

network centric Security

WHERE PHYSICAL SECURITY & IT WORLDS CONVERGE

March 2007

PREMIERE ISSUE

Guardians at the Gates

Trends in smart card
integration **10**

WHEN WORLDS CONVERGE

How security can work
in harmony with IT **16**



VIDEO RIDES the California's Foothill Transit

deploys networked
surveillance system **22**

PLUS: IP Video
Breaks Out **6**

SEE THE FUTURE

NETWORK-BASED VIDEO SECURITY SYSTEMS



Pelco is proud to introduce Endura, a high-quality, high-performance network-based video security system. Endura offers a powerful distributed system architecture and robust hardware/software platform for utilizing the functionality of today's Ethernet networks. With Endura, customers are no longer constrained by traditional, centralized video system approaches. There is virtually no end to how a system and its components can interact and share video, audio, and control information. Endura is the future of video security.



Circle 200 on card.



PROTECTING PEOPLE AND PROPERTY IN A MILLION LOCATIONS WORLDWIDE
TO CONTACT A PELCO SALES REPRESENTATIVE, CALL (800)289-9100 OR (559)292-1981
WORLDWIDE HEADQUARTERS 3500 PELCO WAY, CLOVIS, CALIFORNIA USA 93612

PELCO.COM

EDITORIAL

Editor-in-Chief

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

Art Director

Network-Centric Security
David Hauck

Art Director

Security Products
Cheryl Vaca

Publisher

Russell Lindsay
rlindsay@1105media.com

Associate Publisher

Bill Mahoney
972-687-6716
bmahoney@1105media.com

SALES

District Sales Manager

AK, AZ, HI, ID, MT, NV, NM, OR, UT, WA, WY
Barbara Blake
972-887-6718
bblake@1105media.com

District Sales Manager

MA, CT, NJ
Frank D'Isidoro
908-252-6346
disidoro@comcast.net

District Sales Manager

Midwest, Southeast, North TX
Brian Rendine
972-687-6761
brendine@1105media.com

District Sales Manager

California
Ben Skidmore
972-587-9064
bskidmore@1105media.com

District Sales Manager

UK
Sam Baird
+44 1883 715 697
sam@whitehillmedia.com

District Sales Manager

China
Jane Dai, New Buddy Limited
86-755-82925229

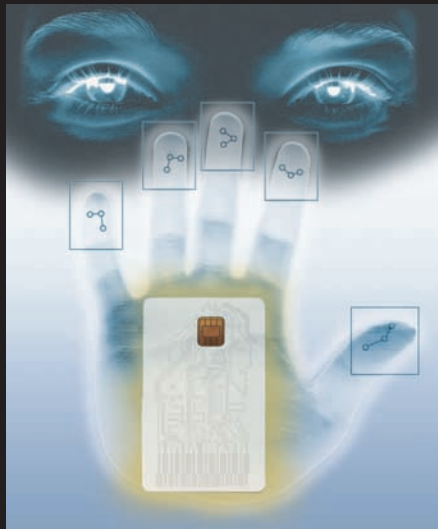
1105 Media

5151 Beltline Road, 10th Floor
Dallas, TX 75254

Editorial services provided by

Expert Editorial Inc.
www.experteditorial.net

features



Guardians at the Gates

By Sharon J. Watson

How do you get more security out of physical and logical systems deployed at dozens of sites on six continents serving more than 7000 employees? We asked Qualcomm about integrating physical access with logical security.

10

When Worlds Converge

By John W. Verity

Differing mentalities, reluctance among executives to surrender turf, inexperience and lack of knowledge are among the many barriers to a successful plan to meld security and IT. And, implemented improperly, convergence can actually make a company less secure than it was before.

16

Video Rides the Bus

By Phil Britt

California's Foothill Transit networked surveillance system is a critical element of its "smart bus" program designed to give better service to its almost 15 million customers per year.

22

departments

Enter

Security becomes a mission-critical business process in the overall enterprise, requiring close-knit cooperation with the corporate IT department, writes Steven Titch, *Network-Centric Security's* editor-in-chief.

