



SENTINEL

ANTI-TERRORISM IN THE AMERICAS

Port Security

Latin America, CSI

Face to Face

Behavioral observation
hits its stride

Show Preview

ISC East Expo, New York

VOL. 1
NO. 2

PUBLISHED BY

TransSec

Guardian™ makes invisible traces of explosives extraordinarily clear

Precise screening of passengers for concealed explosives in seconds

In the war against terrorism, even the tiniest clues are critical and Syagen technology specializes in detecting them. Syagen has designed the Guardian™ Explosives Trace Detection (ETD) Portal for people screening using the most accurate technology available. The patented mass spectrometry (MS) technology detects explosives contamination as small as one-millionth a grain of sand.

MS has a resolution that's 10 to 10,000-times greater than ion mobility spectrometry (IMS). This high resolving power enables MS to screen for more than 30 explosives simultaneously without compromising accuracy and precision. This advanced technology has been recommended by the National Academy

of Sciences as the core technology for explosives trace detection for aviation security.¹

Incorporating the most advanced pre-concentration technology,² Guardian produces performance levels unmatched in sensitivity, specificity and low false negative and false positive rates for the largest number of explosive compounds and is easily upgraded to search for new compounds should the threat scenario change.

Guardian offers a comfortable environment during the brief screening process, high screening throughput and occupies a small footprint. For more information, contact Syagen Technology at 714 258-4400 x28



Guardian Explosives Trace Detection Portal



Syagen Technology, Inc.

1411 Warner Ave. • Tustin, California 92780 U.S.A.

Tel 714 258-4400 x28 • Fax 714 258-4404

Email sales@syagen.com • www.syagen.com



¹ National Research Council, "Opportunities to Improve Airport Passenger Screening with Mass Spectrometry," National Academies Press, Washington DC, 2003.

² Sandia National Laboratories (Albuquerque) "Hoand" technology.

6

Frontlines

- CoCo Communications hopes to answer the age-old problem of uncommunicative communications
- Cognitec snags a federal German contract to help law enforcement there identify suspects
- Dallmeier reloads the matrix, winning a multimillion-dollar deal to provide the world's largest digital matrix surveillance system
- Smiths joins an alliance to help outfit Fast Lanes under the U.S. Registered Traveler program
- NEMA hopes that standards for homeland security technologies will help jump-start the market (already looked pretty healthy to us)
- Euro researchers work on a plane that will just say No to would-be hijackers
- A Rand Corp. author says that civil liberties should be most zealously guarded exactly when they're most at risk
- Anexinet says its tech hub will help expand and improve U.S. Highway Watch program
- Bioscrypt has upgraded its VeriSoft Access Manager software with new network authentication and access to applications and services
- Between the devil and the deep blue egg: Qinetiq's Cerberus diver detector tries life in civvies

1 2

Face to Face

Rafi Ron has exported the Israeli behavior observation model to the U.S. and beyond. Not the whole model, naturally: the aggressive questioning and racial profiling parts of it are out of the question for now.

1 4

Q&A: Southern Cone

Port state control in the southern hemisphere presents a varied aspect, with some nations adopting a model similar to that in the U.S., where the Coast Guard acts as an independent, well resourced body to guarantee ports of entry.

1 7

The Long Arm

The Container Security Initiative has now reached 50 ports around the world. U.S. Customs and Border Protection is actively collaborating with 28 other customs administrations, stationing CBP personnel overseas to check cargoes destined for the U.S. at ports of departure.

1 8

Show Preview: ISC East Expo and Conference

ISC East 2006 takes place in New York. This flagship security event continues to expand.

2 2

Events

Industry conferences, seminars, exhibitions and symposia coming up for 2006 and 2007



The only things we have to fear



Andrew Brooks
Editor

When U.S. President Franklin D. Roosevelt uttered the famous phrase “the only thing we have to fear is fear itself” in his 1933 inaugural address, he was referring to the incapacitating effects of fear on the ability of an entire population to act with the clear-headed resolve required. In that specific case, he was referring to the battle against the effects of the Depression, which as we know was at root a psychological fight, as the problems were largely created by a collapse of investor confidence in 1929.

A decade later the world was embroiled in a conflict whose reality was brutally physical, and in which victory required the fullest possible range of material resources and actions to be employed. But the psychological war – the battle for confidence – was no less important a struggle. Fear was as much an enemy as the armed forces of the other side.

In this issue’s news section, we refer to a new Rand Corp. book by veteran antiterror expert Brian Jenkins. Jenkins has put in his time at the pointy end of his country’s foreign policy, serving as a captain in the U.S. Army Special Forces in Vietnam before launching Rand’s terrorism research program in 1972. His book, titled *Unconquerable Nation: Knowing Our Enemy, Strengthening Ourselves*, is, despite its militaristic tone, a call for sober clear-headedness at a time when fear seems to have carried the day. Jenkins argues that the very civil liberties that are now increasingly seen as a weakness in the ‘war on terror’ are in fact potent anti-terrorist weapons in their own right.

Fear has its own momentum. So much so that, several weeks after the discovery of an alleged airliner bomb plot in London, the truth is still having a hard time catching up. At the

time, security experts on both sides of the Atlantic were quick to claim the plot had been foiled just in time, and that the potential loss of life would have been on an unimaginable scale. They’ve since backed down on those claims – in some cases even admitting they overreacted – although you wouldn’t know it from the way the event is still discussed.

It turns out that the plotters were a long way away from putting any plans into action. More importantly, a number of scientific analyses have revealed that formulating and then using a liquid explosive is exponentially more difficult than mixing Diet Coke and Diet Pepsi. Some of the descriptions of how such a device would have to be activated on an airliner – assuming the bombers had survived the process of formulating one in the first place – are actually comical.

But fear has its own momentum. Even as some of the immediate security measures taken after the liquid-bomb plot have now been relaxed, there are authoritative, respectable voices saying they should be maintained. Clark Kent Ervin, who made his name as a forthright inspector general of the Department of Homeland Security [we interviewed Mr. Ervin in the March/April 2005 *TransSec*], has publicly called for the liquid bans to be maintained, saying that liquid bomb countermeasures are still lacking.

Ervin’s critique aside, Brian Jenkins makes the point that allowing fear to run rampant is more than incapacitating: it’s actively counter-productive. As he points out, surrendering to fear can also mean surrendering to government measures that curtail civil liberties and erode the scope for political action in the first place.

Ominous steps on this path have already been taken in the U.S., and unless something changes more is sure to follow. ■



SENTINEL: ANTI-TERRORISM IN THE AMERICAS is published two times per year (April/May, October) by *TransSec Magazine*, 5720 Timberlea Blvd., Suite 201, Mississauga, Ontario, L4W 4W1, Canada. It is distributed internationally to homeland security executives, regulatory bodies, immigration and customs officials, security and policy makers, academic institutions, training specialists, legal firms, manufacturers, security technology suppliers, consulting firms, maintenance facilities and insurance companies.

Subscriptions: US\$200 for one year, US\$300 for two years and US\$400 for three years. Art and photographs will not be returned unless accompanied by return postage. The views expressed in this magazine do not necessarily reflect the views and opinions of the publisher or editor. October 2006 Volume 1, Issue 2. Printed in Canada. All rights reserved. Nothing may be reprinted in whole or in part without written permission from the publisher. © 2006 Global Marketing Company Ltd.

SENTINEL Magazine
5720 Timberlea Blvd., Suite 201,
Mississauga, Ontario, L4W 4W1, Canada
Tel: 1 905 629 0007 Fax: 1 905 629 1933
www.transsec-magazine.com

PUBLISHER:

Aijaz Khan
aijaz@globalmarketingcom.ca

EDITOR:

Andrew Brooks
andrew@transsec-magazine.com

ART DIRECTOR:

Patrick Balanquit
patrick@globalmarketingcom.ca

SUBSCRIPTION MANAGER:

Pina Lagrotteria
pina@globalmarketingcom.ca

EDITORIAL ADVISORY BOARD

Dr. Abdulla Al Hashimi, senior vice-president, Emirates Group Security

Michael Crye, Esq, president, International Council of Cruise Lines

Theo W. Fletcher, vice-president, supply chain compliance, security and diversity, IBM Integrated Supply Chain

David Forbes, president, BoydForbes Inc.

