Web-Based Data Mining: automating aviation security

The big debate in the aviation security industry today is the question of which is better: behaviour-based security or data-based security? The answer, of course, is that both are critical. The limitation of this argument is that data-based security is neither defined nor standardised. Delving into this data-based security issue begs a myriad of questions that are difficult for a carrier to answer, such as: Can data alone provide operational security? Can data be transformed into information that is actionable? How will this work? What are the requirements? Is there regulatory value? The deeper we dive the more questions arise. ***Philip Baum*** *explores one carrier's initial step into the foray of data-based security for aviation and explains how the carrier determined that a web-based platform should be the cornerstone of a comprehensive security programme.*

The evolution of the Secure Flight system in the United States required passengers to enter unique identifiers, marking the first opportunity for airline systems to substantively differentiate passengers. One carrier, found itself able to seize upon several opportunities to strategically use TSA-required data to monitor a multitude of risks in the operational environment, add value by implementing their own security systems and, in fact, to monitor the TSA and their actions.

For what I trust are wholly understandable reasons, it is not necessary to actually name the carrier which has effected this initiative, but as the system they have developed may be a model for the future of web-based tools for data-mining and automation of airline security systems and, in the interest of sharing best practices, I invite you to review this model and determine applicability to your systems.

Industry not Keeping Pace

The industry norm is today as it has been since pre-9/11: for passenger risk to be identified at the ticket counter, without advance notification. It comes as a surprise to the agent, who is thereafter responsible for the passenger's handling, each time a passenger is initially prevented (inhibited) from checking-in. What is unfortunate about this scenario is that airline reservations systems hold valuable data that uniquely identify passengers travelling to, from and within the United States and many other countries. To date, the TSA has spent $43.38 million on the Secure Flight programme. It runs a multitude of scrubs against watchlist data and performs analytics to evaluate risk. Similarly many governments have adopted systems tailored for their pre-arrival immigration purposes in the form of systems known as APP or IAPP systems and in the US, the Customs and Border Protection (CBP's) APIS Quick Query system at the cost of unknown millions. All of these systems deliver clearance results to the airline reservations system. It is these results that present the first opportunity for a carrier to capture this data from their own systems to identify risks in advance of departure. Clearance results can be displayed for managers to engage in risk-reduction activities that are operationally cost-effective and, for regulatory purposes, are also measureable in terms of international standards: IATA's Operational Safety Audit (IOSA) and Security Management System (SeMS).

Web-based Systems are Key

At the time Secure Flight development work was required, one carrier identified a return on investment opportunity to analyse passenger clearance results data to increase its operational security and regulatory compliance. A web-based platform was designed to extract, manipulate and display security data from the reservations system onto a Dashboard *(see Fig. 1 opposite)* and to drive multiple automated reporting systems designed to add value, reduce risk and support the operation.

The platform begins by extracting passenger clearances to populate a database. Inhibited responses are then run against the TSA's watchlists. It is from this data that the value added systems begin.

The Dashboard displays 5 days of system-wide data [-1, 0, +1, + 2, +3], principally: yesterday, today, and the 3 day/72 hour secure flight window.

Fig 1: Dashboard: the numbers shown below are for example purposes only and not actual

System-Wide Status	Flight Date 10/23/2013	Flight Date 10/24/2013	Flight Date 10/25/2013	Flight Date 10/26/2013	Flight Date 10/27/2013
High	8	2	1	2	2	1
Elevated	16	2	1	3	7	3
No Fly Pax	1					1
Selectee Pax	6		1	2		3
Random	342	63	46	65	115	53
Decline Service Pax	1					1
Review Service Pax	4	2		1	1	
Distinguished Traveler	83	21	18	10	20	14
Armed	114	14	29	22	31	18
Fraud	8	4	6	2	7	1

"...if there are fewer than three data point matches, the name is released and the reservation is not inhibited, effectively eliminating false positive matches for passengers with similar names..."