4

Innovate

Manufacturers say 2007 will be a breakout year for IP video surveillance, driven in particular by solutions that allow images from analog cameras to be converted to IP data streams that can be readily accessed within an open systems environment.

6

Launch

New applications, strategies and solutions.

28

Exit

Joseph P. Freeman offers tips on how security users can get senior management to pay attention to the serious issues affecting continuity of a well-managed enterprise.

32



Out of the Back Room

by Steven Titch, Editor-in-Chief

Even if you see your company as an average-sized enterprise with purely routine security requirements, chances are your job has changed, or is about to.

Security and information technology convergence is at hand. As John Verity reports in “When Worlds Converge” (see page 16), the portion of global corporations that have in some way integrated physical and IT security has doubled in the past three years. During that same time, there has been a near quadrupling of companies that have grouped physical and IT security operations under the same executive.

If you are a CSO, your job objectives are now being set and measured in a new context. If you are a security systems integrator, your customers are demanding a new level of capabilities plus compatibility with networks, systems and databases once outside your scope.

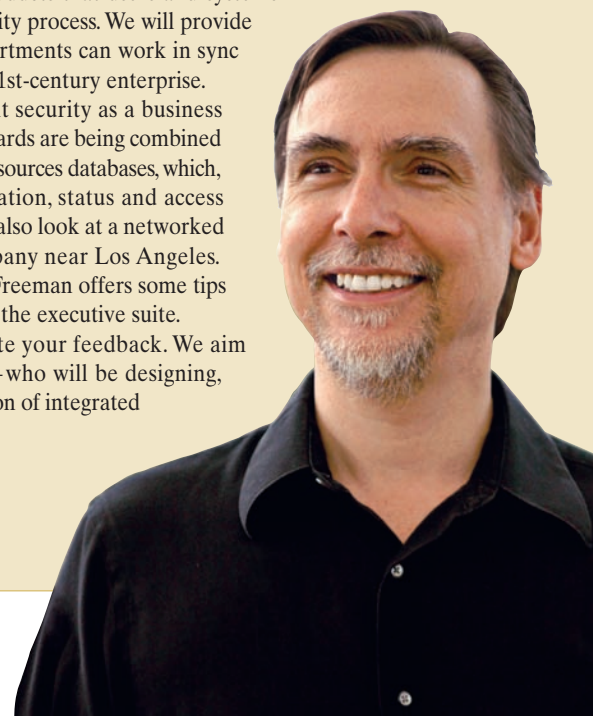
Welcome to the world of network-centric security—where security becomes a mission-critical business process in the overall enterprise, requiring close-knit cooperation with the corporate IT department. Today, enterprise security is more than card readers and surveillance cameras at the entrance, or anti-virus software and firewalls in the computer closet. It’s the strategic combination in the design, planning and implementation of both in order to protect physical assets as well as information, intellectual property, product integrity and brand equity.

In the global economy, effective security must safeguard the corporation in physical space and cyberspace—now understood to be two sides of the same coin. To be sure, convergence is a buzzword, but that doesn’t make it any less real. Just ask any IT veteran. They will recall the organizational upheaval when voice and data converged, and again when proprietary computer networks gave way to the open environment of Ethernet and Internet Protocol.

Network-Centric Security, a special supplement to *Security Products* we will publish three times this year, serves as your guide through the converging world of physical and IT security. We will look at trends in technology, solutions and products that users and systems integrators are applying to the integrated security process. We will provide insight and analysis into the way security departments can work in sync with IT to meet the challenge of securing the 21st-century enterprise.

In addition to Verity’s article on convergent security as a business process, our premiere issue looks at how smart cards are being combined with corporate computer networks and human resources databases, which, among other benefits, keep employee information, status and access authorization up to the minute in real time. We also look at a networked IP video deployment by a public transit company near Los Angeles. Also in this issue, leading industry analyst Joe Freeman offers some tips as to how CSOs can make themselves heard in the executive suite.

