

U.S. Security Market: Changing Dynamics

The U.S. security market is undergoing changes to meet increasing challenges of keeping people safe from threats.

More than five years after the 9/11 tragedy in New York and the July 7, 2005 subway bombing in London, U.S. security professionals are creating some unique but simple solutions to face the growing challenges of protecting people from a terrorist attack.

By Matt Scherer



CHANGE IS UNDERWAY

Take Category 6 wiring as an example. Used primarily as a conduit for the Internet and communication platforms, security professionals have found that they can push packets of information and video to their security monitoring station.

Known as IP-based solutions in the security sector, the change from the more traditional coax cabling that linked a security camera to a video recorder has allowed more people to work in the industry.

Before 9/11 occurred, Palmer Electric, a mid-sized electrical contractor, installed only electrical systems throughout the U.S. Rocky Mountain Region. The attack on the World Trade Center and the Pentagon changed the firm's business perspective. Now, the U.S. firm has moved into the access control space, and it won an annual half a million dollar contract to monitor and manage an access control system for the Air Force Academy.

It's the arrival of other contracting professionals like Palmer Electric who are comfortable with Category 6 or previously Category 5 wiring that make the market even more competitive, notes Trenton Tom, director of research and development for DigitEyes of Orlando, Fla., the U.S. Cable technicians (like Palmer Electric) pull 10 times the amount of cable for other IT needs so they can provide a lower price than a traditional security installation team, said Tom.

Rob Schorr, Sales Manager for MDI Security Systems based in San Antonio, TX, the U.S., who worked with Palmer on their bid to update and manage the Air Force Academy access control system said

companies like this will take on a greater design and management responsibility for security systems. Using an IP-based method, a business can save as much as US\$1,000 per control point, just on the outside labor and wiring costs, Schorr added.

US, EUROPE AND ASIA

Karthik Nagarajan, a security analyst with Frost and Sullivan of San Antonio, the U.S., said the American, European and Asian markets differ in their adoption of the new platforms.

The Americas is the largest market of the three for now, he said. The gaming and government segments are seeing the highest adoption rate in gaming and government segments, he said.

In the U.S. market, Mike Garcia, vice president of marketing for MDI Security Systems, said he expects a larger demand in the government segment for IP-based products in public school systems. With the recent tragedy involving the deaths of five Amish girls and the injuries to the remaining five, it has forced school administrators to truly look at ways to protect their students from another attack like this, he said.

One of the issues on all of our minds right now is school safety, said Margaret Spellings, U.S. Secretary of Education. Our country has seen terrible and senseless violence in our schools and our heart goes out to the families and communities who are coping with these tragedies.

In Europe, Nagarajan said that market is expected to be the largest market for overall video surveillance in the medium term. He adds, There's huge market potential for IP based solutions.

The Frost and Sullivan analyst adds that the Asian market is highly fragmented with numerous regional and local players. Taiwan and China have taken a leadership role in the security sector.

IP-based solutions are not the only change that security integrators will offer their customers. Here are some other aspects of the industry which technology will impact in the next several years.

INFLUENTIAL TECHNOLOGIES

Common Access Control Cards

In the U.S., the newly formed Transportation Security Administration will issue over 17 million TWIC or Transportation Worker ID Cards providing a standard card for everyone from the aircraft captain to the cafeteria dish washer to gain access to their work station in every airport.

According to a statement released by Randy Vanderhoof, the acting president and chief executive officer of the American Smart Card Alliance last year, the TWIC card will standardize on a single common ID card platform, containing at a minimum a digital photo, hologram security layer, a contact chip migrating to a contact and contactless chip, a magnetic stripe, 2D barcode, and a visible TWIC ID number. The chip will store a reference biometric (to be determined) for instant electronic verification, as well as a PKI digital certificate for logical access and electronic signatures.

In the government sector, the U.S. federal government is requiring a common access control card allowing each government agency to read the security credentials of each worker. The major challenges ahead for the government agencies that are involved are the difficult policy issues that come up when defining a mandatory system that crosses over many different departments and agencies -- all having unique requirements and diverse security needs, Vanderhoof added.

Short termed CAC cards, the new credential will allow government workers to verify not only the clearance level but also document a workers specific skill sets. The new ID cards will make it better for the American government if another hurricane like Katrina occurs sometime in the future.