PROTECT AGAINST TERRORISM

With 20 years in the security industry, Mistral has experience needed to protect against terrorism:

- * Experts who have provided security assessments to some of the largest terminals and busiest airlines in the world.
- * Products to Detect and Identify Military and Commercially available explosive materials, **including improvised explosives such as TATP and liquid explosives.**
- * Bomb-mitigating trash cans and Check-Point temporary containment systems.
- * Fully Confined Bomb Containment Vessels to safely remove bombs.
- * Mistral also offers a full Product Line of Forensics and Drug Detection & Identification.
- * *US Purchasers Eligible for Homeland Security Funding.*

KNOW THE THREAT Detect & Identify Explosives



MINIMIZE Terminal Down Time



PROTECT Your Transit Commuters



 **Mistral Security** INC.
Providers of Security Products and Services.

U.S., Central & South America Sales
1-800-964-7872
security@mistralgroup.com

Europe, Asia and Middle East Sales
+972-995-56-8-212
sales@karil.com

WWW.MISTRALGROUP.COM

Un-hijackable planes next?

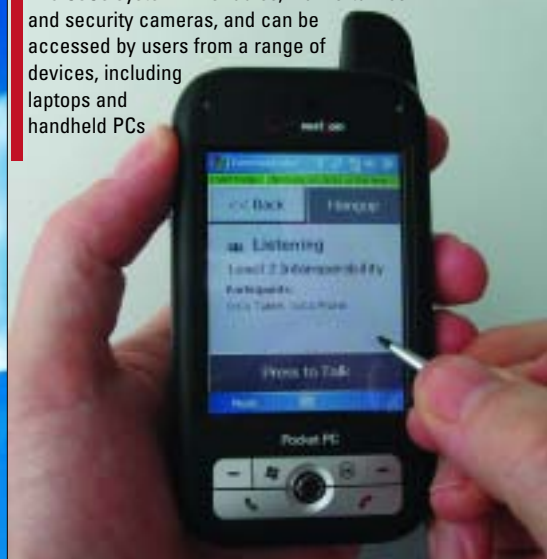
A group of European aviation companies is researching the possibility of developing an airliner that would be impossible to hijack. The project is part of a multi-year plan, and the airliner testing phase launched a few months ago as part of the Security of Aircraft in the Future European Environment (SAFE) initiative. Research will continue into next year at a number of sites in Europe.

The system involves the use of video and audio monitoring equipment being developed by BAE, linked up with CCTV, biometrics and other technologies to keep unauthorized people from taking over at the controls of a commercial airliner. Other elements include technology to match passengers to luggage, biometric ID at check-in, encryption of communications between the airliner and ground control stations, and explosives detection systems.

Even if hijackers do take over an aircraft, one system being researched as part of the project would ensure that the aircraft would simply “refuse” to collide with buildings or other aircraft, overriding the control inputs of the hijackers and steering for the nearest airport. (Whether this would include an auto-land feature has not been indicated, but it seems like a logical step.)

Some 100 aviation experts from 31 companies are involved in the research.

The CoCo system links radios, walkie-talkies and security cameras, and can be accessed by users from a range of devices, including laptops and handheld PCs



CoCo connects the dots

As first-responder agencies struggle to update their communications systems and networking capabilities to keep up with increased security challenges, one common complaint has been that recently adopted newer systems often simply don't ‘talk’ with the older systems that have been in place for years. That challenge has spawned a new generation of technology tools that aim to link old ‘legacy’ communication systems with new, state-of-the-art ones so that cash-starved first responders don't have to throw out existing systems in order to be able to communicate freely with a wide range of fellow agencies.

Recently, federal, state and local officials in the state of Texas announced that Dallas Love Field in Texas had rolled out a fully interoperable communications service that allows police and firefighters, federal agencies, private industry and airport staff to communicate with each other over their existing networks and equipment. The Dallas Love Field Integration Project is the result of a public-private partnership that has delivered the first interoperable network in the U.S. that utilizes secure voice, video and data communications for emergency response and critical infrastructure management.

The system is based on software from CoCo Communications, known as the CoCo Protocol, which ‘rides’ on top of existing network infrastructure. According to a press report, the system can send live video images of passengers at a security checkpoint to a user's laptop PC while also displaying radio contacts for local police and fire departments, linking agencies that until recently “could not hear each others’ radio signals.”

Next-generation airliners could have the smarts to steer clear of tall buildings if taken over by terrorists

Smiths joins FLO Alliance

Smiths Detection will supply security equipment including its Sentinel II explosives detection walk-through trace portal for Fast Lane Option (FLO), a Registered Traveler (RT) program. The system will be delivered for FLO Registered Traveler lanes at major airports (it is already deployed at several).

The Sentinel II uses Ion Mobility Spectrometry, a technology proven in explosives trace detection. The system operates automatically, and Smiths says the throughput rate will help prevent airport delays.

The FLO Alliance for Registered Traveler was originally formed in 2005 and brings together technology, finance and security leaders to provide for the complete Registered Traveler credentialing process. It includes Safflink Corp., Microsoft, JPMorgan Chase, Johnson Controls, ID Technology Partners and the Paradise Shops.



Smiths says the Sentinel II will automate significant security processes, enabling staff to devote more time to high-risk and unknown travelers

X-ray Technology for Baggage, Passenger and Air Cargo Inspection

Amit Verma, Product Manager, Rapiscan Systems
 averma@rapiscansystems.com

X-ray technology has provided the basis of security screening for decades and will continue to play a vital role in the future. Like any technology, X-ray has strengths and weaknesses and when used alone can be inadequate at detecting some types of threats. The most effective way to screen passengers and cargo includes X-ray combined with other approaches. When complementary technologies are combined into a single system, detection is improved and security is better assured.

Passenger screening can be improved with Backscatter systems that complement today's metal detectors. Backscatter X-ray is completely safe, is available today, and is the most effective way to screen for non-metallic threats like explosives or ceramic weapons that may be concealed under clothing. Quadrupole Resonance (QR) in combination with X-ray can be deployed to automatically detect the most dangerous and hard to find categories of explosives in baggage and mail. Combined X-ray and QR systems are now available.

The most effective way to screen airborne cargo is high energy X-ray combined with neutron analysis. The addition of neutron analysis provides automatic detection of explosives (by gamma-ray spectroscopy) whereas X-ray alone provides an image for operator inspection. Automatic detection is a vital part of cargo screening because it reduces false alarms and preserves the rapid flow of commerce.

Technology alone is not the answer. Resources are limited, money does not grow on trees and our society must find a lawful and effective way to allocate the vast majority of security spending to the small fraction of passengers and cargo that pose a real threat. Without a resolution to this problem, scarce resources can drive an unacceptable outcome: the lowest-common-denominator.

When looking to solve the most difficult challenges in security, X-ray combined with other complementary methods is a logical path forward. Learn more about the technologies available before committing to a solution.



