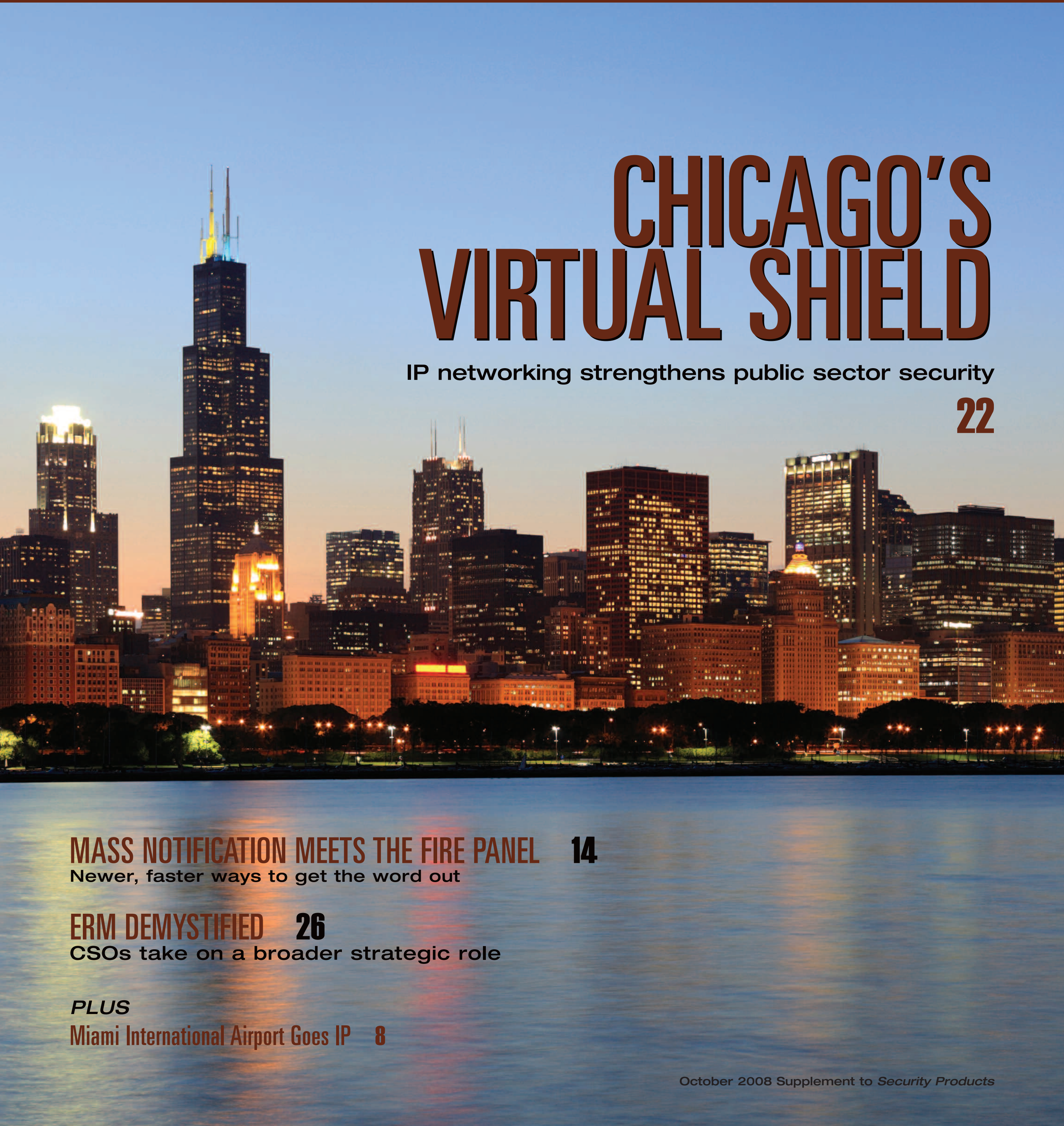
network centric Security

WHERE PHYSICAL SECURITY & IT WORLDS CONVERGE

October 2008



CHICAGO'S VIRTUAL SHIELD

IP networking strengthens public sector security

22

MASS NOTIFICATION MEETS THE FIRE PANEL 14

Newer, faster ways to get the word out

ERM DEMYSTIFIED 26

CSOs take on a broader strategic role

PLUS

Miami International Airport Goes IP 8

October 2008 Supplement to *Security Products*

network centric Security
Where Physical Security & IT Worlds Converge

Content

OCTOBER 2008 VOLUME 2 NO. 5

features

departments

Network-Centric Security welcomes vendor information and briefings. To arrange a briefing, please contact our editor, **Steven Titch**, via e-mail at **titch@experteditorial.net**. Our agreement to accept or review product material or backgrounders is not a guarantee of publication.

EDITORIAL

Editor
Steven Titch
281-571-4322
titch@experteditorial.net

Art Director
Dale Chinn

Publisher
Russell Lindsay
rlindsay@1105media.com

Associate Publisher/Editor-in-Chief
Security Products
Ralph C. Jensen
rjensen@1105media.com

SALES

District Sales Manager
West/Southwest/Central
Barbara Blake
972-887-6718
bblake@1105media.com

District Sales Manager
South/Southeast/Midwest
Brian Rendine
972-687-6761
brendine@1105media.com

District Sales Manager
NE/Eastern Canada/International
Randy Easton
678-401-5543
reaston@1105media.com

District Sales Manager
California/Central and Western Canada
Ben Skidmore
972-587-9064
bskidmore@1105media.com

District Sales Manager
Europe
Sam Baird
+44 1883 715 697
sam@whitehillmedia.com

District Sales Manager
China
Jane Dai - New Buddy Limited
+86-755-82925229

District Sales Manager
Taiwan
Peter Kao–Idea Media
+886-2-2949-6412
peter.idea@msa.hinet.net

1105 Media
14901 Quorum Dr., Suite 425
Dallas, TX 75254

Editorial services provided by
Expert Editorial Inc.
www.experteditorial.net

The information in this magazine has not undergone any formal testing by 1105 Media, Inc. and is distributed without any warranty expressed or implied. Implementation or use of any information contained herein is the reader's sole responsibility. While the information has been reviewed for accuracy, there is no guarantee that the same or similar results may be achieved in all environments. Technical inaccuracies may result from printing errors and/or new developments in the industry.

ERM: What It’s All About

by Steven Titch, Editor

The debate is over.

There is no doubt that when it comes to securing the enterprise, end users are abandoning single-vendor, proprietary models and embracing open, interoperable architectures supported by multiple sources.

Nonetheless, there are a handful of vendors who, while acknowledging the trend toward IP networking, insist this convergence will still take an indeterminate time to mature. There’s still a lot of analog CCTV equipment out there, and users are hesitant to toss that out just for the sake of merging security and IT.

This desperate argument attempts to frame IP as just another procurement option as if it were analogous to choosing a proximity reader vs. a card swipe. To be sure, the amount of legacy security equipment and its relative age factor into any purchasing decision, but these days security RFPs deal (or should deal) with more than how systems purchased in 2009 will mix with systems purchased in 2002.

The limitations of proprietary systems become unavoidable when the conversation turns to enterprise risk management. As the article beginning on page 26 reports, ERM has become the foundation of the chief security officer’s job. Though the emphasis was not too long ago on choosing product solutions to meet specific security needs, the new task is aligning the enterprise’s security priorities with the enterprise’s vulnerabilities taken as a whole.

