The **silent** enemy

Chair of ACI's Cybersecurity Taskforce, Dominic Nessi, tells *Airport World* more about what the organisation is doing to combat the growing threat of cybercrime.

The World Economic Forum has identified cybersecurity among its top global risks in each of the last eight years.

As the world shrinks, governments will continue to focus on open trade policies, allowing for significant trans-border investments, promoting international collaboration and encouraging international tourism, increasing air traffic as a significant by-product.

To meet this growing need, airports will implement transformative technologies to reduce costs, increase customer satisfaction, and increase productivity in airport operations.

Similarly, passengers (business and leisure) will be communicating around the clock at all airport locations and the overwhelming majority will have significant digital literacy and the mobile devices available to stay communicated.

The result is that airport operations, technology and passenger interaction will be fully converged.

It is estimated that by 2025, there will be 4.7 billion Internet users – an almost 300% increase from today. A critical aspect of this growth is that 75% of it will be occurring in emerging economies, primarily in Asia and Africa, where cybersecurity strategies are struggling to keep pace with this explosive growth.

This explosion in the digital landscape will have a significant impact on airports, and while it is fairly obvious that each airport is responsible for its own cybersecurity environment, airports as a community must work together to establish an industry-wide secure environment.

ACI is leading the charge for improving cybersecurity at airports throughout the world through a series of cybersecurity-related projects. These initiatives are focused on improving security awareness at the airport management level as well as providing specific guidance on operational tasks that all airports should execute.

Indeed, ACI World's director general, Angela Gittens, has taken a personal interest in cybersecurity and has directed that the organisation establish "stronger IT security for a stronger airport community."

In 2014, ACI World created a Cybersecurity Taskforce with the objective of developing a comprehensive cybersecurity programme. Composed of airport representatives from across the world, the taskforce has been instrumental in creating a focused approach to airport cybersecurity.

The latest product produced by ACI is the implementation of its 'Airport IT Security Benchmarking Tool, which is based on the international cybersecurity framework ISO 27002.

ISO 27002 is an advisory document, which recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information.

The tool provides a framework for determining a cybersecurity approach, though leaves airports with the flexibility to assess their own information risks, clarify their control objectives and apply appropriate controls using the standard for guidance.

While the full ISO 27002 framework contains over 1,200 detailed with some 35 control objectives focusing on the need to protect the confidentiality, integrity and availability of airport data and physical assets, the newly implemented Benchmarking Tool lists 106 specific controls that an airport should employ to help it assure that its cybersecurity programme is robust and comprehensive.

Once an airport completes its ISO 27002 assessment it receives an over-all score based on a capability maturity model which ranks an airport's cybersecurity practices from non-existent to optimised.

Airports can then develop a risk mitigation strategy to meet the ISO 27002 guidance and regularly test its progress towards achieving a higher level of maturity.

An important aspect of the Airport IT Security Benchmarking Tool is that an airport can compare its cybersecurity programme and readiness against other airports, geographically and by size.

Though all information is maintained anonymously, an airport will still get an indication of where its own programme stands. Furthermore, ACI will be able to use all of the information compiled to get a better picture of cybersecurity globally.

While ACI is focusing on ACI members to start with, the Benchmarking Tool can be used by non-ACI airports as well. It is available on an annual subscription basis and almost 30 airports have already signed up or expressed interest in acquiring it in just its first week of availability.

The Benchmarking Tool is just one of the 'Ten Points of Cybersecurity' that ACI is advocating to its member airports. The ten points are:

1. **Recognise the reality and don't underestimate the problem** – ACI is emphasising that cybersecurity is a real concern and that there have already been enough cybersecurity incidents experienced by airports to make cybersecurity an important topic on ACI agendas at all levels.
2. **Cybersecurity is a top management issue** – ACI is working to inform and educate airport management that cybersecurity is an issue which must be addressed.
3. **Think aviation industry-wide** – ACI is working with the entire air transport industry (airlines, aircraft manufacturers and governments etc) to complement industry-wide cybersecurity goals and initiatives.
4. **Establish a security programme** – ACI is advocating that all airports, irrespective of size, establish a cybersecurity programme with a full governance programme which identifies airport information assets and prioritises cybersecurity mitigation efforts.
5. **Perform risk assessment and prioritise airport defences** – ACI advocates that all airports conduct a risk assessment, identify threats and vulnerabilities and develop an appropriate mitigation programme.
6. **Establish a strong patching programme** – ACI is emphasising the importance of each airport developing a comprehensive and timely patching programme.
7. **Include cybersecurity in all levels of the organisation** – ACI emphasises that cybersecurity is not just an information technology issue. It affects all airport organisations and education specific to each function is essential.
8. **Increase airport internal capability/acquire qualified external assistance** – ACI encourages all airports to either acquire internal cybersecurity expertise and/or acquire external assistance to assist in the implementation of cybersecurity tools and defensive practices.
9. **Develop an adaptive security architecture** – Because an IT environment is dynamic, ACI encourages all airports to continually evaluate its cybersecurity environment and to evolve its defences to meet the latest security threats.
10. **Acquire the Airport IT Security Benchmarking Tool** – To help evaluate your airport's progress in securing its cybersecurity environment.

We have to take cybersecurity seriously as airports have already been attacked and more will be attacked in the future, and anyone who says that this won't happen is badly mistaken.

Baggage systems, utilities, credentialling systems, ground radar, airport business systems, we have so many potential areas that can be hacked at an airport and it can be done in so many ways, including new 'ransomware' software, which denies you access to systems until a ransom payment is made to unlock it.

This is why sharing critical data on cybersecurity is important as we really don't know how many airports have been attacked or how much money we've lost as an industry.

Also you have to remember that a cyber attack is a completely different animal to a physical terrorist attack, which airports prepare for and its impact is immediate. In comparison, it takes an average of 240 days to discover a cyber attack and many airports would not be prepared to deal with it. AW

About the author

Dominic Nessi is Burns Engineering – AeroTech Partners' senior technology advisor and former deputy executive director/chief information officer at LAWA. For more information about ACI's cybersecurity efforts contact him at dnessi@aerotechpartners.com or ACI World's Serge Yonke Nguewo at SYonkeNguewo@aci.aero