Rapiscan[®]
 systems

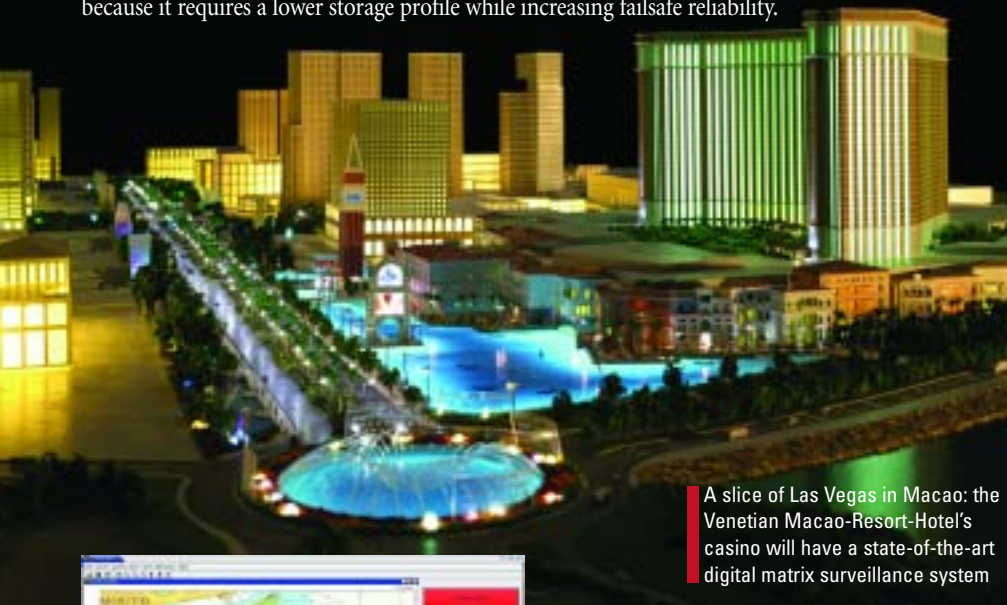
An OSI Systems Company

ONE COMPANY - TOTAL SECURITY

Dallmeier wins landmark matrix contract

Dallmeier International has been awarded a multimillion dollar contract to supply and commission the world's largest digital matrix surveillance system. The system will be installed at the Venetian Macao-Resort-Hotel in Macao, a mammoth Vegas-style US\$1.8 billion project that will be complete in 2007.

The Dallmeier system will be used to monitor the hotel casino, which consists of 546,000 square feet of gaming floor, over 6000 slot machines and 700 table games. The system will include hardware, software, and monitoring and transmission components. It will operate on the principle of decentralized recording, which optimizes security and availability of data and increases cost effectiveness: decentralized recording is about three times as cost effective as traditional centralized recording because it requires a lower storage profile while increasing failsafe reliability.



A slice of Las Vegas in Macao: the Venetian Macao-Resort-Hotel's casino will have a state-of-the-art digital matrix surveillance system



The Cerberus marine detection system (users refer to it as an "egg") shown with a screen displaying the tracks of two detected divers



Swimmer detector protects races

The Cerberus high performance swimmer detection sonar system from QinetiQ had its first non-military deployment this summer when it was part of the security measures for the America's Cup ranking events in Valencia. Two unauthorized divers were actually detected during the deployment – although it turned out that they weren't a security threat.

QinetiQ leased two Cerberus units to Elecpor Seguridad, the Spanish company contracted to provide security systems for the duration of the 2006 ranking events in Valencia. The two Cerberus units were positioned in such a way to detect any divers or swimmers approaching the entrance to the Port of Valencia, and also inside the inner harbor basin.

Cerberus is able to detect and locate swimmers and divers at ranges exceeding 800 meters, providing operators with sufficient time to establish whether that individual represents a threat and decide upon an appropriate response. The system has previously been deployed with naval forces around the world, including the U.S. Navy in the Middle East, but Valencia represented the first non-military deployment of the system anywhere in the world.

Rand author balances security, liberties

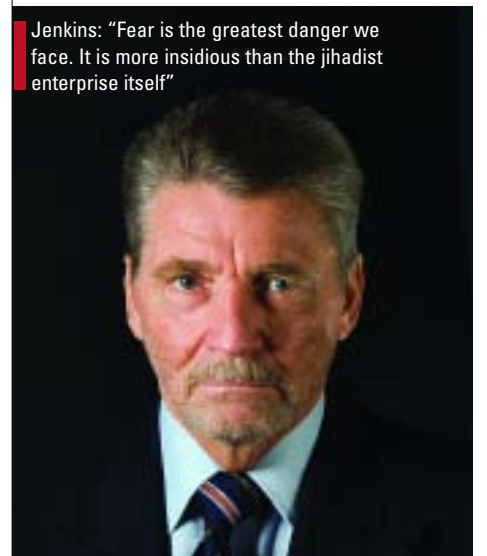
One of the most contentious areas of homeland security is the question of balancing civil liberties with the need for robust counterterrorism activities. In a new book published by the Rand Corporation, veteran terrorism expert Brian Jenkins sets out a strategy for balancing the two imperatives – with a focus on keeping the former from being edged out by the latter.

In *Unconquerable Nation: Knowing Our Enemy, Strengthening Ourselves*, Jenkins asserts that ideals of personal liberty and political freedom should be viewed as part of the arsenal in the war on terror, not as constraints upon it, particularly as it is a war based on ideology. He takes strong issue with government actions to extend executive power and encroach on the freedoms of citizens.

"Whatever we do at home and abroad must be consistent with our values, and here I think we in America are in some danger," Jenkins says. "America cannot claim to be a nation of laws and a champion of democracy when we too easily accept a disturbing pattern by our own government of ignoring inconvenient rules, justifying U.S. actions by extraordinary circumstances, readily resorting to extra-judicial actions based upon broad assertions of unlimited executive authority, and rejecting any constraints on how we treat those we have captured in the war on terrorism. The defense of democracy demands the defense of democracy's ideals."

Jenkins also stresses the involvement of an active, engaged citizenry, and believes that the first step is to combat feelings of helplessness through education, for example by making more people at home understand that the odds of becoming a terror victim are small, and that useful action can be taken on the local and individual levels.

Jenkins: "Fear is the greatest danger we face. It is more insidious than the jihadist enterprise itself"





APTS

Airport, Port & Transport Security
5-6 December 2006, Olympia, London
www.pts-expo.com

“The international exposure adds an extra dimension to APTS. Any international contact is good for the industry and merging the conference with the exhibition makes a far more focused event; it's a good formula.”

Gareth Jenkins,
Business Development Manager,
Thales Underwater Systems

Europe's leading transport and border security event



Now in its **5**th year!



Visit London's largest security event covering transport and border security for FREE

The perfect forum for serious buyers and specifiers

See what's new in the industry, source new products, meet suppliers and learn about new solutions

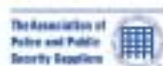
Take advantage of free seminars, workshops and live demonstrations

Attend the high level conference programme

VISIT THE EXHIBITION FOR FREE

Register today at www.pts-expo.com/visit or contact +44 (0)20 7153 4569

Supported by:



Co-located alongside:



New Threats, New Vulnerabilities, New Challenges... **Building a Secure World**

Anexinet extends highway security

Anexinet Corp. has demonstrated technology that it says will dramatically expand the membership of the U.S. Highway Watch program to more than three million truck and bus drivers across the U.S. Highway Watch is the national highway safety and security program that is administered by the American Trucking Associations in cooperation with the Department of Homeland Security (DHS). It trains transportation professionals to respond when they are attacked or if they witness potential threats.

Anexinet's contribution is a new, web-based "Technology Hub of Operations." Already 60 percent complete and in use across all 50 states of the U.S., the hub centralizes and integrates Highway Watch systems for Enterprise Content Management, Association Management, Customer Relationship Management, Web-based Training and Business Intelligence. As a result, says ATA, the system's national call center is now more efficiently operated, and larger numbers of incoming incident reports can be handled quickly, efficiently and with the appropriate response.



Cognitec wins German contract

Face recognition technology provider Cognitec Systems has been awarded a contract to provide software and services to the German Federal Criminal Police Office (Bundeskriminalamt – BKA) after winning a pan-European tender.