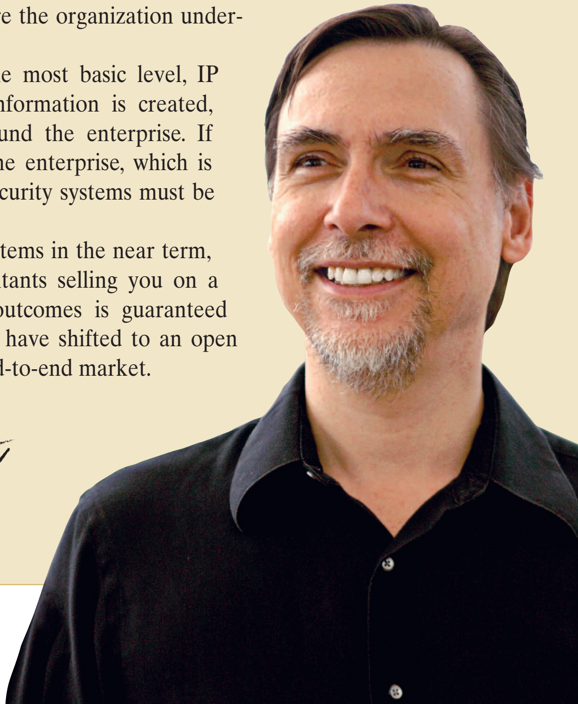
The change is subtle but significant. Yes, the job still calls for extensive knowledge of the nuts and bolts of surveillance, access and alarm systems. What’s new is the requirement to adapt the security process to the goals of the larger corporate mission.

For example, until recently, the CSO’s job was “protect the facility.” Today, it’s “protect shareowner value.” It’s more than semantics. CSOs must now measure, quantify and qualify risks and vulnerabilities against the consequences of a breach or breakdown. “Protect property” has morphed to “protect assets.” To steal your confidential information, I don’t need to filch a disk or a document. All I need to do is find an unsecured work station and use the flash drive I brought with me. Are your surveillance, access systems and IT safeguards integrated enough to catch me before I’m out of the building?

Finally, yesterday’s request to comply with corporate policy has become today’s requirement to comply with the law. Those fax cover sheet boilerplates about proprietary information? Those dictates about not deleting e-mails? Ignoring them could mean criminal liability. It’s the CSO’s job to make sure the organization understands that from top to bottom.

What does this have to do with IP? At the most basic level, IP networking is the foundation on which all information is created, processed, manipulated and disseminated around the enterprise. If security is going to be an elemental part of the enterprise, which is necessitated by laws such as Sarbanes-Oxley, security systems must be compatible with IP.

Some enterprises will do well with hybrid systems in the near term, but beware of vendors, integrators and consultants selling you on a long-term proprietary strategy. One of two outcomes is guaranteed within the next 24 to 36 months: they’ll either have shifted to an open systems strategy themselves, or be out of the end-to-end market.



Miami Airport Goes IP

by Steven Titch

Security convergence has taken a major step at Miami International Airport with Ericsson Federal's completion of a large-scale customized installation of an integrated digital video, audio and access control system. The deal also represents a substantial inroad by a telecommunications company into security contracting, pointing to the growing significance of large-scale networking experience in security work for major infrastructure points.

More than 15 million travelers pass through the airport each year, placing Miami International in the top 30 worldwide in terms of handling passengers. The airport serves as a major U.S. gateway not only to Europe, but also to Latin America.

Ericsson Federal, Plano, Texas, incorporated in the U.S., is the government system integration arm of Ericsson Inc., the U.S. subsidiary of Sweden's Ericsson AB. Ericsson ranks among the world's leading suppliers of wireline and wireless switching equipment and networks. This background will be increasingly important, says Frank McGhee, vice president of marketing and business development at Ericsson Federal, as security and IP networking converge.

The enormous demand for security integration presents Ericsson with a new opportunity to apply network technology.

Ericsson's telecom and wireless background provides a degree of differentiation from integrators with experience in transportation (Bombardier), building management (Honeywell, General Electric), enterprise networking (IBM, Accenture) and defense (Raytheon). Of its competitors, only Germany's Siemens and Cisco Systems, San Jose, Calif., can boast telecom pedigrees. However, Siemens' integration activities draw on a far more diversified infrastructure portfolio. Cisco has so far shied away from approaching end users as an integrator on security projects, choosing instead to develop channel partnerships.

HIGH-SPEED VIDEO

Ericsson Federal was the lead contractor in the Miami airport project, which brings together equipment and channel partners from a number of sources.

Its solution for Miami International includes live high-speed video surveillance, synchronized with two-way audio intercoms, and supports both digital video and audio recording. The system includes live full-frame video feeds from more than 500 cameras—along with audio and telemetry information—linked to security workstations throughout the airport. The system also includes an access control system and alarm system to secure more than 1,000 access points across the airport.

More than 15 million travelers pass through the airport each year, placing Miami International in the top 30 worldwide in terms of handling passengers.

"Digital video and audio integrate with existing CCTV," McGhee says. The IP backbone network uses asynchronous transfer mode switching, a standardized switching protocol used largely in the telecommunications industry. "ATM offers high reliability, especially for video transmission," he says. "It's a robust, hardened solution."

Elements of the Miami International surveillance system include NICE Systems' network video recorders and Telindus' CellStack video management software, McGhee says. He could not disclose the suppliers of access control systems or video cameras, although he says high-definition, megapixel cameras are part of the mix.

The policy-based CellStack system focuses a security officer's attention only on events that require an officer's direct involvement. In the event of a security breach, an automated alarm notifies a security officer at his or her workstation. The security officer can view the video feed in real time and adjust the PTZ camera to follow the event from any camera on the network. Ericsson also added an analytics package to further aid response.

In addition to third party equipment integration, Ericsson brings its own technology to the project. Additional broadband and Ethernet switching comes from Ericsson's Redback Networks unit. Its Tandberg Television division supplied high-definition MPEG-4 video encoders. Although there's no use of wireless in Miami International's security network now, Ericsson is in a position to apply its considerable work with the third generation wireless so-called Long Term Evolution standard, forward-looking technology designed to boost data speeds in commercial wireless networks as high as 100 Mb/s.

"Ericsson brings a comprehensive platform to address video surveillance management end-to-end," McGee says.

TEST LAB ON SITE

A unique component of the Miami airport contract is an onsite interoperability lab where all multi-vendor surveillance equipment and system components can be tested and verified before being implemented. The lab sees regular use, McGhee says. Cameras, pressure sensors, infrared sensors and other devices have been evaluated. "You work out any integration problems prior to putting it into the network," he says.

Moreover, with security priorities shifting away from turnkey vendors toward an emphasis on best-of-breed components, Ericsson sees an opportunity to leverage its experience both with networking technology and government contracting into the security space. Like enterprises struggling to mix legacy security systems with newer, network-centric systems, the federal government seeks system integrators that do best-of-breed evaluation and deliver quality products that are compatible, McGhee says. "It means understanding the value proposition and putting together the best solution," he adds.

With its traditional telecom market maturing and consolidating, the enormous demand for security integration presents Ericsson with a new opportunity to apply network technology, especially with broadband and video. "It's strategically important to Ericsson," McGhee says. "It brings together all the capabilities the company has."

The security surveillance system at Miami International is one example of Ericsson Federal's National Security and Public Safety solutions. Other Ericsson Federal NSPS solutions include National Border Control systems, emergency response systems and critical area surveillance systems.

"As broadband becomes more prevalent everywhere, we're right at the center," McGee says. "We can move into the multimedia or applications space to utilize this great wealth of bandwidth we're going to see over the coming years."

Honeywell Details Video Management Software Platform

by Steven Titch

Honeywell joined the burgeoning list of vendors offering software designed to integrate video surveillance components via the Internet protocol last month, formally unveiling its new IP-based video management system.

Honeywell, which had teased its Video Management System in March at ISC West, was scheduled to begin commercial shipments in September, according to Rob Blasofsel, access/video integration manager at Honeywell Automation and Control Systems, Minneapolis, who was interviewed for this article in August.

Honeywell is positioning its VMS as a "top box," Blasofsel says. Unlike most of its competitors, which include Milestone Systems, Pelco and On-Net Surveillance Systems Inc., the Honeywell software package does not integrate an NVR per se, but is designed to bring together multiple DVRs, NVRS, digital and analog cameras, and other client devices—from Honeywell and other vendors—under a common management platform.

Honeywell is positioning its VMS as a "top box."