We hope you enjoy this first issue and invite your feedback. We aim to build our content around you, the reader—who will be designing, purchasing and implementing the next generation of integrated network-centric security technology.



Receive a
FREE
Security ID
White Paper

Engineered for Card-Carrying Perfectionists.

Self-Aligning Print Head

Provides uniform print quality with vibrant, crisp color.

Angled Card Feed

Patented design consistently feeds each card in the stack.

Built-in 10/100 Ethernet Option

Enables printer networking and simplifies device management.

Mag Card Reject Bin

Eliminates print ribbon waste and reduces cost, by auto-detecting mag stripe encoding errors prior to card printing.



The Zebra P430i Card Printer.

Refined to perfection by over ten years of breakthrough engineering, the P430i delivers consistent high-quality results in the most demanding environments. Zebra Card Printer Solutions can optimize your access control or I.D. badging operations. The closer you look, the better we look.

For more information, please call 1.866.604.2129.



**Card
Printer
Solutions**

For More Information Visit:
www.zebracard.info/sp2

Circle 201 on card.



IP Video Breaks Out

by Steven Titch

Video surveillance technology has reached a key tipping point. Just as the capabilities of analog closed circuit cameras have reached their limit, prices of Internet Protocol cameras have dropped to where they can offer sufficient payback in value and cost of ownership. Meanwhile, a new spate of video servers is about to hit the market that will ease integration of analog and digital cameras into corporate IT networks.

Manufacturers of video servers, NVRs and IP cameras say 2007 will be a breakout year for IP video surveillance, driven in particular by solutions that allow images from analog cameras to be converted to IP data streams that can be readily accessed, stored and manipulated within an open systems environment.

Such developments stand to allow users with a sizable deployment of analog cameras to begin a transition to digital video surveillance networks. Even with the steady introduction of digital cameras, many users, especially large enterprises, have been reluctant to make large-scale commitments to digital and IP video until the costs of their analog CCTV systems could be fully amortized.

VIDEO OVER VPNs

The primary benefit of IP cameras is that they can readily connect to local area networks. IP is an open standard—the common networking language used by devices connected to the Internet. IP is also the protocol used in Ethernet and virtual private networks (VPNs). VPNs use the public Internet infrastructure as a medium for corporate networking. VPN data, however, is encrypted and partitioned from pedestrian Internet traffic, and transmission is enhanced and prioritized through quality of service (QoS) techniques.

IP lets any video feed be routed to any IP device—be it a PC, PDA or cell phone. This can occur over a proprietary corporate network, a VPN or the conventional Internet. The worldwide connectivity dimension adds tremendous value above proprietary CCTV systems, vendors say. Corporate IT departments have been committed to IP for years, and its application in video represents another aspect of its convergence with security systems.