Used to analyze photographs and video data, Cognitec's face recognition software will support the BKA's research and identification of unknown criminal suspects, normally when identification attempts using fingerprints or DNA evidence have failed or are unsuitable. In cases where a photograph of an unknown suspect exists, a central photo archive will be used to determine identity.

Cognitec software should prove helpful in resolving missing persons cases as well as criminal identification

Bioscrypt enables biometric PC access

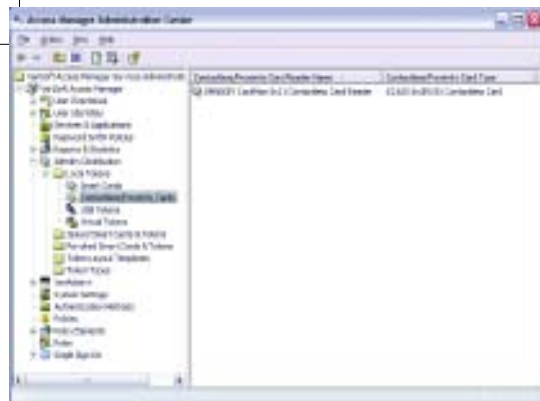
Bioscrypt has released the latest version of its VeriSoft Access Manager software, designed to comply with U.S. Federal Information Processing Standard 201 (FIPS 201) Personal Identity Verification (PIV) requirements. Under HSPD 12, the PIV program uses a smart card that contains two fingerprints to verify user authorization when accessing a federal government building or computer.

Among the new VeriSoft features is the ability to register PIV2 cards for network authentication as well as PIV2 card integration with all VeriSoft applications and services.

NEMA pursues security standards

NEMA, the trade association for the electrical manufacturing industry in the U.S., is embarking on a venture to develop a standard for homeland security systems that it hopes will eventually accelerate the development of a market for scanning, detection and security-related products.

The organization is forming a standards development committee to tie together a number of technologies that NEMA member companies already manufacture, including scanning equipment, physical access control, video, and intrusion and explosives detection. NEMA points out that while the market is already well supplied with these kinds of security technologies, standards that would allow them to interoperate 'out of the box' has yet to be developed. It's not a trivial matter, considering that the difficulty of establishing communications between the disparate systems used by various first responders after the 9/11 attacks was blamed for increasing their death toll. "Providing an environment in which there is a common language and a means of transmitting it to other locations is vital to the nation's national security interests," NEMA said in announcing the standards development committee.



VeriSoft now meets U.S. government requirements for logical and physical access

FlightVu

**aircraft video systems
for security, safety
and entertainment**



- Boeing Technical Offerability on Flight Deck Entry Video Security System
- CabinVu - 123 new cost effective cockpit door monitoring system fully compliant with EUROCAE ED -123
- FlightVu Witness - EFB compatibility, digital recording and full aircraft coverage
- CargoVu - monitoring of cargo bay to deter baggage theft, check for stowaways / terrorists and verification of smoke alarms
- FlightVu provides compliance with ICAO, ECAC, CAA standards, EUROCAE ED-123 and future mandates
- FlightVu certified for B737, B747, B757, B767, B777, DC-10, MD-80, F-100, A320 & A330
- Meets DO-160D, DO-178B



Europe: +44 (0)870 442 4520
USA: +1(770) 874 8750
Asia: +65 6256 4148
Email: adenquiry@ad-aero.com
www.flightvu.aero



USA: +1(407) 4384436
Europe: +44(0) 1276 609061
China: (86-10) 64560246
Email: adenquiry@aeisinc.com
www.aei.aero

U.S. Customs and Border Protection have always evaluated human response: in future that evaluation will be on a more scientific footing. Photo courtesy CBP



Face to Face

Behavioral observation hits its stride By Andrew Brooks

Take a crime, any crime – shoplifting, vandalism, assault, murder – and imagine for a moment that the need to prevent it from occurring, as opposed to apprehending and convicting after the fact, were increased a thousandfold. Imagine that even a single commission of the crime in question carried a price too high to even think of paying: the loss of hundreds or thousands of lives, the disintegration of day-to-day life, the shattering of global economic networks.

That, in a nutshell, is the challenge facing those charged with preventing terrorist attacks, in any venue and in any form. The task of preventing such cataclysmic attacks is so different from the traditional law-enforcement

approach of post-crime detention/conviction that a new, proactive model is called for.

So, at least, thought Rafi Ron when he was approached by Boston's Logan International Airport in the weeks following the 9/11 attacks. Security authorities were interested in techniques Ron had developed for training security staff to recognize suspicious behavior – a program he calls Behavior Pattern Recognition (BPR). Ron was security director of Israel's Ben-Gurion airport from 1997 to 2001 and he has built on his experience with Israeli behavior analysis techniques to develop BPR for use in the U.S. and elsewhere.

Israel is widely acknowledged as a leader in aviation security. In spite of longstanding involvement in conflicts in the region, and, more

recently, an unenviable status as a potential global terror target, Israeli's aviation experts – Ron prominently among them – have succeeded in architecting a system of technologies and procedures that has with very few exceptions exempted Israeli aviation from terror attacks at all levels. So why not just take what they've learned and apply it here?

In a nutshell, that's what Ron has done, with some adjustments for local conditions and cultures. As president and CEO of New Age Security Solutions, Ron has brought Behavior Pattern Recognition to four major U.S. international airports: Logan (his first customer), Miami, San Francisco and Minneapolis/St. Paul. These are only the ones that have adopted BPR

lock, stock and barrel. Others have adopted or are in the process of adopting elements of BPR on a smaller scale. Airports and aviation authorities in the U.K. have picked it up, as well as Hong Kong International Airport.

In a related development the U.S. Transportation Security Administration (TSA) has recently launched a program that will train state and local law enforcement officers to look for suspicious behavior among transportation professionals like truck and bus drivers. And the TSA is ramping up its own airport behavior recognition program, called SPOT (Screening Passengers by Observation Techniques).

But the strong and aggressive model of

passive, reactive mode to a proactive and – it's a loaded term of course – aggressive approach. They, and other airport employees who have received training, will actively look for suspicious signs anywhere in the airport, confident that they can at least narrow down the segment of the population that deserves further attention: longer observation or, if need be, "targeted questioning," where staff engage a passenger in apparently innocuous conversation to see if signs of nervousness increase or emerge.

"This kind of program is useable by a wide range of staff at an airport," says Norman Shanks principal partner of NSAI. "It works for the specialized security and law enforcement

what he was all about," Ron says. "She said that when she saw his English name on the pass she relaxed a bit, and she relaxed more when he answered her questions in a perfect English accent." Her intuition wasn't strong enough to overcome her self-doubt – something that training can correct by scientifically demonstrating that many intuitive observations are sound.

"Richard Reid was a notable success of behavior observation," echoes Norman Shanks. "He was identified twice by security staff as I understand it. On the first occasion he was properly referred to the police – who found nothing wrong with him. He was identified a second time, but because he had already been 'cleared' he was allowed to fly. This was a success in behavioral profiling: it was the subsequent stages that failed." (Fortunately, so too did Reid's attempt to blow up the airliner in mid-flight.)

Some intuitions are sound: others less so. The fact that the flight attendant was put at ease by Reid's racial profile points up one weakness of intuitive methods that behavioral observation must strive to overcome. Some instincts aren't merely politically incorrect: they can be utterly counterproductive in terms of security, a point often lost on some critics who see observational techniques as inherently racist. (Compounding the confusion is the fact that behavioral analysis is often referred to as "behavioral profiling," which conflates it in the minds of many with racial profiling.)

"One thing we've tried to overcome in developing the program is prejudice," Ron says. "The program is 100 percent focused on avoiding racial profiling." This isn't just a matter of cultural sensitivity. Ron notes that Ben Gurion was attacked twice (neither attack came during his tenure as security director, he adds): by Japanese terrorists in 1972 and by German attackers in 1981. A racially based profiling system in that context would have been of no help since it would probably not have emphasized Europeans or Asians as potential threats.