But Honeywell goes one step further. Ultimately, it sees the high-level video platform merging with its access platform to become a single point of security and surveillance management. The video management system tightly integrates with Honeywell's Pro-Watch security management system for access control and management, to the point to where they nearly handshake. "They share common services," Blasofsel adds, referring to code-level software and functions. "They can share common servers. They eventually will form one platform."

For example, the video and access control platforms can work in tandem to ensure there can be video recording and retrieval of all card access entries. It can even do credential imaging if credentialing is part of access policy, Blasofsel says.

Honeywell also provides analytics, an integrated database manager and ATM/point-of-sale support with the system. The software runs on Windows XP and Windows 2003 Second Edition and Enterprise Edition. It can connect to various large-scale storage platforms, including iSCSI RAID from Honeywell, Blasofsel adds. Application protocol interfaces are available, and a software development kit is under development.

Other features include:

- Operator messaging feature enables data sharing of incidents among operators.
- Auto-discovery of cameras connected to Honeywell Rapid Eye, Fusion and Enterprise recorders.
- User-defined macros that can execute common operations.
- Video pursuit made possible with motion detection sensors in surrounding cameras.
- Digital zoom from PTZ and fixed cameras.
- Ability to investigate events and alarms by simultaneously viewing alarm videos at various stages. For every alarm, users can view the video captured during pre-alarm, on-alarm and post-alarm, as well as view live video from the camera that triggered the alarm.

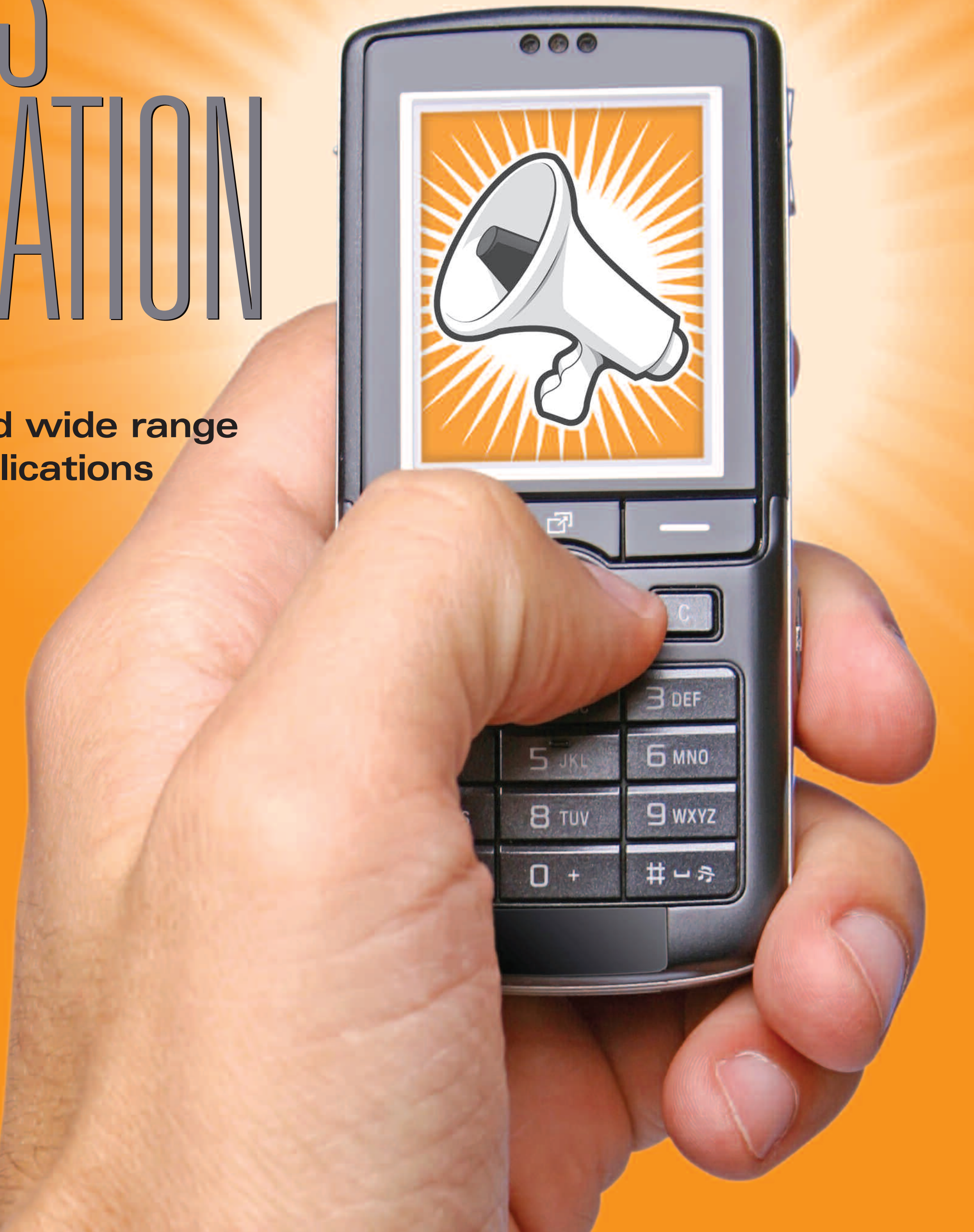
Honeywell licenses the product on a per-interface basis. For example, once the user purchases a license to use the interface for a specific NVR, there is no limit on the number of those NVRs the user can attach, Blasofsel says. The platform is highly scalable from smaller enterprises up through "power surveillance users," he adds.

The software has been in beta testing for most of this year, Blasofsel says, although he declined to disclose any customers. The package is aimed at airports, seaports, large multisite commercial buildings, casinos and other high-profile facilities, he says.

IP SPEAKS CLEARLY IN MASS NOTIFICATION

New solutions add wide range of networked applications

By Sharon J. Watson



How do you tell potentially thousands of people how to avoid an imminent threat?

At Cleveland State University, fire alarm panels in 84 buildings will connect via the school's fiber backbone network. Using a central controller, the school will be able to issue a network-wide warning or to send a message to one building, a specific floor or a single classroom. The system, from SimplexGrinnell, includes Web-based instant messaging to alert students, faculty and parents off campus.

That's a snapshot of a modern mass notification system—not one tool or product but a security solution encompassing an increasing range of networks and applications, many of them Internet protocol-based.

"This market is going through an IP-driven transition and evolution," says Guy Miasnik, president and CEO of AtHoc, a Burlingame, Calif.-based firm providing enterprise-class MNS to military and private-sector clients.

IP is driving the MNS evolution because it enables integration of a wide range of security and business-oriented systems that may then feed to the MNS. The Department of Defense recognizes this ability in Appendix C of its Universal Facilities Criteria 4-021-01 document that details the promise of "net-centric alerting systems" for emergency notification uses.

The appendix acknowledges the ubiquity of IP-based technology throughout public and private entities as well as IP networking and integration opportunities. It encourages DOD facilities to adopt IP-centric notification solutions—and education, industrial and business users are incorporating the UFC language into their own MNS requests for proposal, say vendors.

MESSAGING MATTERS

The higher education market, reacting to highly publicized campus shootings, has driven the market in "software as a service" messaging-based MNS, say vendors. With SaaS, the vendor hosts the application on its own remote servers; the client accesses applications by the Web or virtual private network.

For MNS, these solutions primarily use IP-based networks and communications protocols, like wireless short messaging service, to deliver emergency notifications to personal communication devices, including cell phones, landline phones, PCs, e-mail, PDAs and pagers. Many can convert text to voice as well as send messages in multiple languages.

Most vendors offer Web-based interfaces for creating messaging alerts. "The system has to be easy to launch," says Ann Chamberlin, sales director for channels at 3N Global, Glendale, Calif., which provides messaging solutions. "It can't require an IT person."

Some messaging systems allow individual users Web access for updating and managing their personal contact information. Others query corporate personnel databases, such as Microsoft's Active Directory or Oracle. Most enable administrators to group message recipients into logical categories—by floor, dormitory, function or schedule. Heartland911, a New York-based nonprofit, uses an MNS from Universal Alert, Newark, N.J., to query its databases for volunteers with required skills to respond to natural disasters.