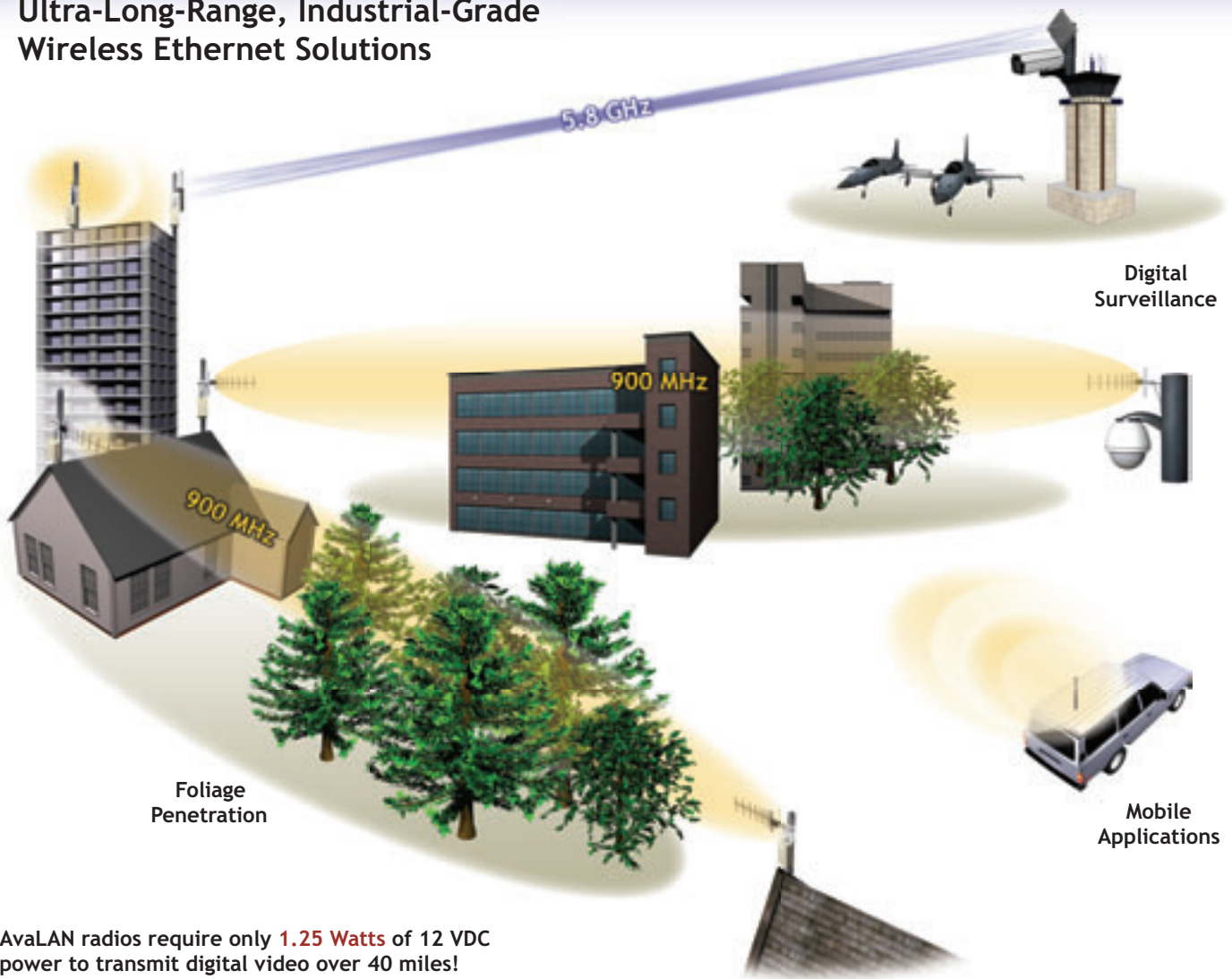
“IP moves the surveillance industry away from vertically integrated solutions with one vendor and opens up the user to ‘best of breed’ cameras,” says Eric Fullerton, president for the Americas at Milestone Systems Inc., the U.S. unit of Milestone Systems A/B, Brandby, Denmark. “Users can choose the camera that fits the application.” This month, Milestone is introducing XProtect Corporate, an IP video surveillance management software package designed for Fortune 500 companies. It represents a new top-end product for the company.

IP lets any video feed be routed to any IP device—be it a PC, PDA or cell phone.



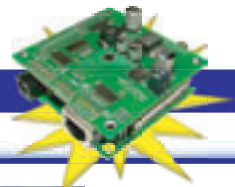
Canon's VB-C50FSi IP camera

Ultra-Long-Range, Industrial-Grade Wireless Ethernet Solutions



AvaLAN radios require only **1.25 Watts** of 12 VDC power to transmit digital video over 40 miles!
Call and ask us about our solar options.

AvaLAN products currently provide wireless connectivity for the following security devices:



Integrated Wireless Housings

Military / Industrial Robots

Biometric Scanners & Access Control

Covert Retail Video Surveillance

AvaLAN will be speaking at the upcoming ISC West 2007 show.
Come see us in Las Vegas!

(866) 533-6216

www.avalanwireless.com

Circle 204 on card.



