felt uncertain," said Morgan. "So, now we have a big program of management

training. We are training people on what to do during a crisis, so they know what their responsibilities are."

The aim is to build on this training to create a security culture in the organization, rather than just setting security rules.

Fellow panellist, Alexis Long, Head of Security Policy at London Heathrow Airport, noted that regular collaboration with the authorities was critical. At Heathrow, executives responsible for security at the airport have meetings each month with the police and intelligence agencies and this has proved invaluable.

Long said that it took some time to change the mindset and have authorities accept that it was good to be sharing information with individuals from a private organization. But that hurdle has now been overcome, and there is no going back to the past when people worked in silos. •



YB Dato' Sri Liow Tiong Lai, Minister of Transport, Malaysia

"As air passenger traffic rises, so must our vigilance. Safety and security are all the more important with the rise in terrorism and cyber threats. It is our responsibility and duty in aviation security community to work together to implement the necessary standards of security and ensure they are upheld."



Join over
500
Industry Experts
at IATA's
World

Do you wonder what the future of aviation security might bring?

Exchange ideas and share insights in a digital management and future strategies through collaboration, coordination and communication.

www.iata.org/itw

Aviation Security: An ongoing challenge in any language.

How can our you get to, go back, secure, an air line, aviation / aviation security opportunities to search and expand your scope here.

www.iata.org/itw/eng



Aviation industry **INVESTS** over \$70B per year...

A SOLUTION FOR EVERY SECURITY CONCERN



How do you stay compliant with constantly changing international travel rules?

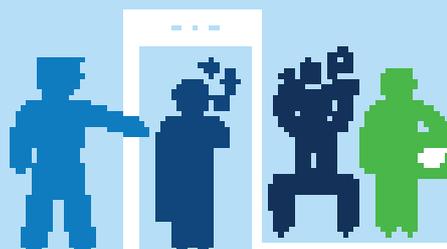


Travel solutions cover internationally and every destination, globally. We update our Travel solutions on average of 50+ times each day, with information from 1200+ governmental and industry sources.

Our **TERRA & TRAC** solutions enables you to automate the passenger travel document check process and to check 100% of international passengers' documents automatically.

www.iata.org/itw/itw/terra

Is aviation security embedded from top to bottom in your organization?

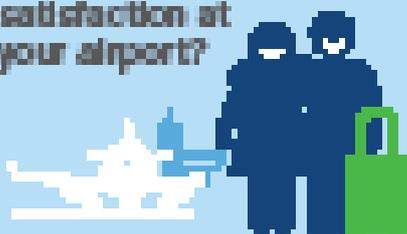


SECURE is a fully integrated security solution that covers all operational security and security risks.

The integrated Security Manual covers all security and security risks.

www.iata.org/itw/itw/secure

Have you recently experienced a security audit? Are you looking to improve your performance and boost customer satisfaction at your airport?

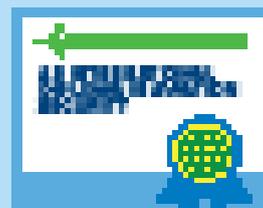


93% of passengers are happy with security screening process

IATA's **Checklist** helps you enhance your airport security delivery, improve customer satisfaction, maximize your security investment and apply recommended best practices.

www.iata.org/itw/itw/checklist

Would you like to pack your experience and knowledge into an international diploma?



Over 100,000 professionals in 100+ countries participate in IATA security training, globally. IATA Training will update, still you up and give you the best practices in aviation security.

www.iata.org/itw/itw/training



Participating in industry meetings pertaining to security can help improve your business

Industry can be used and working groups are organized for your needs

Discuss a strategic partner and stay informed of the latest topics and the industry's security priorities

www.iata.org/itw



TO REPRESENT, LEAD AND SERVE

Providing you an experience to help you, your team and your organization achieve, as defined as if one of the security challenges of the day... and tomorrow

www.iata.org



Strengthening the weakest link

Speaking on the *Integrated Security Risk Management* panel yesterday, Mike Woodall, Assistant Director of Security Consulting at IATA, said that it is important to remember that some organizations lack the resources to do integrated security risk management. And some are still struggling to do risk assessments.

“Many of you in this room, who represent the top 1% of the aviation security community, are ready to look at integration and many may already be doing that ...but there are still huge numbers of people in our industry who are struggling to even start the basic processes,” he said.

“I work with many organizations that struggle to do risk assessment programs,” he added. “And many don’t integrate those risk

assessments within their own organization, let alone across other boundaries.”

Woodall described one of the issues as different risk appetites. That means merging or blending risk assessments with a third party is difficult due to the wide range of perspectives.

He said that even if we accept we face a common threat, there will be different points of view on how to deal with it, and the approaches will often be very different. But it is essential to overcome these discrepancies because the outcome is all important.

