Biometrics and the global transportation infrastructure

Enhancing security and improving operational efficiency through the implementation of enhanced identification technologies

Since 9/11, the transportation industry has been under near microscopic scrutiny. Intense efforts by governments, international organisations and commercial interests worldwide have focused on identifying processes, programs and technologies that will prevent the occurrence of another terrorist attack. To date, these efforts have focused on the "front end" of the air travel sector - passengers, baggage, airport employees and crew. While these efforts have provided, and will continue to provide, innovations that improve security around the globe and while it would be less than prudent not to pursue such an intensified course of action, vulnerabilities in the transportation infrastructure are hardly limited to this sector of the industry. It is, in fact, the "back end" of the global transportation infrastructure which encompasses cargo, shipping, logistics and warehousing which is far more susceptible to attack, has the potential to create much greater human and economic harm and provides an even more complex security problem to solve.

Ever increasing reliance on worldwide commerce is pushing the global transportation infrastructure to its limits. The need to accelerate and streamline the flow of cargo has exacerbated security risks across what has become an increasingly complex web of interconnected transportation services. Vulnerabilities exist throughout this web, particularly at "chokepoints" - ports, borders and transportation hubs – which provide crucial links in this global network. As we learned quite painfully on 9/11, one devastating incident in the transportation sector can significantly impact worldwide commerce even when no damage occurs at a transportation facility. One cargo-related incident at key chokepoint could wreak havoc on the transportation infrastructure bringing global commerce to a virtual standstill.

Transportation related security risks

Governments and international organisations are now keenly focused on evaluating

transportation related security risks. Many of these initiatives require the evaluation or integration of biometrics to authenticate the identities of individuals with access to critical cargo, secure areas of transportation facilities and associated information technology systems. This should provide a tremendous impetus for widespread biometrics adoption throughout the cargo transportation sector. Though biometrics alone cannot fully address these vulnerabilities, biometrics integrated into sophisticated security systems can up the security ante making it much more difficult for perpetrators of terrorism, sabotage or theft, while providing the intelligence community more time to uncover conspiracies and prevent disaster before it occurs.

There is considerable debate within the transportation, security and biometrics industries regarding the development of these complex security systems. Both proponents and critics of the biometrics technologies indicate high levels of concern regarding the development and management of centralised government or commercial databases, ownership, operation and maintenance of the necessary information technology infrastructure and funding sources for these new systems. Regardless of the obstacles, consensus among forward-thinking industry leaders is that the global commerce infrastructure will evolve in a way that addresses twenty-first century business security threats and biometrics will play a significant role in this evolution.

Advantages of biometrics

Process improvement is key to the mainstream adoption of emerging technologies. When faced with serious business-process deficiencies and technology solutions proven to address these deficiencies, mainstream adopters integrate new technologies into their existing infrastructure. Post 9/11 security concerns have forced transportation providers to look more closely at their vulnerabilities and focus substantial resources on assessing and reducing risk. However, ultimately it is process improvement - cost reduction, productivity increases and improved customer service - that will drive transportation companies to aggressively adopt new technologies, including biometrics. This is particularly true as the dynamics within the highly volatile transportation marketplace require continual process improvement and related cost reductions for market players to stay competitive. These dynamics include on-going industry de-regulation and re-regulation, the acceleration of global commerce, the unprecedented expectation of instantaneous worldwide communication, intense competition among and between transportation sectors, low operating margins and the opposing forces of fragmentation and consolidation in certain industrial sectors.

Case studies

The adoption of biometrics technologies for cargo transportation applications has been in process for several years. The biometrics based projects profiled in the following case studies - with the exception of the concept piece for the U.S./Canadian border crossing - were well underway long before 9/11. And security enhancement was only part of the motivation for choosing biometrics. Equal, or in some cases greater, emphasis was placed on the potential for increased operational efficiency gained through expediting the movement of cargo and reducing paperwork and document processing.

Secure access: marine-to-truck transfer at Rotterdam seaport

Rotterdam, the world's largest seaport, handles more than three hundred million tons of freight each year and accounts for forty percent of all European cargo. Rotterdam is the central hub for European commerce. Faced with the increasing demands of global commerce and reliance on inter-modal cargo transfers throughout the freight distribution chain, Rotterdam has pushed its seaport to the forefront of modernisation. One part of this modernisation process has centred around the deployment of a hand-recognition system to control truck driver access to the port. The system, which was installed in June 1999, expedites the movement of cargo from marine vessels to trucks, verifies the identities of "known" or trusted drivers and provides a detailed electronic audit trail. Drivers access the system's hand recognition reader via their vehicle windows as they pass through the facility control gate. Their identities are verified against the template stored on a radio frequency activated smart card. The system serves more than six thousand truck drivers and has successfully completed well in excess of three million transactions.