Proudly Made in the USA

Part and parcel with connectivity, says Fullerton, is scale and integration. IP allows easier integration with data associated with other security processes, from access card entry to point of sale. For example, IP solutions make it much easier for controllers to program video cameras to record in tandem with other data events. For example, a video recording of a large transaction at a casino cage can be logged with data that records the amount of the transaction, the time it took place and the player's account number. While casino systems routinely collect this

which manufactures NVR software as well as associated software for content analytics and video clients, including PDAs. "IP can integrate different manufacturers," he says. "IP video can be formatted and manipulated in more complex ways. Video can be delivered anywhere in the world using off-the-shelf operating systems. The user gets video anywhere, anytime by request or by push." For example, a security director in the field who needs to be brought in on a problem can view video using a cellular connection or via public WiFi.

They also run off the new Power over Ethernet capability, further reducing user costs.

Add to that the value they offer through higher resolution and ability to supply images in low-light conditions, "why would you buy analog?" asks Underwood.

INTEGRATING ANALOG

Yet the large installed base of analog cameras—and the comfort level users have with them—still proves a barrier to IP migration. Milestone, Exacq and onSSI all provide video encoders that can convert analog video feeds into digital IP streams. Once encoded, the analog-turned-IP can be managed and manipulated with other digital video images. "Once you can encode analog video to digital, you turn the analog camera into a network device," says Nilsson.

Likewise, storage solutions can be very flexible. While some vendors centralize storage at a single server, others, such as Bob Banerjee, IP video products marketing manager at Bosch Security Systems, Fairport, New York, say distributed server architecture can work just as well. "Where you store video is not as important as the design." Banerjee goes as far to suggest that the days of NVR may be numbered—more intelligence will be placed in the camera, which will link to standard redundant array of inexpensive disks (RAID) schemes using iSCSI, or the Internet Small Computer System Interface, a transport protocol that operates within IP networks. ☺

Once encoded, analog-turned-IP can be managed and manipulated with other digital video images.

information, when IP extends to surveillance, it can be instantly matched with video should there be an error or dispute regarding the transaction.

Moreover, IP can integrate with more sophisticated processes, including facial recognition and analytics. "Existing customers can do the integration and new customers can future-proof themselves," says Fullerton.

ANALYTICS AND OTHER PROCESSES

Analytics can be slow with proprietary systems, notes Gadi Piran, president and chief technical officer of On-Net Security Systems Inc. (onSSI), Suffern, New York,

But above all, prices are dropping. "IP cameras were once expensive," says Dave Underwood, president of Exacq Technologies, Indianapolis, another supplier of NVR software. "The cost is coming down."

Although when compared heads-up, the price of an IP camera can still be \$200 to \$300 more than an analog CCTV counterpart, total cost of ownership is lower. That IP cameras do not require their own cabling, but can operate on common Category 5 cable or via wireless (see box) is one way they offset the cost of proprietary analog, says Fredrik Nilsson, director of business development at Axis Communications, Lund, Sweden, a camera manufacturer.

Who's Afraid of Wireless?

Ray Shilling admits that radio connections can be intimidating. "Wireless is always a little scary," says Shilling, vice president sales and marketing with AvaLAN Wireless, a Palo Alto, California-based supplier of diverse radio networking equipment for various applications, including security.

Wireless IP exploded earlier in the decade with the widespread introduction of WiFi, a low-power radio transmission format standardized under IEEE 802.11 that operates in the 2.4 GHz band. This makes it ideal for short range, high-speed, over-the-air data connections—about 100 to 150 feet in ideal conditions.

When using WiFi in a private network, however, reliability and security remain major concerns, one reason enterprises

tend to shy away from it in security applications.

That may change, Shilling says, with the growing trend toward mesh networks, which spread signal coverage over wider areas and allow for greater reliability and quality of service. Mesh networks are currently available from vendors such as Motorola, Firetide and Tropos Networks. AvaLAN Wireless can optimize radio systems for enterprise customers. In addition to WiFi and 802.11-based mesh networks, AvaLAN also deploys microwave and mobile radio systems for industrial applications.