Matches or potential matches to the No Fly and Selectee lists are displayed, names that are inhibited but not found on either watchlist are identified as 'Random'. Note that the discontinuation of watchlist distribution is not expected to have great effect; inhibited response will remain under the Random identifier unless specifically identified.

The Dashboard is actionable by a single security analyst; sufficient because the layout clearly delineates risks system-wide and removes the need for research or to piece the picture together from multiple sources. This may present a significant cost savings opportunity over carriers that need to maintain a security desk in their 24-hour Operations Control Centres.

Service Evaluation Program

Airlines have had their own internal watchlists for years; this is not new. What is new is that the system can be fully automated. The company's security systems overlay the foundation provided by government clearances and its internal watchlists make use of 'buckets' in the reservations system that can be used to inhibit passengers for internal reasons; the buckets are namely a 'Decline Service List', and a 'Review Service List'. Name matches to any of these buckets are placed in a queue for processing. The processor then opens each reservation and searches for at least three of 12 captured data points to avoid false positive matches. Examples of these data elements are frequent flyer number, email address, phone number, etc. If there are fewer than three data point matches, the name is released and the reservation is not inhibited, effectively eliminating false positive matches for passengers with similar names. There are business and process rules around each bucket that are trained in regulatory required initial and recurrent security courses including role playing.

From a process perspective, the Decline Service List disallows a passenger from any future travel. The Review Service List requires Ground Security Coordinator (GSC) engagement with the passenger before the reservation is released and the passenger is allowed to check in.

Value Added Automation

Separately from the bucket system above and displayed at the bottom of this section, 'Distinguished Traveller' is a pseudonym the carrier uses to indicate Federal Air Marshals (FAMs) in order to protect their anonymity. 'Armed' indicates the passenger is a law enforcement officer that has disclosed in advance they are travelling armed. The 'Fraud List' indicates reservations flagged by the fraud team and are inhibited from automated check in. Agents require proof of purchasing card or are able to accept an alternative form of payment.

Detailed supporting data for each figure captured on the Dashboard is available in drop down lists form the tool bar for analysis or action.

Additionally, a display indicates numbers of system-wide risks by flight departure time by hour *(see Fig. 2 below)* and, for the three day secure flight window, displays any spikes in activity for investigation by the analyst. Opportunities also exist to validate TSA intent with the carrier's liaison partners, increase staffing and service centre positions, and have reservations conduct call outs to request passengers to arrive early.

Automated Station Security Reports

Each evening, the site disseminates station-specific security reports *(see Fig. 3 on page 18)* to frontline leaders to identify known risks for the following day's operation. Managers use these reports as a planning and briefing tool to effectively differentiate passengers with known risk. The goal is to allow managers to prepare for passenger engagements that will occur for Selectee, Review, or Fraud passengers, to expect FAMs and to be able to ensure armed individuals on board are informed of each other. Flights with high numbers of risks on board are flagged as High or Elevated Risk.