These one-to-many systems have the advantage of being easy to implement. "You deploy once, centrally, on the network," Miasnik says, giving an MNS wide coverage quickly, yet cost effectively.

Messaging systems can vary significantly in terms of infrastruc-

Know Your Fire Panel

Is there a mass notification system hidden in your facility?

"Most don't realize the huge potential they already have in place with their fire alarm system," says Tom Giannini, CPP, director of security and emergency communications marketing at SimplexGrinnell. "It offers a layered technology approach and lets you leverage your infrastructure for a comprehensive plan."

The word is getting out about fire alert systems-based MNS. National Fire Protection Association members are reviewing a new, draft chapter for the National Fire Alarm Code (NFPA 72). Known as Chapter 12, "Emergency Communications Systems," and drawing from the Department of Defense's UFC document, the chapter lays out specifications for when code-compliant fire alert systems could be used for "routine, frequent use" and when an MNS alert could take priority on such systems.

"The fire alarm system has always been sacred ground," says Peter W. Tately, sales development manager, MNS, at Siemens Building Technologies. "Chapter 12 opens the door to using it for additional purposes."

Modern fire alert systems can incorporate paging, horns, sirens, speakers, preprogrammed voice announcements and LED screens, most now restricted by fire codes for use only in a fire emergency. Highly survivable token ring networks connect fire panels, many of which are IP-addressable and can be managed from a central workstation. Further, they are routinely inspected and tested. All of these qualities make the fire alert system a natural focal point for MNS and beyond, say some vendors.

"In 2010, as horizons broaden, the fire control panel becomes the centerpiece," Giannini says. He says increasing the functionality of the fire control panel is the most cost-effective way to implement MNS as well as enhance security.

Other vendors expect fire alert systems to remain independent while communicating with other systems via IP. "The fire system really needs to retain primacy as a life safety system," says John Weaver, director of marketing for Gamewell-FCI in Northfield, Conn.

Some entities may prefer to use their existing IP corporate backbone networks for MNS, say vendors.

"There's no [regulatory] code associated with mass notification, so customers want to use their existing networks," says Fred Santos, senior product manager, systems marketing, Siemens Building Technologies. "You can communicate easier with IP."

"Today, people are more comfortable with the network for mission-critical applications," says Guy Miasnik, president and CEO of AtHoc. He points out many corporate networks are now built with redundant routers and data centers.

It's an open question whether local fire officials could require IT networks used for MNS purposes to meet specific survivability and availability requirements—and how those requirements might compare to the ones fire alert system networks meet.

ture robustness and redundancy. That's true in part because some systems now being marketed as MNS originally were designed for non-emergency functions, such as paging groups of employees or sending desktop alerts.

Throughput also can be an issue for less robust messaging systems. Sometimes lower prices mean the vendor is using a non-guaranteed service level from telecom providers—so a time-critical message may take hours or even days to arrive.

Questions to ask include how many servers a vendor operates, where these are based, what its survivability strategy is, how many telecom lines it has available, how quickly messages are sent and how often it upgrades its key system components, says Mark Bomber, strategic products manager for ADT Security Services, Boca Raton, Fla.

"We actively replicate data across all our data sites," says Marc Ladin, vice president of global marketing for 3N Global. The company, which supplies messaging solutions to SimplexGrinnell, runs multiple data centers across the United States and Canada, with each of those sites protected by extensive security measures, he says.

> Some messaging systems allow individual users Web access for updating and managing their personal contact information. Others query corporate personnel databases, such as Microsoft's Active Directory or Oracle.

GREAT VOICE STILL SPEAKS

However, even with redundant data servers and dedicated lines, if a recipient's cell phone or PDA is not enrolled in the system or is turned off—a requirement in many classrooms—the one-to-many personal message fails.

"We've seen institutions that have purchased these systems and find text messaging isn't enough," says Tyler Johnston, director of marketing development, MNS, at Cooper Notification, Long Branch, N.J.

"You've got to work the Web messaging into the overall MNS strategy," says Peter W. Tately, sales development manager, MNS, at Siemens Building Technologies, Buffalo Grove, Ill.

A comprehensive MNS strategy, vendors say, includes one-to-many personal messaging as well as components typically associated with fire alert systems: visual displays, sirens, horns and loudspeakers capable of projecting intelligible "great voice" messages over significant distances. Large education or industrial campuses might need to cover athletic fields or parking areas with wireless networks.

The University of California at Los Angeles, an AtHoc client, has an MNS that incorporates traditional fire emergency devices like sirens and horns and also uses an IP network to communicate to all types of mobile and desktop devices. Further, IP technology integrates the IP tools, fire system and radio to a unified console.

"They've achieved a very high level of redundancy in the way communication goes out to people," Miasnik says.

"One solution doesn't fit all scenarios," Cooper's Johnston says. "If you have multilayered systems, you can target your audiences and give each group specific instructions."

ONE SYSTEM, MANY TRIGGERS

Vendors report that many customers ask them to integrate MNS to other internal and external systems, ranging from industrial sensors to local police departments.

"We see more technologically advanced customers saying they want as many of their systems to be interfaced as possible," says Tom Giannini, CPP, director of security and emergency communications marketing for SimplexGrinnell.

Planning For The Worst

A mass alert will be effective only if it's been well thought out in advance, all vendors agree. Clients must consider what threats—natural, criminal, terrorist—they face as specifically as possible and what their responses to those threats would be. That includes knowing how messages would be worded, how they would be delivered and to whom.

Answering these questions helps define the true scope of a client's MNS needs, says Mark Bomber, strategic products manager, ADT Security Services. He says some messages must reach just a few key people empowered to act on them and an existing access control or video management platform may already accomplish this. "We might be able to implement existing procedures, not rewrite them," he says.

"Utilize triggers and information points to create event-driven scenarios for MNS," suggests Tyler Johnston at Cooper Notification, director of marketing development, MNS. He notes IP-integration enables systems to trigger actions as well as messages, such as closing a gate and activating cameras.

Some vendors, including 3N Global and AtHoc, offer clients prepackaged response templates tailored to potential situations in vertical markets, such as military, higher education and industrial. These can be starting points to help clients develop comprehensive MNS strategies.

"By having precreated messages based on best practices, there's a better chance people will take the right actions," says Marc Ladin, vice president of global marketing for 3N Global.

Systems triggering the MNS range from National Oceanic and Atmospheric Administration weather bulletins to hazardous materials sensors to security systems such as access control and video analytics. Giannini says a fire system could trigger video cameras to switch on at high resolution to record an area where a smoke alarm is active.

Such integration is relatively easy to achieve, provided the other systems also use common IP protocols, including RSS, XML and CAP. Vendors may provide software application protocol interfaces, making it easier for third parties to integrate with their systems.

"What we see is MNS becoming a component of a complete physical security architecture," Miasnik says. "The notification space opens a path to a more comprehensive security solution."

> The flexibility of an IP-based MNS also leads clients to use their systems for a variety of non-emergency purposes, vendors say.

The flexibility of an IP-based MNS also leads clients to use their systems for a variety of non-emergency purposes, vendors say. For instance, Raytheon uses its system for multimedia video presentations to specific business units; Boeing has added an RSS news feed. Both are AtHoc clients.

One Siemens healthcare client implemented an MNS for fire alarms and then realized it could be used to manage certain clinical procedures and physician on-call schedules. "They've found three or four daily use applications when the original goal was emergency use," Tately says.

Some consultants worry daily use of an MNS could dull its impact in an emergency. Vendors, however, say using the system often helps administrators be comfortable and familiar with it instead of coming to it cold during an incident. In addition, emergency communications can easily be demarcated so they are not mistaken for a routine message.

"Our system provides capabilities to create different user experiences based on the types of data coming in," Miasnik says.

That range of user experiences made possible by an MNS means many functions should be represented in MNS implementation specifications, say vendors. These include facilities, security, IT, business continuity and upper management.

"You really need them all in the room to figure out how to cover all the constituencies," Johnston says.

