

# INSURANCE DAY

WWW.INSURANCEDAY.COM

MY ACCOUNT LOG C

SEARCH



Advanced Search

Archive Search

HOME

REGISTER

SUBSCRI



- FRONT PAGE
- NEWS
- IN BRIEF
- TRADING PLACES
- NEWS ANALYSIS
- COMMENT
- DIARY
- LETTERS
- FEATURES
- EYE WITNESS
- SPECIAL REPORT
- LAW



Cover

## ISSUE: 25 FEBRUARY 2003

CHOOSE A RECENT ISSUE

Select issue

- Risk Management
- Technology
- Art
- Insurance
- Regulation
- Broking
- Results
- Reinsurance
- Conferences

FREE SERVICES

OVERVIEW

SUPPLEMENTS

JOB FILE

WEB DIRECTORY

EVENTS

MARKETS

TRIAL ACCESS

SPECIALS

ABOUT US

ADVERTISE

PREMIUM SERVICES

SUBSCRIBE

BUY NOW

DIRECTORIES

NEWSLETTERS

MAGAZINES

NEWSPAPERS

BOOKS

CONFERENCES

INSURANCE

FINANCE

LAW

## Using biometrics for airport security

By Oliver Tattan, Daon, 25 February 2003

OVER the past year the dynamics of airport security have changed dramatically.

From post-September 11 imperatives to international legislation calling for improved employee and passenger screening, the call has been clear airport personnel must step up and take proactive measures to enhance security.

But where to start? From a government point of view, legislation like the Aviation and Transportation Security Act makes it clear it is the federal government's responsibility to improve airport security. But what actual steps should the airports take?

### London City airport: setting the stage for biometric security

The use of biometrics as a means of ensuring airport security is fairly new. To date, only a few forward-thinking airports have implemented a biometric security solution.

In the past the majority of biometric deployments focused on point solutions such as fingerprint, iris and facial scanning technologies.

Unfortunately, point solutions only authenticate a user locally, under a very specific set of enrolment guidelines, and do not provide the scalable technology platform needed to handle the millions of "users" at airports around the world.

To its credit, London City airport reviewed these security initiatives when considering how to implement biometrics. The challenge for London City

Insurance Age

Health Insurance

The Review

IRM



was to leverage the security benefits that biometric point solutions can bring while meeting specific security concerns unique to the transportation industry.

Similarly, London City felt it vital to integrate the infrastructure that would support the proposed biometric solutions with existing technology at the airport a wise approach for any enterprise trying to bolster security while aggressively managing costs.

In the end the desire was to secure physical access to the airport while ensuring an audit trail was established, security systems would be linked to one another, and biometric authentication would serve as the "engine" that would drive the initiative.

#### First steps

Often the first decision the scope of a biometric implementation is the most crucial. The recent news from the Transportation Security Administration concerning the Transportation Workers Identity Card project helped compel London City to start with secured physical access to sensitive areas of the airport for its 1,600 employees.

Many biometric implementations have fallen victim to grand ideas that the technology simply is not ready to support.

The lesson to other airports is clear: start with the basics, see how the first implementation integrates with "traditional" security measures, and take broader steps only after the initial tactics gain acceptance.

"We're starting with something very simple," says London City managing director Richard Gooding.

"But our vision is to take this further, speeding airport customers through the airport and passport check-in."

#### Phase two

After outlining the initial scope, London City moved ahead with fingerprint scanners integrated into existing security systems, and "smart cards" for physical access, authenticated by a proprietary identity management platform. To drive security through biometrics, the underlying infrastructure must be able to support thousands of identities and accept changes to rules and policies as the implementation grows.

Additionally, the infrastructure must be integrated with existing legacy systems to ensure relevant information about an employee is updated and recognised by administrators.

Having set the stage for an effective implementation by understanding the infrastructure issue, London City has practically guaranteed a solution that will deliver tangible results instead of round after round of technical revisions.

Keeping on top of the infrastructure issue also allows a biometric implementation to grow organically as greater security functionality is required. Having created the foundation to support an extended biometric security initiative, discussions are already under way to implement a biometric log-on for all PC applications throughout the airport and establish a "trusted traveller" check-in system that uses biometric authentication for security clearance. Finally, in light of the UK Ministry of Transport's Airport Guard Register programme, London City can also facilitate a biometric log-in for security personnel at x-ray machines across multiple security access points, creating an audit trail to monitor the baggage-screening process.

Phase three: education

London City is just getting started on the rollout of its biometric physical access solution. As the implementation begins, London City will begin educating its employees on the benefits of the new security initiative.

Employees will learn that biometric security is not an intrusive solution that limits privacy. The value in biometrics is that an individual's biometric identifier cannot be stolen or shared the smart card is what you have, the PIN is what you know and the biometric is who you are. The lesson here is simple: no matter how secure biometrics can make London City, it is vital to educate the employees on the basics of the programme, ensuring all employees have the opportunity to voice their concerns about the initiative and that their Big Brother concerns have been put to rest.

Conclusions

The London City example shows how an organisation should approach biometric security. First, scope out the project, understanding where the limitations of your organisation lie and what you can realistically accomplish in a first effort with biometrics.

Secondly, embrace the infrastructure approach and look at your first biometric initiative as the foundation for future efforts. Creating a biometric infrastructure that works in tandem with other security platforms will help IT strategists realise the potential of biometrics as implementations expand beyond the first case.

Finally, educate your key audiences. Biometric applications are not the agents of a Big Brother police state. Rather, biometrics should be seen as an enabling technology that drives security and allows employees to feel safe in their jobs.

Oliver Tattan is chief executive of Daon, which is exhibiting at Infosecurity Europe at London's Olympia from April 29 to May 1.

[Printer Friendly Version](#)

[Email this article](#)

## Basel II regulation or revolution?

[TERMS & CONDITIONS](#)

[SITE](#)

[Home](#) | [Events](#) | [Bookshop](#) | [About](#) | [Advertise](#) | [Contact](#) | [Help](#)

[ASSOCIATE SERVICES](#)

[InsuranceAge.com](#) | [the Review](#) | [Health Insurance](#)

**USERS PLEASE NOTE:** Informa UK Limited actively monitors username and password usage and reserves the right to terminate the account if abuse occurs

The content of this web site is © Informa UK Limited 2002. Reproduction, retrieval, copying or transmission of the content of this site is not permitted without the publisher's prior consent. Reproduction of part or all of the contents in any form is prohibited.