"When we started four years ago in the U.S. most people still believed that technology would provide the silver bullet," Ron says. "This is a cultural tendency here, to look for technology to solve a problem." But after the discovery of the alleged 'liquid bomber' plot in London in August, security agencies are realizing that a broader approach that uses technology but doesn't depend on it exclusively makes more sense. This, Ron believes, is where BPR comes in, and it helps to explain the program's new popularity. "This is not a checkpoint concept – this is a full-airport concept." ■

"This is not a checkpoint concept – this is a full-airport concept"

Rafi Ron, New Age Security Solutions

behavior analysis practiced in Israel airports simply can't be adopted in the U.S. – or pretty much anywhere outside Israel. For one thing the Israeli model involves interviewing every single passenger, which alone rules out its use in the high-volume U.S. international airports like Los Angeles, Atlanta and Dallas/Fort Worth, which have around ten times the traffic of Ben-Gurion. Ron also notes that cultural and legal issues preclude the use of some of the more aggressive and politically incorrect Israeli techniques in the U.S.

Another weakness of the Israeli system – or a feature that would become a weakness if the system were transplanted wholesale – is that, since it's based on interviewing literally every passenger, it doesn't involve training airport staff at any level to spots signs of suspicious behavior among the raw airport population: those signs are picked up in the mandatory interview. Because BPR can involve any and all airport employees – there are some 35,000 involved at Miami International – the ability to pick up on behavioral clues must be propagated out to a broader base and in a wider variety of forms and intensities.

Paradigm shift

As Ron explains it, the program really hits its stride in changing the attitudes of those who participate, at any level. Law enforcement and security staff, who normally tend to think of themselves as practicing the "apprehend and convict" model referred to earlier, switch from



BPR training at Miami International Airport: all 35,000 employees are involved

staff right through to the people who work with the public on the concourse floor." Of course the training is tailored according to the depth of contact involved: security staff are trained in exhaustive interview techniques and targeted questioning, while non-specialist staff – who after all have other things to do – get only a few hours' training on some of the more obvious signs to look for.

But at any level the mere fact that an employee has received training backs up their natural human intuition, gives them new clues to look for, and can make the difference between investigating further and deciding that one's own suspicions are groundless.

Ron cites the example of Richard Reid, the unsuccessful "shoe bomber" – a case that inevitably arises in any discussion of behavioral observation. An experienced flight attendant who had been greeting passengers at the door to the aircraft later told authorities that she became suspicious as she saw Reid walking toward her. "So she decided to ask him for his boarding pass and ask him a few questions to get a sense of

Southern Cone

An insider's view of port security in Latin America

By Andrew Brooks

Francisco Piccirillo is principal surveyor and country manager in Argentina for Lloyd's Register, an independent global risk management organization that covers a range of industry sectors, including maritime transportation. Piccirillo is based in Buenos Aires, but covers several other countries in Latin America, including Paraguay, Uruguay and – when we spoke with him –

Venezuela, but his knowledge of the maritime sector in this part of the world is comprehensive and extends throughout South America.

For our question and answer session with Mr. Piccirillo, we began by asking about the state of port security in his home base of Argentina, and how it compared to that of other countries in the region.

PICCIRILLO: Argentina has more than 3000 kilometers of seacoast, and there are many ports in the south part of the country. Buenos Aires is the only container terminal port, and it also handles some passenger traffic, and some general cargo.

In all the country's ports, security has been improved – Buenos Aires most importantly, and Rosario [190 miles from Buenos Aires on the Parana River] but also the upriver ports. The most important commerce is through the upriver ports, which handle about 90 percent of Argentina's grain exports. In the south we have tanker ports in Bahia Blanca and Comodoro Rivadavia, where mooring is done by monobuoy, which means the tanker doesn't actually enter the port but is connected by pipeline to the shore.

Port security is in good shape in Argentina because it's managed by the local port authorities. Practically all the installations have received security certification, especially the container terminals: they have container scanners and other systems to improve port security. Practically all the installations at upriver ports are managed by private companies and security levels meet international standards: to enter and leave port you have to present authorization.

Part of the reason for the good security is the presence of Prefectura Naval Argentina [PNA, founded in 1810], which works similarly to the U.S. Coast Guard. They use the same methods and operate as a very important local force. They employ 14000 people, a big number to have involved in port security. It's a very professional force with its own vessels and aircraft to monitor the coast. Compare this with the situation in some other Latin American countries where the local port authority is a branch of the navy, not a special independent body.

In Chile port security has also been improved very much. It's managed by the Chilean Navy, but very strictly. The ports are well controlled, and the Navy is very professional too.

I believe that the weak partner in South America when it comes to port security is Brazil. You still have piracy in ports like Rio de Janeiro and Santos [the largest port in Latin America, just outside Sao Paulo]. The statistics bear this out. Many anchored ships are attacked at night, and the navy is less efficient at controlling security. I lived for three years in Rio, and security in the port there is very weak.

The problem is that in Brazil all port security and all port state control is performed by the navy, and they have very few resources to

control all the port activity. They're more involved in what you'd call police-type activities. That's a big problem that Brazil has with port security control. There are so many vessels going to the large ports of Rio and Sao Paulo that they have to wait, and they prefer to wait far out at sea to avoid attacks. In private terminals security does tend to be better, and I believe that Rio de Janeiro is now in discussions with the Brazilian navy with a view to establishing something like the Coast Guard: a body of people fully dedicated to port state control and port security.

The problem with a port like Rio is that it's in a bay, which is very big and is surrounded by very poor people who have every motive to attack ships at night. Rio especially is a very dangerous place to be anchored, but security is bad enough throughout Brazil that many masters close up their vessels when they arrive.

Right now I've been put in charge of Venezuela too. I can't say too much about the situation there, as so far I've only spent a few days there, but in some ports the security is good. I saw it at oil terminals, which are very safe, which have a lot of security control. Beyond that I can't say what's happening there in terms of port security, but more generally Caracas is

“I believe that the weak partner in South America when it comes to port security is Brazil.”



very unsafe, and the country as a whole is unsafe: there are a lot of political problems right now. In terms of personal safety it's dangerous to walk at night, especially if you're a foreigner. Compare that with Buenos Aires, where you can see lots of people walking at night, where you feel more comfortable and secure personally. Sao Paulo and Rio are still quite unsafe from that point of view also. In fact South America generally is not a good place from the security point of view. We have advantages and attractions but security is not one of them.

SENTINEL: What about the pace of port privatization, and its effect on security?

PICCIRILLO: In Argentina the last government put all ports under the management of private companies. That's the main reason security has improved so much: the private companies invested lot of money in port development and most of the security measures are certified by local authorities. Also a lot of terminals are certified to ISO 9000 standards. The port system in Argentina has improved a lot in the last 20 years. The same is true in Chile.

In Brazil, I believe all the private terminals have also improved. But in ports that are still

state-owned the situation is not very good right now.

SENTINEL: In what other ways does increased port investment improve security?

PICCIRILLO: Port operators invest money to be more efficient in the terminal. The terminal in Buenos Aires is now equipped with modern cranes. This means that ships stay in the port for only a few hours, like what you find in Europe. If you improve the efficiency of the terminal you drastically reduce the cost of operation: because the time a ship spends in port is reduced, you increase profit.

Also the grain terminals are now loading much larger loads – two to three thousand tons a load. In 20 hours they can load a Panamax vessel, efficiency has improved so much. Of course that shortens the vessel's stay in port, which isn't necessarily good as far as the crewmembers are concerned. But that's the reality now.

SENTINEL: Does a country like Argentina, where port security has improved, notice a boost in trade as a result?