Secure access: rail-to-truck transfer - Canadian National Railway

Canadian National Railway (CNR), the fifth largest railroad in North America, is integrating fingerscan biometrics into its Speedgate control system. The Speedgate system was designed to monitor and expedite commercial truck access to CNR's inter-modal transfer facilities located throughout North America. Speedgate uses Optical Character Recognition (OCR) surveillance to identify vehicles by reading license plates, container numbers and company names and logos printed on trucks. Electronic bills of lading - the documents describing shipment contents - are activated as the containers are recognised by the system. Fingerscan biometrics were added to the Speedgate system to speed driver authentication at the gate – previously managed by a guard - and to link cargo containers to driver identity. This system improves traffic flow through intermodal facilities, reduces theft and fraud, creates an audit trail for all transactions throughout the facility and improves operational efficiencies. Five hundred drivers were enrolled in the initial pilot in Edmonton. Total enrolment when the Chicago, Montreal and Toronto facilities are fully operational is expected to climb to two thousand. Drivers need only enrol once to access the system at any of the locations.

Logical access: rail car release - Union Pacific Railroad

Union Pacific, the largest freight railroad in North America, has integrated voice recogni-

Table 1 - Biometrics in transportation – case studies

Locations	Company/ Sponsor	Application	Biometric	Vendor/Solution Provider	Status
Rotterdam	Rotterdam Seaport	Secure Access – Commercial Truckers	Hand	Recognition Systems	Deployment
Edmonton, Chicago, Toronto, Montreal	Canadian National Rail	Secure Access - Commercial Truckers	Finger	SAIC	Deployment
St. Louis	Union Pacific Railroad	Logical Access – Rail Car Release	Voice	Speechworks	Deployment
Canada/US Border	InterVISTAS	Border Crossing - Commercial Vehicles	TBD	unknown	Concept/Strategy
Chicago	FAA, ATA, Sate of Illinois	Logical Access – Cargo Supply Chain	Finger	SecureCom	Pilot

Problem	Conventional Solution	Issues	Biometrics Solution
Theft - High Value Cargo	Inventory counts, restricted and secure access, surveillance, employee background checks, movement sensors	Relatively easy to breach	Identity Confirmation, Watch list, Vehicle/Facility Access, Logical Access
Contamination – Agricultural, Food, Pharmaceutical	Restricted and secure access, surveillance	Detection of tampering or contamination	Identity Confirmation, Watch list, Vehicle/Facility Access, Logical Access
Hijacking – Hazardous Material	Restricted access, surveillance, "known" shipper	Containment of material	Identity Confirmation, Watch list, Vehicle/Facility Access, Logical Access
Bombs - Conventional, Radiation, Nuclear	Restricted access, surveillance, "known" shipper	Originator identification, controlled access/tampering, detection	Identity Confirmation, Watch list, Vehicle/Facility Access, Logical Access
Smuggling - Drugs, Weapons, Explosives	Targeted security checks	Originator identification, controlled access/tampering, detection. Solutions ineffective to date I.e. US War on Drugs	Identity Confirmation, Watch list, Vehicle/Facility Access, Logical Access
Audit Trails	Manual system, confirmation based on licenses and shipment numbers	Cumbersome, human error, easy to fool or forge	Identity Confirmation, Logical Access

Table 2 - Cargo security problems

tion technology into its customer service operations to enable customers to release empty railcars. Prior to integrating this technology, eighteen percent of Union Pacific's total customer service calls - approximately twenty two thousand monthly - were placed to notify the company of empty railcars to be moved out of the customer's inventory. Transferring thirty percent of these calls to a secure automated system has expedited release requests and reduced call centre costs by offloading calls from human operators. One thousand users access the system to release approximately seven thousand railcars per month.

Concept piece for expedited border crossing between Canada & US

InterVISTAS Consulting, Inc, a strategic consulting firm in Vancouver, has introduced a concept piece - a strategic approach - to address the management of land border crossings between the United States and Canada. The plan addresses the movement of both passenger and commercial vehicles with an emphasis on expediting freight movement. InterVISTAS project was motivated by the Smart Border Declaration, a thirty-point action plan designed to speed and secure the flow of goods across the U.S./Canadian border. The Smart Border Declaration addresses the impact of post 9/11 security measures on cross-border transportation and specifically references the need to create a common biometric platform as part of an overall border-crossing solution.