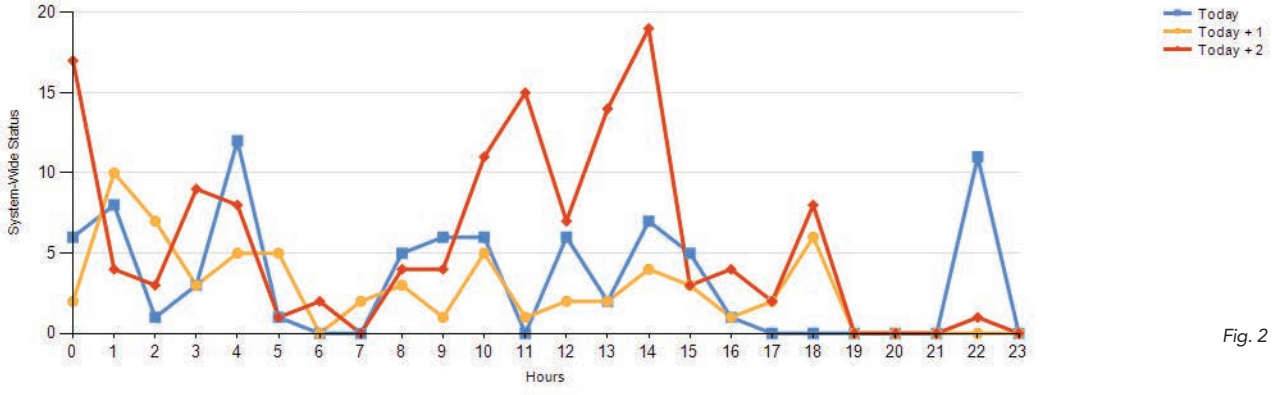


Fig. 2

Fig. 3

Station Security Report

Station Stats	
NoFly	2
Selectee	1
Random	1
No Clearance	533
O/B Review List	1
I/B Review List	0
Armed	1
Distinguished Traveler	3
Fraud	1
PreCheck	5489

High
722

Elevated

Outbound Station: LHR **Travel Date: 1/18/2014**

Flight	Potential Match	Last Name	First Name	Held Seat #	REC LOC
722	No Fly	NARINE	ALEX	13A	WUHKUM
		TRICOCHE	RICHARD	13B	KYL7REV
	Fraud	OWEN	TCHAKA	14C	WUTKR
	Armed	ARCHER	JOHN	19B	HTXQBF
620	Distinguished Traveler	BARRETT	THOMAS	3B	HPCEZE
		RICHARDS	CRAIG	33C	ULEPXC
229	Decline	JOHNSON	ROBERT	16J	YEKO6M
282	Distinguished Traveler	LYONS	DANIEL	3G	FZHOHH
366	Random	NERO	EDUARDO	9D	VITMWY
	Selectee	WINGO	EUGENE	26E	LMYSTP
304	Review	FRASCARELLI	KYLE	17C	KRTLMY

Changing the Landscape

Considering the modern model with >98% passengers using automated web/kiosk/mobile check in methods, we know that each of these inhibited passengers will be driven to service counters.

Similar to the physical security evolution that has taken place in the banking industry, airport service centres (for this carrier) are designed with the consideration that risk passengers will be handled there. Egress to these podiums is secured, there is increased camera surveillance and these positions are manned by trained specialists, supervised by GSCs. The information contained in the security report does not have to be relayed to all front line personnel; rather, it is briefed to this targeted group of employees working the service centres and they have immediate access to these reports during their shift. Coordination exercises with law enforcement and security providers' results in increased uniformed presence and behavioural detection officers at these locations, adding to the level of security at these strategic locations.

Regulatory Implications

There are important additional outcomes to the management of security data at this level.

Perhaps the most apparent from a regulatory perspective is the application of these risk mitigation tools to the Security Management System (SeMS). Incident reports associated with behaviour that indicate a risk rating that is moderate or higher are captured on the SeMS Security Review Board (reports of negligible or low are trended only). With the application of the Service Evaluation Program, risk is immediately diminished, allowing for quick resolution and close out of these issues. Similarly, these examples serve extremely well as evidence of a functional security system compliant with relevant ISRPS in the bi-annual IOSA re-certification process.

"...airport service centres are designed with the consideration that risk passengers will be handled there. Egress to these podiums is secured, there is increased camera surveillance and these positions are manned by trained specialists..."

For example, common incident report trends for airlines are intoxicated passengers. Once the airline has reviewed its policies and training, residual risk remains due to the inherent nature of the problem. By placing offenders on the Service Evaluation Program as a mitigation tool for SeMS, the risk of repeat offenders diminishes to negligible, to the point where we are sufficiently confident to close the item off the Security Review Board Action Log.