The primary advantages wireless cameras offer are flexibility and quick installation. They have become an increasing choice for video surveillance at schools, gas stations and strip malls, Shilling says.

— Steven Titch

Inscape Data

The Expert in Wireless and IP Video Systems

Long Range Wireless

Remote Monitoring

Outdoor Installation

Easy Integration

User Friendly Software



AirEther AB54
2.4GHz AP Base Station



AirEther BR108
5GHz Backhaul Bridge



AirEther CB54E
2.4GHz Client Bridge



AirGoggle NVC210
IP Box Camera



AirGoggle NVC3026
IP Outdoor Speed
Dome Camera

About Inscape Data Corporation

Inscape Data is the expert in long range wireless and IP video systems. Inscape Data offers a full suite of turnkey solutions for long range outdoor 2.4GHz, 5GHz and IP based video surveillance applications including IP67/68 (Ingress Protection) certified all-weather IEEE 802.11a/b/g wireless systems and the IP video security based on MPEG-4 video compression standards.

Inscape Data's AirEther long range wireless and AirGoggle IP based video security products based on the latest wireless and video compression technologies offer the most cost effective remote monitoring solution in the market. The AirEther wireless enables long range point to point and long range point to multipoint connections for wide varieties of extended indoor and outdoor remote monitoring applications, i.e., public safety, transportation, law enforcement, industrial and commercial, and homeland security, etc.

Inscape Data Certified Professional Training, IDCPT, is available to all qualified resellers and system integrators. Please check <http://www.inscapedata.com/cpt.htm> for more details.

Visit us at ISC West booth 2042

All Dealers, Distributors, and Manufacturer Rep are Welcome

Live Demo

AirEther™ Outdoor Long Range Wireless

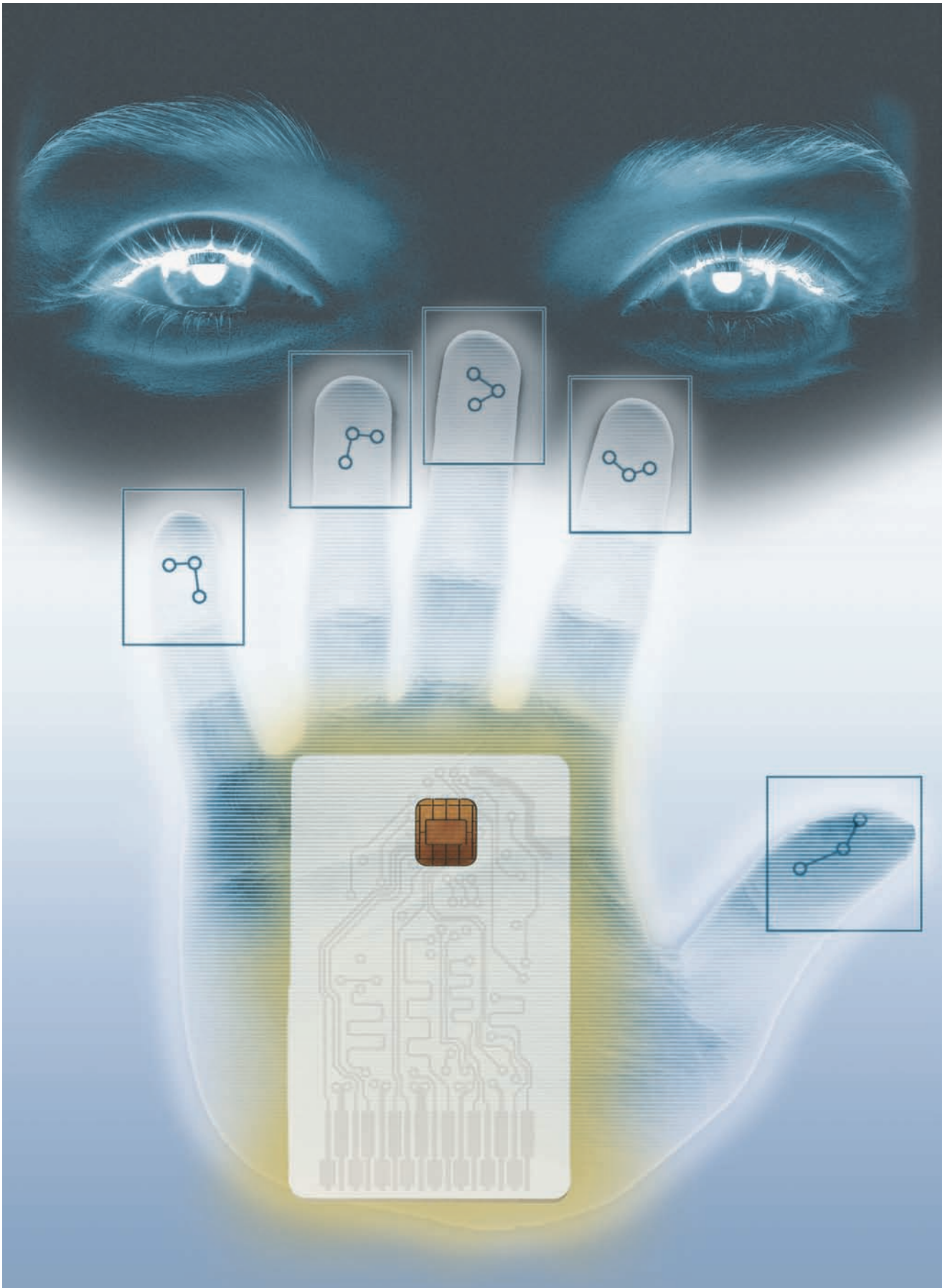
Wireless and Remote Video Monitoring Applications