Sharon J. Watson is a freelance writer based in Sugar Land, Texas. (sjwatson@experteditorial.net)

PUBLIC SECTOR PROTECTION

From Chicago to San Diego to Houston, networked security strengthens surveillance, perimeter protection and threat detection

By John W. Verity

Mark Denari, director of aviation security and public safety at San Diego International Airport, quickly rattles off a list of advantages when asked about using IP with security systems.

"Moving to IP means more simplified systems with fewer controls and fewer boxes to contend with," Denari says. It's easier to attach devices to IP networks and get applications to share data, he adds, but with their fine-grain addressing schemes, it's also easier to limit access to those devices and applications on a selective basis. "We see IP systems as the way to go," he says. "Clearly, digital technology gives a greater degree of flexibility, alacrity and effectiveness."

Denari's enthusiasm is evident across the government sector. From San Diego to Houston to Chicago, airports, school districts, educational campuses and entire cities are embracing IP as a networking and operational platform.

IP-POWERED SHIELD

Easily one of the world's most ambitious municipal video surveillance systems is the city of Chicago's Operation Virtual Shield. And it's putting IP to the test across a wide spectrum of technologies and applications—serving as a showcase for both suppliers and the Department of Homeland Security.

The project's first phase saw the installation of several hundred PTZ cameras around what Jim Argiropoulus, acting executive director of the city's Office of Emergency Management and Communications, calls "especially hot areas" of the city's downtown business district. Now, several hundred more cameras are being added, along with sophisticated analytics from IBM, and the city is moving to exploit IP's superior flexibility in tying together many disparate technologies located across the city's 237 square miles.

One example: In addition to viewing scenes and incidents via the city's own street-mounted cameras, Chicago safety and law-enforcement officials also can selectively harness private video surveillance networks. The set-up mirrors the networked video surveillance system in London that proved successful last year in preventing a car bomb detonation in the West End and identifying the suspects (see "The London Eyes," November 2007).

Argiropoulus declines to state how many video networks are available to his command centers, but he cites the Sears Tower, the Board of Trade and Blue Cross Blue Shield of Illinois buildings as typical examples. At the city's request, each location's private video net can securely connect via a virtual private network concentrator to the city's own surveillance system. Software supplied by Genetec, St. Laurent, Quebec, melds the city and private video streams to create the illusion of a seamless whole. Staffers at the city's emergency command and control center can readily switch between views as needed and bring up related information on the city's 911 emergency map.

"IP enables us to create a single solid video solution" from potentially many different video sources, Argiropoulus explains. "It enables us to gel video packets with some highly sophisticated applications, too." He offers the example of plume modeling—a computer-based method for predicting how, say, poisonous fumes released by an overturned tank truck will disperse over time. By combining the output of such a program with imagery from a PTZ camera on or near the scene, safety officials can determine how best to get emergency crews to the accident site and how to evacuate. "We can sweep the appropriate areas and get a more granular idea of exits," he says.

IP enables more than just melding different data sources. In addition to operating its own extensive fiber-optic network and telephone company, the city of Chicago has arranged to distribute safety-related data feeds via satellite links. Using leased, 24/7 satellite capacity, the city can deliver virtually any amount of real-time traffic to a fleet of custom-designed mobile command centers. These $2 million vehicles can be driven to wherever the police and fire department may need them.

"We can put PTZ cameras right there on the scene," Argiropoulus says.

Achieving that mobile broadband connectivity, however, took some doing. The challenge: how to overcome the 1-second latency incurred as signals travel the 44,500-mile roundtrip to outer space and back. That delay's enough to cause data packets to be dropped and thereby interfere with voice, video and other real-time traffic.

> Chicago is moving to exploit IP's superior flexibility in tying together many disparate technologies located across the city's 237 square miles

"We can't afford to have our applications hanging" because of latency, Argiropoulus says.

The solution proved to be a satellite-link emulator supplied by the Office of Naval Research, with which Argiropoulus and his team had previously developed close relations. They used this test gear to "tweak the IP stack," he says. Now, the satellite links look like local wireless connections or Cat-6 cabling in terms of providing near-zero latency. "We had to do what the military would do, and we take a lot of pride" in streamlining the satellite links, Argiropoulus says.

In addition to the fiber-optic network, Chicago is employing a wireless mesh network to backhaul video streams from its street-mounted cameras. More than 500 transceivers, supplied by Firetide, Los Gatos, Calif., use licensed spectrum in the 4.9 GHz band to provide 85 megabits-per-second of IP bandwidth. Meanwhile, the city is experimenting with WiFi as a way to send streaming video and other security-related data to laptop computers and other devices out in the field.

IP GOES TO SCHOOL

IP technology's helping smaller cities to achieve high-grade security, and it's helping specific agencies within those cities. Schools in particular are adopting the technology to beef up surveillance while coping with limited capital budgets.

Take the Deer Park Independent School District, serving 12,200 students in the Houston metropolitan area. It has wired its four junior high and three high schools with IP-based video surveillance networks from locally-based LenSec that replace aging and somewhat awkward VHS tape-based setups. By opting for an IP system, says Don Dean, deputy superintendent, the district is able to gain substantial operational efficiencies and prepare for possible addition of new devices and technologies.

Taking advantage of IP video's ability to display on standard PC screens, for instance, the district provides comprehensive coverage of its campuses without incurring the costs of a full-time monitoring staff. Instead of sending video to a central location, the streams from as many as 100 cameras in a single school are divvied up between a number of full-time administrative personnel already working in that facility. Dean explains that most problems in public schools occur just before school begins, during the time between class periods, at lunch and immediately after school. So, at each of those limited periods of time, paraprofessionals such as secretaries and assistant principals stop their regular work and, using a dedicated PC monitor on their desks, watch activities at school entrances and in hallways and common areas.

"There's no empirical data, but we believe a lot of issues of student-on-student disturbances have been reduced because students are educated to the fact that we have these cameras in place," Dean says.

The IP surveillance—running on the same Ethernet cabling that conveys the district's traditional IT traffic—also makes it possible to send live video directly to police and fire safety officials, Dean adds.

> 'We need to maintain situational awareness by leveraging technology and integrating data from multiple sources.'
>
> —Mark Denari, San Diego International Airport

IP TAKES FLIGHT

Feeling more pressure than schools to improve their security are airports, which are reaching for IP-based solutions, too. The core strategy of airport security is summed up as detecting threats, delaying those threats (with fences and screening procedures, for instance) and responding with law enforcement personnel. It's mainly in the detection of threats where technology will play a growing role, replacing human operators with various forms of automation that can share information and act in a coordinated way.

San Diego International Airport provides a good example of how airports are counting on IP to help in this regard. In mid-June, the airport chose a consortium of three companies, led by Munich, Germany-based Siemens, to implement a $4 million upgrade of its physical security systems, with IP providing connectivity and fostering integration of numerous types of sensors and devices. Possibly $9 million more may be spent in the future.

"We can't rely on humans," security chief Denari says, to improve the detection of threats and achieve what he calls "airport domain awareness." Instead, "we need to maintain situational awareness by leveraging technology and integrating data from multiple sources."

Consider how the airport plans to use radar—not to watch aircraft but to detect people and ground vehicles approaching the airport's sprawling perimeter. Thanks to IP networking, Denari says, it will be relatively easy to pass radar-generated alerts with those from other types of sensors, such as thermal-imaging cameras, to a central point for analysis. The key will be a so-called fusion engine, a computer specially programmed to rapidly collect and, using preset rules, analyze and even act on many streams of live data at once. San Diego has chosen such a product from Proximex Corp., Sunnyvale, Calif.

"If data from two different kinds of sensors indicate evidence of a suspicious vehicle penetrating our perimeter, the fusion engine would send a single 'target inbound' alert to the operations center," Denari explains. Among the other technologies that might feed into this mix are shock sensors, buried fiber optics (able to detect movements on the ground above) and infrared video cameras. All, Denali says, will be provided in products that are IP-ready out of the box. "We're really working from the outside in, with every piece of the network being IP-centric."