The smart card of the future could not alert a senior government manager when a person arrives into his work section in an emergency, but it also could provide their full resume of skills and expertise, said Jim Lowder, the chief technical officer of MDI Security Systems.

°The future of the industry is to adapt a platform that allows everyone to communicate with each other,± he said. °A simple solution like the ASCII text (or American Standard Code for Information Interchange) helped the technology industry move information. We are working on something similar in access control by taking our intelligence, decision making capabilities and short term storage to the edge of the network.±

Biometric Access Control Cards

Biometric devices with an access control card are also gaining favor among security professionals and government officials. In 2005, the Australian government adopted one of the world's first biometrically enabled ePassports, paving the way for more secure travel and a smoother transition through airport customs. The Unisys Corporation, the advocate of the program, said it hopes other government and agencies like the International Civil Aviation Organization will encourage further development of these biometric devices.

°Travel security has driven the adoption of biometrics faster than commercial pressures would have,± says Terry Hartmann, a Unisys executive. °However, now that the concept has been proven in a public context it will pave the way for adoption of biometrics by the commercial sector.±

In Malaysia, the government has adopted a MyKad card which is given to everyone of its citizens, 12 years and older.

°We faced two major challenges when we embarked on this project,± said Datuk Azizan Ayob, former Director General of the Malaysian National Registration Department. °The first one was technology, and the second was changing the mindset of the people to accept the new card. To address the technology challenge we evaluated leading edge technologies and chose the best suited for our needs. We used the latest chip and biometric technology to ensure the data on the card are accurate and secure. Now, with a thumbprint image, photograph and surface information, we can verify the cardholder's identity with a Card Acceptance Device (CAD) rather than the naked eye. This helps prevent forgery and misuse of cards.±

Today, these cards not only provide personal verification; they also provide important record-keeping services such as health records.

°In a medical emergency, health records are available for instant information during emergencies,± said Jamaludin Jarjis, the Malaysian Minister of Science, Technology and Innovation at the World Congress on Information Technology held last May in Austin, TX, the U.S.

°The card also has a reloadable 'e-purse' called MEPS-cash that is accepted at government agencies, restaurants, clinics, book stores and gas stations.±

Port Security

With billions of goods moving by ocean going ships, more and more government and private sector analysts are focusing resources on protecting their harbors and business infrastructure. More and more, governments and businesses will work together to set standards such as the Customs-Trade Partnership Against Terrorism (C-TPAT).

°This voluntary (for the time being) government-business initiative can provide the necessary cargo security only through close partnerships with everyone involved in the international supply chain,± said Schorr. °Importers, carriers, consolidators, licensed custom brokers and manufacturers all have to adopt policies that will safeguard the international maritime shipping industry.±

With the increasing threat of terrorism, C-TPAT depends on the complete cooperation of the entire global supply chain. Most consumers take for granted the security needed to safely move goods from a manufacturer to a retail outlet. Yet, a major attack or even an incident like Hurricane Katrina can impact the delivery of everything from petrol to food.

°The changing nature of the threat, and the need to stay one step ahead of the game is always a challenge,± said Hani S. Mahmassani, the Charles Irish Sr. Chaired Professor in Transportation

Engineering at University of Maryland. The fragmentation of authority and responsibility through the various steps of a shipment's trajectory, particularly as it is handled through transshipment nodes or intermodal terminals, remains an important challenge and window of vulnerability.

Radio frequency identification monitoring devices will help organizations like C-TPAT monitor the movement of containers from port to port.

Joseph McGrath, the chief executive officer of Unisys, said the U.S. Government has built the security infrastructure to track shipping cargo steaming from more than ports in the U.S. Our Department of Defense has created four servers that can track these goods at over 1,500 locations, he said.

Still, many shipping companies still use security devices that cost about 25 American cents to make, he added.

One major attack will motivate the (U.S.) government to adapt a national standard, said Admiral (Retired) Bobby Inman, the former American CIA director, and the Lyndon Baines Johnson Chair.

Whatever the threat, security professionals need to look at ways to upgrade their technology that allows for a safe and open architecture design. Security professionals, regardless of their location, must embrace something that is scalable to their client's need and allows them to grow and expand their base of operation.

Matt Scherer is a frequent contributor to American security publications and this is his first article for SecurityWorld International.

For more information, please send your e-mails to swm@infothe.com.

©2007 www.SecurityWorldMag.com. All rights reserved.

Close