PICCIRILLO: Yes. At least you notice this for

cruise passengers. Last year more than 100 cruise ships went to Argentina. Tourism is improving generally. When cruise ships start noticing better security that's an important sign, because if they have any doubts about it at all they just stay away, they call somewhere else. Cruise ship traffic has improved very much in the last five years in Argentina. This is a good sign because it means people like visiting the country.

SENTINEL: To what degree have countries in Latin America bought into concepts like the Container Security Initiative and the ISPS Code? Are they serious about trying to follow these standards?

PICCIRILLO: All Argentinian flagships are certified under ISPS. Some local coastal ships too, small ships under 55 tons, even though it's not mandatory. Many companies have done so. There is pressure to certify because in so many terminals the vessel can't be operated if it's not certified. If a terminal has a security certification they also request that ships operating in that terminal do also. That means that local operating ships are pressed to certify in order to operate in the terminal. ■



The Long ARM

CSI "offshores"
port security

By Andrew Brooks

The Container Security Initiative was created by U.S. Customs Service, the forerunner of U.S. Customs and Border Protection (CBP) in the months immediately after the 9/11 attacks. The main objective is to target the threat represented by freight containers, of which over 100 million are shipped annually around the globe. In cooperation with customs administrations around the world (28 have joined so far), CSI assigns teams of CBP officers to work in overseas ports to inspect U.S.-bound cargoes before they leave their ports of origin.

The four main elements of CSI include:

- Identification of high-risk containers.
- Pre-departure screening and evaluation of containers.
- Deployment of technology so that these processes slow trade as little as possible.
- Development of 'smart container' security systems that can detect attempts to tamper with containers in transit.

After it was announced in January 2002, CSI was initially implemented in the 20 international ports shipping the greatest cargo volumes to the U.S. The work was completed by September 2003, at which time CBP announced Phase II: the expansion to strategic ports beyond the initial 20. As of September 28, some 50 international ports were listed on the CBP web site as meeting CSI criteria, most of them in Europe and Asia.

The World Customs Organization (WCO),

European Union and the G8 have promoted the expansion of CSI by adopting resolutions that endorse its security profile. In addition, the program is reciprocal, and allows for participating foreign nations to station their customs staff at U.S. ports to prescreen cargoes headed for their own countries. So far Canada and Jamaica have availed themselves of this opportunity.

Global trade stands to benefit with the adoption of CSI, and has already done so. For instance, ports close to the Malacca Strait, including Singapore and Malaysia's Port Klang and Tanjung Pelepas, have signed on, and piracy in the Strait has declined in recent months (although many more factors besides port security are involved).

By the end of 2007, CBP hopes to expand CSI to 58 global ports, which would cover about 85 percent of goods imported to the U.S. But however desirable, the program is hardly a panacea. Ports in developed countries, including the U.S. itself, still have security loopholes, with governments often engaged in fierce political battles over port security funding. In Australia, the chairwoman of the Labor Party's Transport and Maritime Security Task Force recently warned that Australia's Newcastle port, north of Sydney, could easily become a terror target, with cargoes of ammonium nitrate – used as a fertilizer but also as in improvised explosive devices (IEDs) – being one obvious potential target.

"These ships could be floating bombs,"

Anna Burke said. "I don't want to sound alarmist, but it is a reality. We've got security briefings from various individuals saying that Osama Bin Laden may have ships under his control. Whether that is true or not, I don't know, but we have had those reports."

The debate is vigorous in CSI's homeland also. At the end of September, the U.S. Department of Homeland Security announced the distribution of some US\$168 million in previously appropriated funding for port security projects. At the same time the U.S. Congress finally passed a bill that basically guarantees annual federal funding for port security (the SAFE Port Act).

While the attention and funding is welcome, and goes some way toward combating the widely held view that aviation security accounts for a hugely disproportionate share of resources, the money still falls well short of the American Association of Port Authorities (AAPA) recommended US\$400 million. The AAPA says that figure is based on U.S. Coast Guard estimates of port security requirements.

"It's important that the next annual spending bill provide the full \$400 million for the Port Security Grant program to help ports pay to install TWIC card readers and other terrorism prevention programs at their facilities," said Kurt Nagle, president and CEO of AAPA. "AAPA will continue to work with members of Congress to achieve this funding level." ■



By Roma Ihnatowycz

Merging IT with Security

ISC East partners with a leading information technology event to offer delegates the best of both worlds

When this year's ISC East Expo takes place Oct. 24-25 in New York, it won't be the only security event stealing the show at the celebrated Jacob Javits Convention Center. Taking place alongside it will be InfoSecurity 2006, the largest IT security exhibition on the eastern U.S. seaboard. Delegates registered for either event will be able to freely attend both trade floors.

For Reed Exhibitions, the organizer of the two events, the decision to converge the shows was a logical one and is about more than just boosting attendance. "What we've been seeing within the ISC and physical security industry is a very rapid convergence with the IT community based upon the advancement of the technology," says Dean Russo, group vice-president of Reed Exhibitions. "It was the right time to

put these shows together because basically that's the way the industry is going."

The move also marks one of many new developments at ISC East since the security expo returned to New York in 2004, after a two-year stint in Washington, DC. The return to the Big Apple is proving a wise move, with attendance figures steadily growing. This year, organizers are expecting about 10,000 attendees and 400 exhibitors – marking a 12-15 increase in vendor numbers from last year. "It's the [result] of many vendors coming back, as well as growing the even in new product segments," says Russo.

One of these new product segments is a "show within a show" called Urban Security, a dedicated floor area for companies representing products and services directed toward municipal and state security applications. A

similar section proved popular at ISC East's partner exhibition ISC West held in Las Vegas last April. "It works well with the east coast event because we get very strong attendance from city and state government buyers from New York and surrounding states," says Russo.

Also new at this year's ISC East is a special all-day training program for physical security dealers and integrators called the IP Institute. "Basically they go through an intense training program that teaches them the applications and how to design and install physical security systems that work over IP networks," says Russo.

The two-day security event will also have numerous additional sessions and seminars, on topics ranging from applying smartcards and biometrics to access control and new technologies in digital video storage. There will also be a keynote address by Mark Mereshon, assistant director of the FBI for New York City, touching on issues affecting both the security and IT industries. ■

ISC EAST Exhibitor Showcase

Cutting edge fire protection technology

Fire-Lite Alarms will showcase its MS-9200UDLS addressable control panel. Combining the capabilities of Fire Alarm Control Panel (FACP) and Digital Alarm Communicator/Transmitter (DACT) into one circuit board, the MS-9200UDLS offers a compact, cost-effective design. The MS-9200UDLS features LiteSpeed, a Signaling Line Circuit (SLC) protocol that simultaneously polls ten devices at a time, polling each several times to receive new data. This improvement allows a fully loaded panel to report an incident and activate the notification circuits in less than ten seconds.



Fire-Lite's MS9200UD addressable fire alarm control communicator

BOOTH 1708

Conquering access control

CDV Americas Ltd. launches the new 4.0 version of its Centaur Access Control System. This PC-based system is mature, robust, stable, flexible and scalable. It can support up to 2048 doors per site and up to 64 sites using the Enterprise Edition. Its reliability, ease of use and expansion capabilities allow companies to handle extreme access control challenges. CDV Americas will also present its keypads, RF transmitters, Mifare devices, photobeams, electric door strikes and electromagnetic locks at ISC East.

BOOTH 1945

Digital Identification Solutions card printers

Digital Identification Solutions introduces the *EDISecure* Professional Line that includes the XID570i, the XID580i and the high-production XID590i re-transfer card printers, plus the DCP360i direct card printer. This entire line includes options for in-line lamination, Ethernet connectivity, contact chip encoding and contactless encoder/readers, including MiFare, DESFire, Prox and iCLASS. The XID5xxi series is fully FIPS 201 compliant when combined with other *EDISecure* components, such as the Inline Lamination Unit (ILU). To complement the Professional Line, the company also has a new Value Line of direct card printers, which includes the sub-compact DCP100, the single-side DCP240 and the dual-side DCP340.