Video surveillance will surely play a key role in the airport's future. Today, some 350 cameras are in use, but that number could eventually top 1,000, Denali says. Perhaps more important than numbers, though, will be increased video "intelligence." Until now, he says, video has been largely a backward-looking tool, able to record events for later forensic analysis. But emerging analytic methods that autonomously detect anomalies aim to make video much more useful for providing real-time information about an immediate potential threat.

In certain cases, analytics will run within cameras, in others that will be left to servers located upstream on the IP network. For instance, a camera able to detect no activity in a baggage-screening room might stop sending its images to a server for storage. Where it's necessary to automatically recognize and look up license plates on cars at a gate, the analysis might be left to a server.

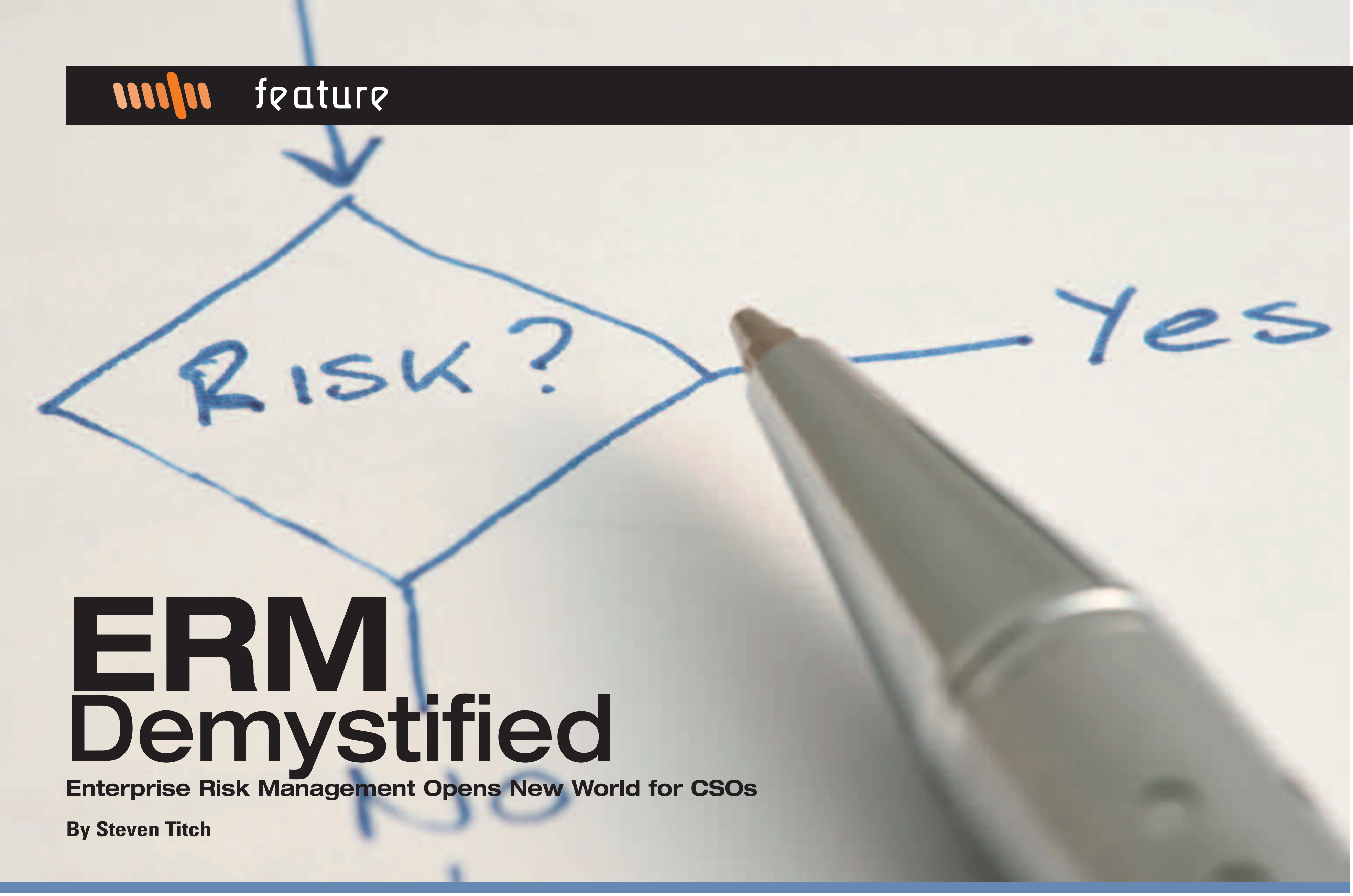
PROPRIETARY IS OUT

Smaller airports are adopting IP, too, if only to reap the benefit of hardware savings. At Orlando Sanford International in Sanford, Fla., security and police chief Bryan Garrett says he's fed up with proprietary security gear. Certain legacy manufacturers, he says, have become notorious for bidding low to win government contracts, only to charge relatively high prices for add-on gear once the customer is locked in. Or, by discontinuing certain product, they might force customers to pay for unwanted upgrades.

With IP, Garrett says, "I can choose from 50 [network] switch makers. IP saves us a lot of money by taking the proprietary nature out of vendors. There's no reason things have to be proprietary." In one case, he recalls, video camera supplier Verint didn't respond to some of the airport's technical needs, so Garrett turned to Genetec. There was no need to change anything at the network's head-end, he says. "All we had to do was reflash some firmware. We were all done in two days."

Orlando Sanford, expecting to serve some 2 million domestic and international passengers this year, has about 300 surveillance cameras installed, many of them analog. But from now on, all new cameras, Garrett says, will be IP-ready, as will every other physical security device that needs to be networked. "We're always looking for better, cheaper ways of doing things, and right now, that means IP."

__John Verity__ is a freelance journalist based in Maplewood, N.J.. He can be reached at john@jverity.com



ERM Demystified

Enterprise Risk Management Opens New World for CSOs

By Steven Titch

Chase Farms in Walkerville, Mich., didn't plan to turn video surveillance into a risk management tool; it just happened.

The agricultural producer originally set out to watch over a seasonal work force by positioning Internet protocol (IP) cameras wherever they were needed. Because the cameras recorded the pace and volume of each day's harvest and processing, the number of laborers working specific fields and the number and frequency of truck pick-ups, Chase realized the cameras were providing a wealth of information it could use to more efficiently manage business operations.

With quantifiable numbers, Chase could better anticipate labor requirements, match shipments to hourly volume, reduce waste, increase safety and compliance and train new workers faster. Savings from all of these improvements plummeted to the bottom line. Beyond reducing Chase Farms' exposure to theft and other physical security vulnerabilities, the process contributed to measurable reductions in workplace accidents, emergency response time, and product spoilage and loss.

Security tools such as video cameras, management software and analytics applications once perceived as purely surveillance tools now have a key role in managing corporate risk, says Eric Fullerton, president of the U.S. office for Milestone Systems A/S, Brøndby, Denmark, which supplies video management software to Chase Farms.

Enterprise risk management is one of many buzzwords bandied about the executive suite these days. Because it is often an ill-defined term, it can be intimidating to chief security officers who suddenly find themselves part of an ERM initiative emanating from the corporate board. In truth, once launched, ERM is a fairly simple process. Most companies have ERM principles in place, although they may never have been identified or qualified as such. Nonetheless, a sudden directive from the executive suite, accompanied by few details, that department managers collaborate on an ERM plan can add pressure and confusion.

But it shouldn't be overwhelming. ERM might be the new watchword of the day, but it is what security has done for years, says Bob Hayes, managing director of the Security Executive Council, a Marietta, Ga.-based professional association of CSOs. ERM is about protecting the assets of the corporation. What's new is that, because of compliance laws designed to protect corporate shareholders such as the Sarbanes-Oxley Act, ERM has senior management attention.

"A lot of this was done internally, but it didn't go very high in the organization," Hayes says. "Now it has to be reported and monitored by the board."