Cross Functional Applications

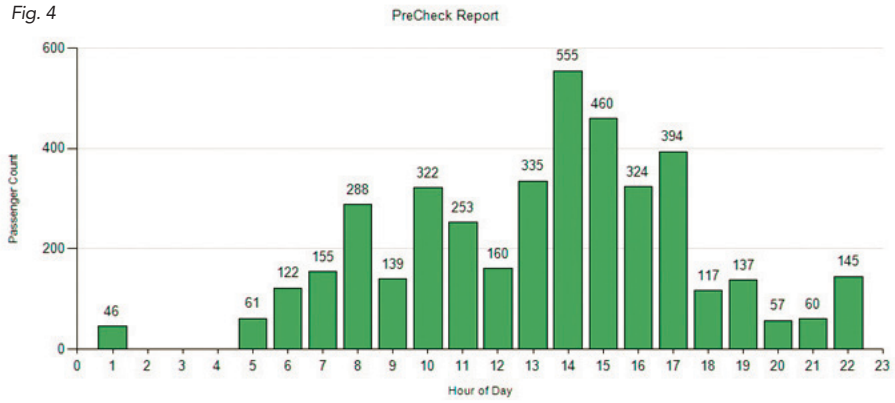
From an operational perspective, the differentiation is the primary value. However, applied more broadly, the systems allows the company to monitor TSA activity and engage strategically. One possible example is that of a Selectee travelling: should a FAM team be traveling on the same flight, the station security report would identify that and, because of the report, the GSCs will discreetly advise FAMs of the seat number and description of the party including confirmation or changes at the time the aircraft door is closed, ensuring the highest security level for the carrier

Another case would be where a heightened threat level is declared, in which one of the TSA's options is to increase, potentially significantly, the random factor for selectees. For example, in the aftermath of the attempted Times Square Bombing, initial field intelligence indicated the perpetrator may have been headed for the airport. If this scenario were to happen today, the TSA's new tools presumably allow them to increase the random selectee factor, potentially with significant impact to operations. Most carriers would have no notice and be affected by delays at the checkpoints. In today's world this would choke the few manned service podiums and the airline as much as the checkpoint. However, for the airline that is monitoring passenger clearance data, advance preparations can be made to handle the temporary increase in selectee traffic.

Most Recent Evolution: TSA Pre✓™

The TSA Pre✓™ system deployed in the United States creates a significant advantage for those passengers who receive the clearances. With minor code adjustments, the Dashboard *(see Fig. 4 on page 20)* is now capturing TSA Pre✓™ clearances by flight departure time per hour; the carrier has applied passenger arrival curve data and incorporated the TSA Pre✓™ report into their Station Security reports. This allows the front line manager to also anticipate when TSA Pre ✓™ lanes will need to be open for peak activity and when other programmes like Managed Inclusion will be most valuable. Armed with this data, the station managers are able to effectively engage with local TSA management to maximise throughput performance for the benefit of their passengers.

Fig. 4



Complete Toolbox

While these steps are the beginning of strategic use of data applications for aviation security, the ease with which the Dashboard articulates only those passengers with known or possible risk from the entire operation is an extremely valuable tool. The fact is, the results of millions of dollars of government security systems lay dormant in airline reservation systems. Mining this data, manipulating it into a user friendly display, adding airline specific processes over their results and passenger differentiation systems is not only a return on the investment already required for regulatory compliance but is also an intelligent solution that is actionable and perhaps destined to become the industry standard.

There are many growth opportunities from the current state of this model and various other applications that may better benefit carriers with different operational needs. One example would be for airlines operating in the Middle East, carrying passengers of varying degrees of loyalty programme affiliation with common names and high levels of exposure to false positive watchlist matches. If data in their loyalty programme database could be independently validated, automation may be able to be applied to check-in environments that automatically compare this data as opposed to requiring agent validation, resulting in the release of many known/high value customers with expedited service.

"...the Dashboard is now capturing TSA Pre✓™ clearances by flight departure time per hour..."

While behavioural analysis must continue and cannot be replaced, opportunities for data applications exist and can serve as the foundation for a truly comprehensive security system. Security managers have a responsibility to stay ahead of the threat. The differentiation that data affords security programmes cannot be ignored and will be relied upon with exponential value to those that invest their efforts in this area. ■

Philip Baum is the Editor-in-Chief of Aviation Security International.

Should any readers wish comments regarding the system outlined in this article to be forwarded to the carrier behind the initiative, please e-mail Philip at editor@avsec.com