“Post event, the critical questions people are going to ask will not be ‘what terminology did you use?’, ‘whose system did you adopt?’ and ‘who did you integrate with?’” suggested Woodall.

Rather, the post event questions most asked by most lawyers, business executives, and the media are:

- What did you know?
- When did you know it?
- What did you do about it?

“We can integrate and the top 1% [of the aviation security community] can rattle on and have a conversation about what comes next,” said Woodall. “But for most people out there, those three simple questions need a risk assessment.

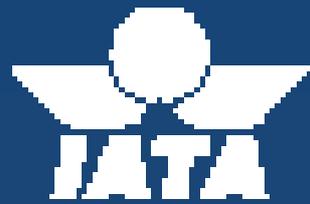
“The people outside this room [who are not part of the 1%] need our support,” he continued. “We need to give them the tools and confidence to start creating timely evidence-based risk assessments that can be reviewed, managed, and implemented.”

He noted that IATA is helping organizations to start the risk assessment process and optimize the security resources that they already have. “We are helping them to design and deliver improved levels of security and it doesn’t really matter if some of our terminologies are not the same as yours, and some of our methodologies aren’t exactly the same as yours,” he stressed. “Because if you are not in a privileged position, any support or assistance has to be good for all of us.”

He concluded: “We can’t wait for a perfect solution, we have to help today. If you genuinely believe that the weakest link is a problem for all of us... then strengthening the already strong links just makes the weaker links look even weaker. I think we should do our best to help everybody.” •

Scenes from AVSEC

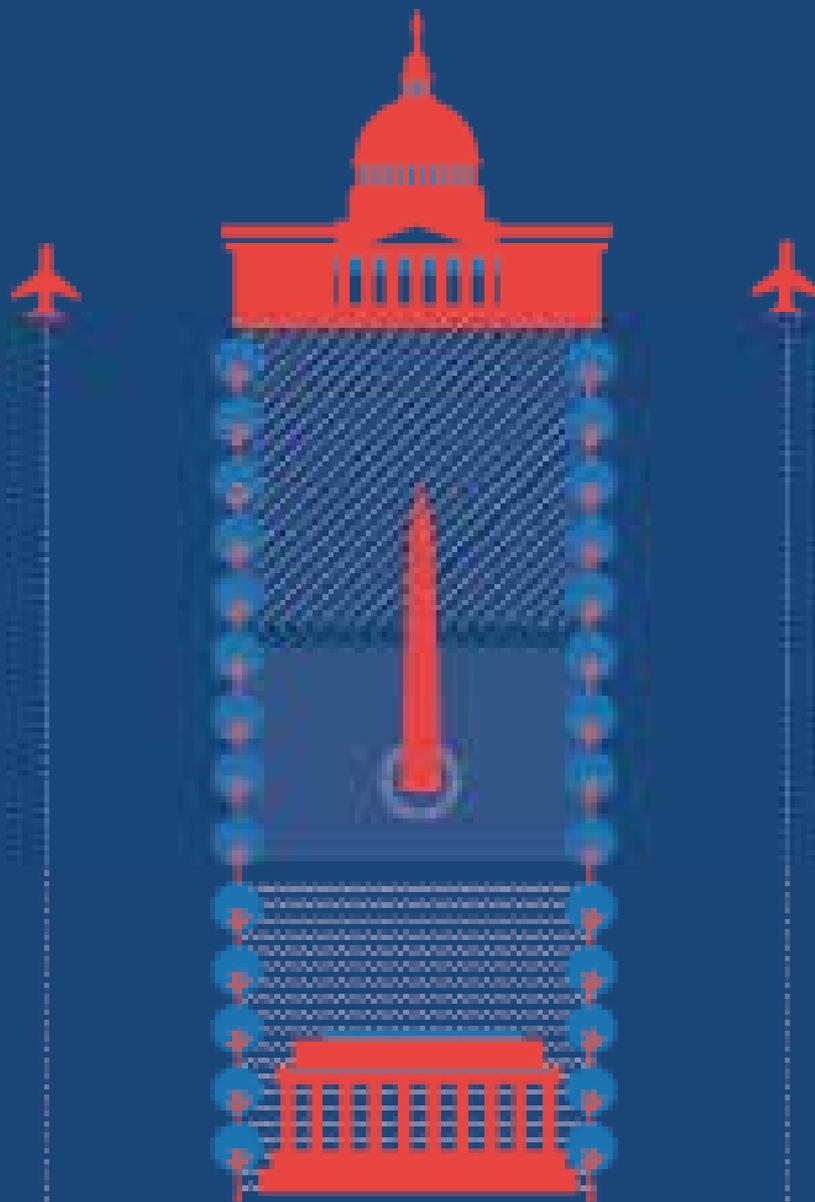




21-23 February, 2017

LEGAL SYMPOSIUM

WASHINGTON DC





Aruba's happy passengers

Aruba Happy Flow is the world's first end-to-end seamless passenger flow enabled through the use of a biometric single token, says *Annet Steenbergen*.