A CONVERGENCE DRIVER

ERM also goes hand-in-hand with convergence. First, there's convergence from a management perspective. Once senior managers get involved, they look at how security operations can be applied to a broader ERM strategy that takes in finance, information technology and even marketing and branding.

"What's changing is that the board and executive management are looking at all hazards and all risks and asking for a plan that handles all," Hayes says. Business continuity, disaster recovery, emergency planning, supplier disruption planning, weather emergency planning and crisis management planning, which may all have once been independent processes, are unified under one plan.

This process is not much of a shift for CSOs in the Fortune 1000, Hayes says, but for some in the "Fortune 50,000," it can be very different. "It's new for companies that have never done this before," he says.

BROADER ROLE FOR CSO

For security professionals, ERM presents new opportunities.

"The CSO needs to assist in crafting a security policy plan," says Mario Sanchez, chief security architect for Hewlett-Packard's ProCurve unit, Palo Alto, Calif. Questions of risk must be viewed from a holistic perspective that addresses both the protection of tangible assets—people and property—as well as intangibles such as brand equity. "It's a process, not a product," Sanchez says.

John Szczygiel, president of Mate Inc., McLean, Va., the U.S. subsidiary of Israel's Mate Ltd., agrees. "ERM forces a CSO to put the security investment in the context of a number of possible risk responses," he says. Those responses cross IT, human resources, financial and legal departments. As a result, risk becomes more broadly defined, Szczygiel says.

> ERM might be the new watchword of the day, but it is what security has done for years.

Szczygiel, who is also vice chairman of the Open Security Exchange, a cross-industry forum promoting platform interoperability, says another change is that many CSOs now must create a business case for their investments. That means assessing the impact of a negative event, delineating methods to handle the risk and articulating the cost.

Szczygiel offers key questions: "What's the right place to protect? Where is the risk to expose? Can you weigh business objectives against the corporate risk appetite?" A CSO who can supply a board with the answers to these questions can end up being elevated to a position where he or she is creating solutions that allow the business to expand, Szczygiel says. He advises CSOs not to view the business case requirement as just a layer of overhead but as an opportunity to work "elbow to elbow as a partner" with other executives in creating and protecting value for the company and its shareowners.

CONVERGED AND OPEN

Along with organizational convergence comes technology convergence. ERM arguably would not be possible without the convergence of physical and logical security. "When people talk about ERM, even without realizing it, it turns into a convergence discussion," says Fredrik Nilsson, general manager with Axis Communications Inc., Chelmsford, Mass., the U.S. unit of Sweden's Axis Communications AB.

The integration of physical and logical security stimulates a process that is greater than the sum of its parts. IP integration allows CSOs to network surveillance, access control and system sensors to derive information that can be used to create more business value and efficient operations.

Data from converged systems also enables better risk identification, evaluation and management. This in turn leads to additional IP integration of security systems. It's a virtuous circle.

It's almost a given that there is a robust IP network within the enterprise to support convergence, says Nilsson, who argues

The New Risk Management Matrix

Position	Individual ERM Responsibilities	Common ERM Responsibilities	
Chief Security Officer	Protection and safety of personnel and property	Theft Attack Contingency planning Disaster recovery	Shareowner value Brand protection External and internal fraud protection SOX and other general legal compliance
Chief Information Security Officer	Protection of information assets		
Chief Financial Officer	Sound budgeting, accounting and general fiduciary practices	Specific regulatory compliance Shareowner relations Procurement review and approval Vendor and partner selection	
General Council	Protection against civil and criminal legal liability		

using IP-based products is the best way to manage security convergence. “It’s the only way to ensure the operation is keeping current with technology evolution,” he says.

Milestone’s Fullerton emphatically agrees. “A CSO must choose a truly open platform to get best-of-breed. No one today knows what the best piece of equipment will be tomorrow,” he says. “That’s why it’s important to choose an ecosystem with partners that play together.”

“They must be able to incorporate the benefits of new technology when it comes along,” adds Fred Wallberg, director of marketing for the Americas at Milestone.

SEC’s Hayes, however, advises end users not to get too caught up in breathless vendor pitches. They still should consider costs, and even a sound ERM program doesn’t necessarily call for a forklift overhaul. “Would I put in an all-new system for that reason?” he asks. “No.”

Hayes advises that CSOs begin with systems that help them assess the threats they face and how they are prepared to handle them. “I think there are products that will help,” he says.

ANALYTICS AND OTHER TOOLS

Hayes is referring to analytics and situation awareness tools, which sit on top of a security system and gather information that can be analyzed and mined for security weaknesses and vulnerabilities. Users then set policies and procedures via the software that identify and confirm a threat or emergency and ensure a proper response. Vendors include Orsus, New York, and Or Yehuda, Israel; ioimage, Herzliya, Israel; and Mate.

Analytics and forensic tools also can help strengthen the all-important value proposition, says Divr Doron, vice president of marketing for ioimage. Analytics, he says, provide statistical information for aggregating types of threats and their causes, a key ERM data set. “It is instructional in providing information patterns—high-risk sites, high-risk time frames,” Doron says.

This approach can be especially effective in achieving cooperation and buy-in from IT security counterparts, who already are accustomed to making procurement cases through identification and cataloguing of events, adds John Whiteman, ioimage’s vice president and general manager for the Americas.

“The equipment a CSO has becomes more valuable to the organization. All of a sudden you can extract value from that,” says Rafi Bhonker, Orsus’ vice president of marketing (see “Finding Danger in the Data,” April 2008). Situation management systems allow CSOs to map the risk concepts, he says.

“The platform takes the ERM concept and implements it in a way you can use,” Bhonker says. Consultants are big on the “book”—the binder that describes top to bottom security policies—but in the heat of the moment, Bhonker says, “no one’s going to open the book.”

STAY ON TARGET

Threats and vulnerabilities are always changing. That’s why CSOs must work to understand not just security issues purely related to physical protection but also the larger risks their organizations face. Security at a defense contractor or pharmaceutical company might be excellent at stopping trespassers or blocking a denial of service attack but fail to recognize other threats.

“The threat landscape is more professional,” ProCurve’s Sanchez says. “Attacks are elegant and finessed.” For example, someone may use a password-guessing program to log on to a corporate network, or they may simply try to walk off with a laptop or flash drive left in an unsecured area.

“People are after information, not to take down the network for the sake of doing it,” Sanchez says. “It’s important not to remain stagnant in the ever-changing environment.”

But there’s no reason this should happen, Bhonker says. Because of ERM, enterprises are making security a strategic part of the organization. “ERM is an issue to everyone,” he says. Certain verticals—transportation, seaports, airports, railroads—are ahead of the curve because of their high-profile vulnerability. But ERM-driven convergence is visible in the growing trend of end users investing in interoperable video, access control, radar, infrared systems, emergency notification, analytics and situation management.

“Two years ago, no RFP addressed this,” Bhonker says. “Now there are RFPs that are very specific as to how the end user wants all their technologies to work in a coordinated manner.”

Steven Titch *(titch@experteditorial.net) is editor of Network-Centric Security*

Applications, Strategies, & Solutions

1 LPR Links with Situation Management

Hi-Tech Solutions Ltd., a developer of optical character recognition computer vision systems, and Rontal Applications Ltd., a provider of incident management and operational continuity systems, have introduced Eagle Eye, a comprehensive system for real-time tracking, monitoring and surveillance of vehicles on campuses, complexes and compounds. Eagle Eye combines HTS's license plate recognition devices and Rontal's SimGuard incident management system.

Eagle Eye's LPR devices can be deployed at entrance gates and various locations including airports, seaports, train stations, industrial parks, military camps and universities. The LPR devices are connected to SimGuard. When a vehicle crosses the first LPR device, it is recorded in SimGuard's database. If the vehicle crosses the main gate and fails to cross the next expected LPR device, the system shows the vehicle's whereabouts by marking the area on SimGuard's situational awareness 3-D display of the site. Operators can then track the suspected vehicle while maintaining full situational awareness and, if necessary, direct a response to the exact location.