Integrated Wireless and IP Based Video Systems

North America Headquarters
Inscape Data Corporation
1611 South Main Street
Milpitas, CA 95035
Phone: 408-935-8500
Fax: 408-935-8900

Asia Headquarters
Inscape International Co., Ltd
11F-2, No. 335, Section 3, Rosefu Road
Taipei, 106, Taiwan, R.O.C.
Phone: +886-2-8369-1681
Fax: +886-2-8369-5661

Visit our website at www.inscapedata.com





GUARDIANS AT THE GATES

TRENDS IN SMART CARD INTEGRATION

By Sharon J. Watson

How do you get more security out of physical and logical systems deployed at dozens of sites on six continents serving more than 7000 employees? Integrating physical access with logical security is the answer for Qualcomm Inc.

More than 18 months ago, the San Diego-based wireless communications giant began working with Honeywell International, Inc. of Morris Township, New Jersey, its physical access control system vendor, and Waltham, Massachusetts-based Novell, its security information management system vendor, to develop an integrated authentication and user provisioning solution that would use the capabilities of both systems to greater effect.

The first step was to centralize all card readers—worldwide—having them report to and be managed by a single server, says Chuck Kelly, security engineer for Qualcomm.

“We told the physical security people we weren’t after their jobs – just their data,” says Kelly. “We wanted to know who was accessing an asset.”

Honeywell also needed education. “It was a learning experience for them—they didn’t understand why we wanted to centralize or why IT would care about a badge,” says Kelly.

Novell and Honeywell collaborated to ensure data from Honeywell’s ProWatch physical access system would flow to Novell’s Sentinel event management

system and eDirectory, a Lightweight Directory Access Protocol (LDAP) directory service. These also integrate with Qualcomm’s human resources database from Oracle.

“You can do a lot of things based on identification and physical access when those two are merged,” says Kelly. At Qualcomm, the ProWatch, Sentinel and Oracle systems synchronize once a day with eDirectory. New employees can be provisioned within hours, while badges and physical and logical access automatically de-activate at termination.

A GROWING TREND

Use of a single card or device to access physical and logical systems is a slow but sure trend. It’s driven in part by technological advances vendors are achieving as they respond to federal customers and prospects who must meet the physical/logical convergence requirements of Homeland Security

Presidential Directive 12 (HSPD-12).