BOOTH 2251



The DIS line of card printers

One-stop shopping

Boyle & Chase's motto is "We stock it so you don't have to." At this year's ISC East Expo, delegates will learn why this is more than just a catchphrase for the distribution company. Boyle & Chase will present various products

from its many product lines, which include ACSI, Alarm Controls, Baldwin, Burns, Codelocks, Doromatic, Omnia, IEI, Folger Adams, Glynn Johnson, Hager, HES, Ives, Kaba Ilco, LCN, Locknetics, MS Sedco, RCI, Schlage, Secura-Key, Visonic, and Von Duprin. The

company provides every possible design, function and finish, and is ready to ship out the same day. It offers on-line stock checks, blind drop shipments and faxed or e-mailed invoices with pricing and tracking information.

BOOTH 1756

A schematic showing the workings of Absolute's Computrace data protection agent

REMOTE COMPUTER

Location, user, hardware and software data is transmitted daily without user input or knowledge (client-initiated, TCP-based and encrypted).



ABSOLUTE MONITORING CENTER
Information is confidentially stored in our secure offsite facility.



IT ADMINISTRATOR

Responsible for managing remote/mobile computer assets and for setting up Data Delete.



ONLINE CUSTOMER CENTER

Absolute Website: Log into Customer Center to track and manage your PC assets..



Tracking online computers

Absolute Software presents Computrace Data Protection, a protection system that tracks online computers with a small, virtually undetectable software agent called the Computrace Agent. This agent is embedded in the BIOS, or firmware, of most Dell, Fujitsu, Gateway, HP and Lenovo notebook models. Computrace Data Protection allows customers to track computers and remotely wipe sensitive data, such as sensitive files or directories, if a computer is lost, stolen or nearing the end of its lifecycle. Computrace Data Protection provides two main benefits – Information Technology (IT) asset management and remote data deletion.

BOOTH 2378

ISC EAST Exhibitor Showcase

Open integration platform

Entelec Control Systems offers their Sky-Walker Solution integration platform that manages buildings, tunnels, airports, subway and railroad stations, and any structural constructions. The Sky-Walker Solution incorporates all the underlying techniques and systems needed to manage different computer-based building automation and control systems. It presents a uniform graphical interface to the end user for the control of systems like fire detection, intrusion, CCTV, access control, public address, HVAC, lighting, electricity and others. Communication with the various systems is accomplished by means of drivers. Any intelligent hardware can be integrated as long as it provides a communication port and a communication protocol.

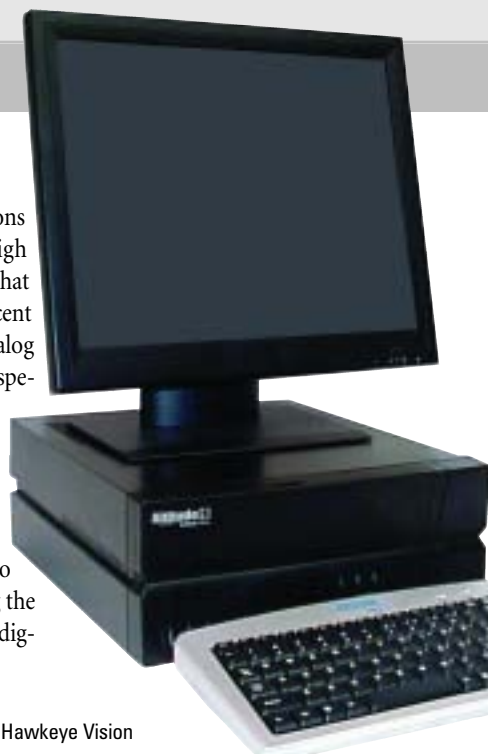
BOOTH 1872

High definition, high-res video

Hawkeye Vision, a division of Advanced Imaging Solutions Inc., presents its recently launched Altitude High Definition (HD), a digital video surveillance system that captures and records high definition video at 300 percent to 400 percent greater resolution than a standard analog camera. Customers requiring higher picture quality in specific areas can simply exchange an existing analog camera with Altitude HD without rewiring their existing analog infrastructure. Altitude HD is capable of supporting up to nine High Definition video inputs per system. It features outstanding dynamic range and unique contrast mapping technologies to record HD video under low-light and strong backlight conditions. Using the picture quality of the CoVi EVQ-1000, the Altitude HD digital video solution can capture events in fine detail.

BOOTH 2341

The nerve center of the Altitude HD surveillance system from Hawkeye Vision



Avigilon's complete line of performance surveillance systems



Leveraging digital capabilities

Avigilon will showcase its 11 megapixel surveillance camera with digital PTZ. Delivering resolution equivalent to 36 conventional surveillance cameras, the cameras provide image quality and flexibility for monitoring large public spaces. While conventional PTZ Systems are unable to monitor the surrounding scene when an operator zooms in on an image to get more detail, Avigilon's unit records the entire scene even when zoomed into a particular detail. It has full PTZ capabilities on recorded surveillance footage as well, allowing details to be extracted after an incident has occurred.

Offering high-sensitivity Gigabit Ethernet cameras, ranging in resolution from VGA to 11 megapixels, and high-capacity recorders that capture and preserve surveillance evidence using lossless compression, the Avigilon Performance Surveillance System was designed to deliver maximum imaging performance.

BOOTH 1457



Fencing solutions

Swan Fence, a specialist in SECURITY mini-mesh chain link fencing, will be on hand to highlight its various different fencing options. Swan Fence weaves an anti-climb diamond of 1/4", 3/8" to 1/2", 5/8", 3/4", 1" and up to 2" mesh. It provides a variety of 12 stock colors of PVC Extruded Bonded chain link, as well as six stock colors of PVC Fused Bonded chain link. The company will also match any color for specialized jobs, and stocks stainless steel, aluminum, aluminized and galvanized wire.

BOOTH 1980

Surveying hazardous sites

Extreme CCTV International has two new products for this ISC East. The Moondance ExD is an explosion-protected, vandal-proof PTZ speed dome designed for surveillance in hazardous locations. Its robust machined metal ball design makes it one of the toughest, most versatile explosion-protected PTZ cameras available. Moondance features 320-degree tilt to capture surveillance images from both directly above and below the camera, thus eliminating the blind spots typical with conventional PTZ cameras.

Also from Extreme CCTV is the WZ20, which brings together 550 TVL high-resolution LXR imaging, the latest advances in mechanical filter CCD technology and dealer-friendly design. The camera delivers 150 feet of high performance night vision.

BOOTH 1931

Extreme CCTV's Moondance ExD PTZ speed dome





Elk Products offers complete control

Elk Products, Inc. touts M1 Gold as the central nervous system for a home or business. M1 Gold is a cross-platform control that networks with other industry-standard systems to become the brain to control virtually everything electrical in a home or business. It is a security, automation and access control that interfaces well with controls for lighting, HVAC, CCTV, entertainment and other electrical devices, providing the user with complete control through keypads, touchscreens, software for PCs and PDAs, telephones, keyfobs or proximity fobs/cards. Telephones and internet browsers provide remote control and remote monitoring for the system with the proper passwords.

BOOTH 2151

Rainbow CCTV delivers adaptive illumination

Rainbow CCTV launches a new variable infra-red illuminator, providing customers with the opportunity to use an illuminator like a varifocal lens. The new illuminator is the first to provide adaptive illumination that can be adjusted to match a field of view. A single unit can provide up to 180 degrees of view.