2 Codec with Fiber Connection

Bosch Security Systems has released the VIP X1600 XF, a multichannel codec with high-speed fiber connectivity.

The XF series is designed to increase network connectivity and video storage options for end users. The devices feature a 1 GB/s Ethernet port on the rear of the base units and two Ethernet ports and a 1 GB/s pluggable optical transceiver slot on the front. These allow for system designs that incorporate direct connection to an iSCSI storage array or fiber connection to a remote storage area network, among others, and make inside-rack cabling easier.

3 Wireless Surveillance System

AVerMedia Technologies Inc. has unveiled a video surveillance system that combines an NVR, a wireless router and four preconfigured wireless IP cameras.

The EB1704HB WiFi-4 standalone NVR surveillance system offers an innovative surveillance system for residences, small businesses and convenience stores. By using plug-and-play IP connectivity and compatibility, the system can be installed and configured in less than 10 minutes, the company says.

The wireless video system can be connected to virtually any CCTV, LCD or TV monitor with real-time recording and advanced MPEG-4 compression. Onboard intelligence lets motion detection, smoke detectors and other external sensors be added. Alarms can trigger an alert to a cell phone, PDA or remote computer.

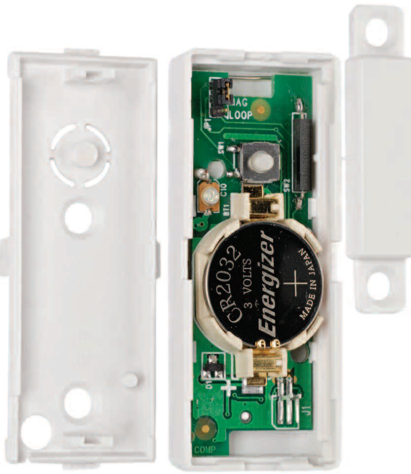
4 Biometric Identification

Sagem Morpho Inc.'s Morpho RapID 1100 line of mobile biometric devices integrates a larger screen, a keyboard, enhanced wireless communication capabilities and digital cameras to support facial recognition.

The Morpho RapID 1100 is built on the Psion Teklogix iKon, a rugged, dust- and rain-resistant PDA. Wireless communication options include WiFi, cellular and Bluetooth with GPS localization. A 500-ppi forensic-quality ruggedized scanner captures digital images of a suspect's fingerprints. Using Sagem Morpho Automated Biometric Identification System technology, the prints are instantly compared against an onboard watch list of up to 180,000 records or transmitted wirelessly for automated identification against a centralized database. Mug shots can be captured with the integrated 2 megapixel camera for facial recognition.

5 Video Server

StarDot Technologies has introduced the Express 2 video server. It features a single input video channel at 30 fps D1 resolution with looping output. With the press of a button, the BNC connectors both become inputs, turning a single input video server into a dual input video server. The device also supports S-video.



6 Low-profile Transmitter

Napco Security Group has introduced a low-profile transmitter designed to mount unnoticed in slimline-type window frames. The GEM-TRANSLP measures 2.5 x 1 x 0.5 inches and comes with one replaceable lithium PL2032 coin cell battery. An internal reed switch and 24-inch external mini connector pigtail lead also are included for wiring jumper-selectable external devices. The transmitter is designed to support alarms, access control systems and video and electronic digital and proximity locks.

7 802.11 Access Point

Strix Systems has introduced a plug-and-play wireless access point supporting up to 64 users per node and industry-standard security algorithms for secured backhaul and client connectivity.

Strix's Integrated Hot-Spot Systems is a dual-radio system delivering 802.11a (optional 4.9GHz) and 802.11g access. Powered by Strix Edge OS, the system scales efficiently and economically, maximizing coverage areas affordably and reducing deployment and operating costs.

8 Facilities Management Software

Continental Access has introduced a facilities management software suite for government users. CardAccess 3000 software supports FIPS 201, TWIC and CAC interim regulations. Integrating software, access control hardware, readers, badging and controllers, the suite can manage an unlimited number of doors, the company says. CardAccess 3000 supports all reader technologies from proximity to biometrics and is a turnkey solution for stand-alone entry level through networked world-class enterprise systems.

Threat level management enables security personnel to react quickly to present or pending dangers by multi-hierarchical threat levels. Security professionals can instantly deactivate access privileges by badge or by entire groups, depending on the threat level. Visitor management, new category counters and activity links provide enhanced building supervision.

Information in this section has been supplied by the respective vendors. *Network-Centric Security* magazine does not accept responsibility for the timing, content or accuracy of the product data or for the quality or accuracy of the photos.

New Standard Boosts PoE

By Steve Bowcutt

Power over Ethernet (PoE) is being widely advertised as a panacea for access control system users. Certainly, we have all looked forward to the day when a single network drop at the door will replace the multitude of cables currently needed for card reader communications, requests to exit, door position and lock power.

The primary objective of any PoE system is to reduce costs. Stringing wire throughout a building for a proprietary access control network is often the most expensive part of the total system. If any system commonly found in today's modern building needs an alternative to standard AC power, it is the access control system.

A basic PoE system will consist of powered devices (PD) and power sourcing equipment (PSE). A typical example of a PD is PCSC's door interface module, which distributes power to the card reader, the locking mechanism and request-to-exit (REX) device. A typical example of PSE is a PoE switch.

RELEVANT STANDARDS

Since 2003 the applicable IEEE standard for PoE has been P802.3af. This standard permits use of Cat-3 cable, but limits power per port to a maximum of 12.95 watts. As PoE has become more popular, the power limitation of this standard has stifled device manufacturers' ability to meet marketplace demands.

> The new standard nearly doubles the power from the older AF standard.

The new PoE Plus standard (IEEE P802.3at, also known as Hi PoE) is nearing completion and is expected to be ratified soon. Draft 3.0 of the new standard, dated March 2008, nearly doubles the power from the AF standard. However, the standard will require the use of Cat-5 (or better) cable. The eight wires of Cat-5 cable versus the four of Cat-3 allow more power to be transmitted. The AT standard also requires PoE Plus equipment to be compatible with existing AF equipment.

Table 1 shows power requirements for PDs vary according to the device type, manufacturer, load, cable length and other factors. PCSC's door interface module, for example,

continued on page 34

Table 1: Power Required at the Door

Powered Device at the Door	Required Power
Door interface module	2.4 watts
Reader	3 watts
Lock	6 watts
REX device	1 watts
Total power requirment	12.4 watts

Table 2: Powered Device Classification

PD Classification	Power Available for the PD
“Default, Type 1”	0.44-12.95 watts
Type 1	0.44-3.84 watts
Type 1	3.84-6.49 watts
Type 1	6.49-12.95 watts
Type 2	12.95-25.5 watts

requires 200 mA at 12 vdc or 2.4 watts. A typical door locking mechanism may require 500 mA at 12 vdc or 6 watts. A REX sensor may require another watt. A card reader may require 3 watts. Even without allowing for environmental factors and cable length, a fully loaded access control system can easily start to approach the upper limit of the older AF standard.

Table 2 shows the powered device classification defined in P802.3at. Minimum power available for PDs, factoring in cable length and environmental factors, is shown.

Type 1 PDs, or IEEE P802.3af devices, have a maximum wattage requirement of 12.95W. Type 2, or IEEE P802.3at devices, have a maximum wattage requirement of up to 25.5 watts.

PoE is quickly becoming a viable alternative for access control system designs. Well-designed PoE-based access control systems will comply with the new IEEE P802.3at standard by incorporating Cat-5 or better cable and Hi PoE power availability; consist of PDs that have been designed and tested to meet the PoE Plus standard; and incorporate power back-up systems that keep the access control functioning during a power failure.

The long awaited panacea for access control systems may very well be a reality given the new, soon-to-be-ratified, IEEE P802.3 at PoE specification. Be careful when looking through the marketing hype to identify those access control system and PoE device manufacturers that understand and conform to the developing industry standards.

***Steve Bowcutt** (sbowcut@1pcsc.com) is business development manager at PCSC Inc.*