Fifty percent all Canadian cargo is destined for the U.S. and more than four hundred thousand containers cross the border each year. The border covers fifty five hundred miles and includes one hundred thirty crossing points with three locations -Windsor, Vancouver and Niagara Falls --accounting for seventy percent of this traffic. InterVISTAS's strategy integrates several technologies including electronic seals, radio frequency identification (RFID), global positioning (GPS) for freight containers and commercial vehicles and biometrics for attendants, drivers and other individuals involved in the management and distribution of cargo. The idea is to pre-clear low-risk cargo delivered by pre-approved or "trusted" drivers to reduce border choke-point congestion.

Logical access: Electronic Supply Chain Manifest - O'Hare Airport

The Chicago O'Hare Electronic Supply Chain Manifest System (ECSM) was the second phase of a pilot initiated in 1996 to design, develop and test a technology-based alternative to existing manual air cargo processing. The project goals were to automate traditional manual processing of cargo documents to improve operational efficiency and to secure cargo integrity by confirming the identify of responsible parties along the entire distribution chain. Phase-one of the pilot used biometric identification linked to smart cards to secure electronic manifests and confirm identity of all individuals originating, transporting or receiving cargo.

Phase-two extended the efficiency and security achieved in phase one by introducing a secure virtual private network (VPN) to automatically transfer cargo information and shipping data across multiple transportation modes and political jurisdictions. The system tracked shipments from origination in the Chicago area through delivery to JFK across twenty individual distribution chains.

The market innovators profiled in this section have linked human identity to the transfer of goods and delivery of services. As these organisations have learned, this link not only creates accountability but expedites cargo processing, helps address fraud

and theft risks, and provides an accessible and reliable audit trail. For these market innovators, biometrics solutions contribute to increased operational efficiency as well as enhancing security. In the Chicago O'Hare electronic manifest pilot, biometrics-based driver-authentication system proved two to four times faster than traditional paper based systems. Union Pacific Railroad's voice-recognition rail car release program reduced call centre traffic for these calls by thirty percent. These examples highlight the dual benefits of biometrics based solutions - improved efficiency and increased security.

While the actual adoption of biometrics technologies for cargo applications has been limited, these initial deployments have met with great success.

Problems and solutions

Table 2 highlights the most pressing security issues facing cargo transportation companies and indicate how the application of biometrics technologies can help provide solutions.
Proponents of biometrics enhanced security perceive great potential for the use of this technology to address many urgent security concerns including theft, hijacking and contamination of critical cargo. Critics of biometrics (and other security related technologies) point to the United States War on Drugs as an example of a serious failure in the ability of a major industrialised national to control the flow of illicit goods across it's borders in spite of a substantial resource commitment.

Who is adopting biometric solutions?

Inter-modal transportation, the movement of goods via a container using two or more modes (maritime, rail, air or truck), is the one of the fastest growing sectors of the transportation industry. As the built-in efficiencies of various transportation modes are leveraged to squeeze margins out of an increasingly competitive industry, more of the world's cargo is shipped inter-modally. This has significantly increased the opportunities for compromising the integrity of these cargo shipments. Each time an additional mode of transportation is accessed, an additional transfer point is introduced along with a new opportunity to tamper with containers. Each individual who accepts or transfers responsibility for contents at each of these points introduces another accountability factor.

Traditional paper-based tracking and manifest systems provide a minimal level of security by matching transfer agents, dispatchers and drivers against licenses, organisation identifications and shipment numbers. These methods cannot address the enormous security gaps that currently exist. They provide minimal, cumbersome audit trails and no way to confirm the identities of the individuals handling, monitoring, screening and authorising specific shipments. While electronic-based vehicle tracking and manifest systems (using RFID, GPS and electronic seals) improve the accessibility and usability of audit trails, they do nothing to address the accountability issue. This opens the door for the adoption of biometrics to address the process vulnerabilities created by the current inability to confirm identities of individuals shipping, receiving and transferring containers.

Market evolution

The advantages of biometrics in global transportation are clear. The only way to reliably authenticate individuals originating, transporting, screening, clearing or handling cargo and the associated documentation and information technology systems is through the use of biometrics.

The emergence of 21st century global transportation infrastructure has begun and will drive the kind of large scale technology deployments that will herald the "mainstreaming" of biometrics. Over the next several years this infrastructure - integrating land, sea and air transportation - will be more tightly linked, more closely monitored and more efficiently operated than ever before as emerging technologies, such as biometrics, RFID and GPS, provide the tools to create reliable chains of custody and trust.

by C. Maxine Most, Acuity Market Intelligence