The two-year pilot, which started in May 2015, is a combined effort of the Government of Aruba, the local airport, KLM, the Schiphol Group, and Vision-Box.

Happy Flow creates a uniform, secure, and passenger-friendly approach for the different steps the passenger has to go through at an airport. Instead of cumbersome and repetitive checks of travel documents, there is one secure identity check that is reused through a single biometric token.

At check-in, a passenger's e-passport is authenticated and verified and the person holding the document is matched to the biometrics stored in the e-passport. From then on the person's identity and process information is stored in a personal data envelope that is matched at each step, such as bag drop, border/access control, and boarding.

The Happy Flow platform is built according to the privacy by design principle. This means that, although airport, airline, and government are using the same platform to enable a passenger journey with a single token, the way information is shared is in strict accordance with all relevant privacy

laws and regulations. This is crucial and forms the foundation of a multi-stakeholder, public-private cooperation.

The result is a drastic reduction in waiting times and better use of infrastructure. Moreover, it generates real-time data that enables dynamic support of the airport process for all stakeholders involved. By adding business rules to the platform, based on security or process indicators, efficiency for both public and private stakeholders increases.

Aruba Happy Flow is an innovative airport process, maximizing both flow and security while keeping a passenger-centric focus. •

Reporting a cyberattack

The need for partnership in cybersecurity strategies is paramount. An open, sharing environment would make it easier to find that crucial piece of information that reveals the origin or design of a cyberattack.

Reporting and communication is one of three pillars in IATA's cybersecurity strategy, alongside risk management and advocacy. The strategy is designed to help airlines combat cybercrime and details the challenges and potential solutions.

For example, a first step toward more extensive reporting is clarifying exactly what needs to be communicated. Internal reporting, reporting between

airlines on specific threats, and reporting across the industry value chain all must be considered. Additionally, there can be reporting via an authority or to an authority, similar to detailing safety incidents.

And though an open cyber culture is being further developed through the Information Sharing and

Analysis Centers (ISACs) coming online in the United States and Europe, many are asking whether the mandatory reporting of cyberattacks might be the best way forward.

Cybersecurity consultant, Menny Barzilay, CEO of FortyTwo, has noted that many of the most interesting and sophisticated cyberattacks were not publicly disclosed. "This

creates two major problems," he said. "First, another organization cannot improve their security solutions based on the lessons learned from the attack. That means that the same attack can be effective many times before someone discovers it. Second, public criticism is an effective incentive for senior management to act and invest the needed resources in addressing cybersecurity issues."

The use of such terms as mandatory or recommended can be equated to ICAO Standards and Recommended Practices (SARPs) and, globally speaking, ICAO would be the only place to implement such SARPs.

However it is achieved, the industry needs to work out ways to combat the cybercriminal and develop cybersecurity methodologies that put airlines ahead of the curve. •

Why airlines are vulnerable

Two rules of thumb illustrate why airlines must take the cybersecurity threat seriously. First, complex systems are more vulnerable. It is harder to protect a building than to protect a room, and harder to protect a city than a building. Many airlines have city-sized networking.

Second, security-by-design is the most effective way of securing things. The aviation industry, however, contains many legacy systems that were not designed to face current threats and were usually developed without considering the security implications.

Of course, airlines are not the only companies that failed to anticipate the rise of the Internet and its associated dark side. It is quite probable the Internet would have been designed in a completely different way if its ubiquity was assured. One potential redesign solution is software-designed-networking, an umbrella term for an emerging architecture that provides more flexibility and control over Internet traffic flows. While this might be the light at the end of the tunnel, that tunnel is very long, and software-designed-networking has some way to go to reach maturity.



Securitas Aviation

Knowledge and Focus on Aviation Security

Our approach

The aviation industry is a complex international environment in constant evolution.

Our security solutions combine years of experience with the state-of-the-art technology and our industry-leading expertise.

Our aim is to raise awareness, to protect and to dissuade.

Securitas Transport Aviation Services
Sint-Lambertusweg 3 Post-Bus 1404
B-1120 Brussels - Belgium

T +32 2 269 55 2122

www.securitas.com

Our Services

Through planning, protection and prevention, our services offer security and peace of mind for airports, airlines, freight forwarders and many other airport-related businesses.

- Passenger and Staff Screening
- Hand and Hold Baggage Screening
- Physical Baggage Inspection
- Cargo Security
- Explosive Detection Dogs (EDC)
- Catering Security
- Mail Security
- Passenger Profiling
- Document Verification
- Gate Security, Boarding Control
- Aircraft Guarding
- Aircraft Search
- Access Control
- Control Room
- Perimeter and Fence Control
- Guarding of parking lots, hotels, shops and banks
- Patrol Services
- Fire and Rescue Services
- Aviation Security Training Courses
- Auditing Services