BOOTH 1448

M1 Gold from Elk Products integrates security systems and devices



The BL-229 from Automatic Control Systems

What's new in rising barriers

Automatic Control Systems highlights the BL-229, a rising barrier designed for flexible application and operation. Field modifications are quick and easy, making it a flexible vehicular security solution. Boom (arm) lengths can be changed without difficult mechanical assemblies and with only a slight variability in the unit's high-speed one-second opening, and the BL-229 can easily be adapted to any length arm from seven to 20 feet. As well, switching the gate's orientation from left to right will not require additional parts or laborious assembly – the easy switch has been calculated into the design.

BOOTH 1655

Enhancing IT convergence

Cypress Computer Systems re-introduces its network enabled door interface (DPX-7200). The company recently added new functionality and security to the IT capabilities of its door and gate security controls. It continues to design, develop and market further enhancements to its award-winning Suprex Technology including "network door" offerings. This open architecture design adds IT capability to virtually any manufacturer's door hardware and card readers and is platform and access control system independent.

BOOTH 2003

High-resolution IP recording cameras

German network camera manufacturer Mobotix introduces its new M22M camera, which it says displays improved image quality and considerably greater performance. The new camera has improved 960-line, high-resolution sensors, and a Standard Ethernet connection that enables the use of common network components such as fiber, copper and

wireless networking (WLAN). Intelligent recording technology reduces required storage, and an event-controlled image rate minimizes storage costs. As well, no additional power or heating is required and back-up power requirements are reduced by eight times thanks to low power consumption.

BOOTH 2028



The M22M wallmount camera from Mobotix

High-level tailgating detection

Boon Edam Tomsed is presenting a number of products at this year's ISC East event, including its Speedlane 996 Series. Offering one of the highest levels of tailgating detection available in optical barrier lanes, the Speedlane 996-BPL has angel wing biparting glass leaves with standard lane widths of 22" or 36" for ADA compliance. The units allow bi-directional traffic in one direction at a time, and each direction can be independently controlled. Compatible with any access control system, the Speedlane 996-BPL accommodates a wide variety of operating modes for maximum flexibility. Standard cover is 1" thick solid surface, and optional metal, marble or granite covers are available. Also, available only with the Speedlane 996 Series is the unique PathMinder 96-beam matrix, which can reliably and accurately detect tailgating within 1/4", including side-by-side traffic.

BOOTH 2143

Boon Edam Tomsed's Speedlane 996



Event round-up

Industry conferences, seminars, exhibitions and symposiums

2006

OCTOBER

- **CIHSPS 2006 – IEEE International Conference on Computational Intelligence for Homeland Security and Personal Safety.** Organized by IEEE, Oct. 16-17, Alexandria, VA. <http://cihsps.dti.unimi.it/cihsps2006/Venue/Venue.html>
- **AVSEC World 2006.** Organized by IATA, Oct. 18-20, Sydney, Australia. www.iata.org/events/avsec2006.htm
- **Biometrics 2006.** Organized by Biometric Technology Today, Oct. 18-20, London, U.K. www.biometrics.elsevier.com
- **Summit for Disaster Management Planning.** Organized by Environmental Tectonics Corp., Oct. 23, Philadelphia, PA. www.readinessnow.org
- **2nd Annual Border Management Summit.** Organized by IDGA, Oct. 23-25, Washington, DC. www.bordermanagementsummit.com
- **ISC East 2006.** Organized by Reed Exhibitions, Oct. 24-25, New York. www.isceast.com
- **RISCON: Security & Safety Trade Expo 2006.** Organized by Tokyo Big Sight Inc., Oct. 24-26, Tokyo, Japan. www.kikikanri.biz
- **Security China 2006.** Organized by E.J. Krause, Oct. 30 – Nov. 2, Beijing.

NOVEMBER

- **Cartes 2006.** Organized by Expositum, Nov. 7-9, Paris. www.cartes.com

- **Securing New Ground – The Business of Security.** Organized by Securing New Ground LLC, Nov. 15-16, New York, NY. www.securingnewground.com
- **Global Border Security Conference & Expo.** Organized by E.J. Krause, Nov. 27-28, San Antonio, TX. www.globalbordersecurity.com
- **International Aviation Security Technology Symposium.** Organized by Safe Skies

2007

FEBRUARY

- **RSA Conference 2007.** Organized by RSA Security Inc., Feb. 5-9, San Francisco, CA. <http://2007.rsaconference.com/US>
- **IV International Congress for Victims of Terrorism.** Organized by National Memorial Institute for the Prevention of Terrorism, Feb. 20-21, Oklahoma City, OK. www.mipt.org/Congress/
- **Fourth Annual Worldwide Security Conference.** Organized by EastWest Institute, Feb. 20-22, Brussels, Belgium. <http://wsc.ewi.info>

APRIL

- **Biometric Technology for Human Identification IV**(part of SPIE International Defense and Security Symposium). Organized by International Society for Optical Engineering, April 9-13, Orlando, FL. <http://iris.usc.edu>

Alliance, Nov. 27 – Dec. 1, Washington, DC. www.sskies.org/symposium.htm

- **ID World International Congress 2006.** Organized by Wise Media, Nov. 28-30, Milan. www.idworldonline.com
- **The Gartner Identity & Access Management Summit.** Organized by Gartner Group, Nov. 29 – Dec. 1, Las Vegas, NV. www.gartner.com

DECEMBER

- **APTS Europe 2006** (co-located with Counter Terror World, Event & Venue Security and Infrastructure Security). Organized by International Business Events, Dec. 5-6, London, U.K. <http://www.aptsexpo.com/ME/>
- **Advanced Identification Systems with Biometrics & Security.** Organized by Intertech, Dec. 6-8, Washington, DC. www.intertechusa.com

MAY

- **Global Border Security Conference and Exposition.** Organized by E.J. Krause, May 9-10, San Antonio, TX. www.globalbordersecurity.com

JULY

- **92nd International Educational Conference – The International Association of Identification (IAI).** Organized by IAI, July 22-27, San Diego, CA. www.theiai.org/conference/2007
- **Force Protection Equipment Demonstration (FPED) VI.** Organized by U.S. Army Product Manager, Force Protection Systems (PM-FPS), Aug. 14-16, Stafford, VA. www.fped5.org
- **ICB 2007 – International Conference on Biometrics.** August 27-29, Seoul, South Korea.

Is Your Security Staff ASIS Board Certified?

For employers, the best employee is the proven employee. ASIS certification reduces the risk of hiring because it provides independent validation of an individual's skill level, commitment, and continuing education.

Credentialed security employees add immediate value with their proven expertise and knowledge of best practices. A certified staff delivers bottom-line benefits by strengthening performance and documenting conformance to high industry standards.

Stay competitive with a security staff that's ASIS board certified.



CERTIFIED PROTECTION PROFESSIONAL

Acknowledged as the security profession's highest recognition. The CPP identifies security management practitioners who have demonstrated advanced knowledge in eight major areas of security.



PROFESSIONAL CERTIFIED INVESTIGATOR

A specialty certification in security investigations. The PCI is evidence of proven investigative skills, including gathering intelligence, conducting undercover investigations, and managing cases.



PHYSICAL SECURITY PROFESSIONAL

A specialty certification in physical security. The PSP demonstrates expertise in operating and maintaining physical protection systems, conducting threat assessments, and using security forces.

Learn more today! Go to www.asisonline.org or call 703-519-6200.

**ACCEPTED AS THE STANDARD.
WORLDWIDE.**



Efficient Checkpoint Screening

Rapiscan Systems has provided comprehensive security screening solutions in more than 60,000 applications in over 50 countries. Our expansive product portfolio and professional, knowledgeable consultants will help find the perfect security solution for your needs.



Rapiscan[®]
systems

An OSI Systems Company

ONE COMPANY - TOTAL SECURITY

www.rapiscansystems.com

BAGGAGE AND PARCEL INSPECTION / CARGO AND VEHICLE INSPECTION / HOLD BAGGAGE SCREENING / PEOPLE SCREENING