Yet physical and logical authentication is under way not just where mandated, but also in enterprises that want the increased security—and savings—of combining physical and logical access controls. Their quest is helped by the industry’s adoption of standards and Internet Protocol (IP) for authentication devices such as cards and readers.

These standards make it easier to integrate authentication devices and systems with logical security systems, enhancing the capabilities of both. IP-enabled devices can become nodes on a corporate network, enabling integration of elements as incongruous as door locks and desktop PCs, card databases and human resources software. Such integration gives physical and logical security experts more effective tools for safeguarding the assets in which they specialize.

Choosing an authentication device is “a less stressful decision now,” says Eric Skinner, vice president, product management for Entrust Inc., based in Addison, Texas. With open standards-based devices, he and other vendors say companies can avoid being locked into proprietary solutions that could compromise long-term security integration strategies.

At Qualcomm, new employees can be provisioned within hours, while badges and physical and logical access automatically de-activate at termination.

Sharing the Keys to the Security Kingdom

Getting more value and security from existing software and systems is one reason IT departments are driving physical-logical authentication integration, say vendors. Yet IT departments don't want to issue badges or maintain door locks.

Meanwhile, physical security teams are beginning to see how authentication convergence can enhance their ability to keep a company secure.

"Convergence elevates the importance of physical security in the IT structure—the cards and readers are not just another thing on the network," says David Ting, chief technology officer at Imprivata.

Regardless of which department drives converged authentication, the smartest card or gatekeeper can't do its job without thoughtful, comprehensive policies, such as who should have access to applications, specific equipment or locations. Creating such rules goes beyond IT and physical security department boundaries to user department lines.

"It involves different groups who in the past have not communicated very much, and now need to be on the same page," says Eric Larsen, senior product manager at Lenel Systems.

"Neither side should own physical security systems," says Chuck Kelly, security engineer for Qualcomm. "Separate the duties. The physical side should be a customer of the application, the IT side a customer for the data."

He says companies understanding that dichotomy will successfully integrate physical and logical systems, the better to put the smartest, strongest protection at their gates.

— Sharon J. Watson

BIGGER VALUE FROM BADGES

For their converged authentication initiatives, users are choosing smart cards that incorporate proximity technology and programmable chips, say analysts and vendors. Combining passive, relatively dumb technology with smart chips enables the new cards to be used with older card readers while offering companies the flexibility to roll out more sophisticated applications.

"These are devices they can deploy today in limited applications that will evolve over time," says Dave Taku, senior product manager, for Bedford, Massachusetts-based RSA Security Inc.

Dual interfaces on cards for contact and contactless applications also enable IT and physical security departments to use the same card, increasing security for each. For example, physical security personnel continually worry about "tailgaters," or unauthorized persons slipping into facilities behind a legitimate employee as he swipes a badge. "Yet they've no way to enforce badge-in policies," says David Ting, chief technology officer at Imprivata in Lexington, Massachusetts.

Authentication-level convergence provides that enforcement. A person who has not badged in can be denied authorization to network applications until she's responded to a series of questions onscreen or via phone calls verifying her identity.

Similarly, if a person is logged into the network from a remote location, anyone attempting to use his card at another corporate facility would be denied access by the logical security system—which could then also alert the physical security system and staff.

Yet while increasing security, converged authentication devices make it easier for employees to access systems without

remembering several passwords or carrying multiple tokens. A single smart card can be endowed with digital certificates, Public Key Infrastructure (PKI), Java-based programs, biometric data and even cash values for debit purchases in the company cafeteria or vending machines.

THE CARD AS COMMODITY

"Adopting smart cards over proximity cards is a great value even in physical security," says Erik Larsen, senior product manager at Pittsford, New York-based Lenel Systems International Inc. Smart cards are blank slates, not pre-encoded the way proximity-only cards are, so an enterprise can essentially customize the card.

"The customer is in control of the card," says Larsen.

Smart cards may also incorporate a range of legacy technology, including

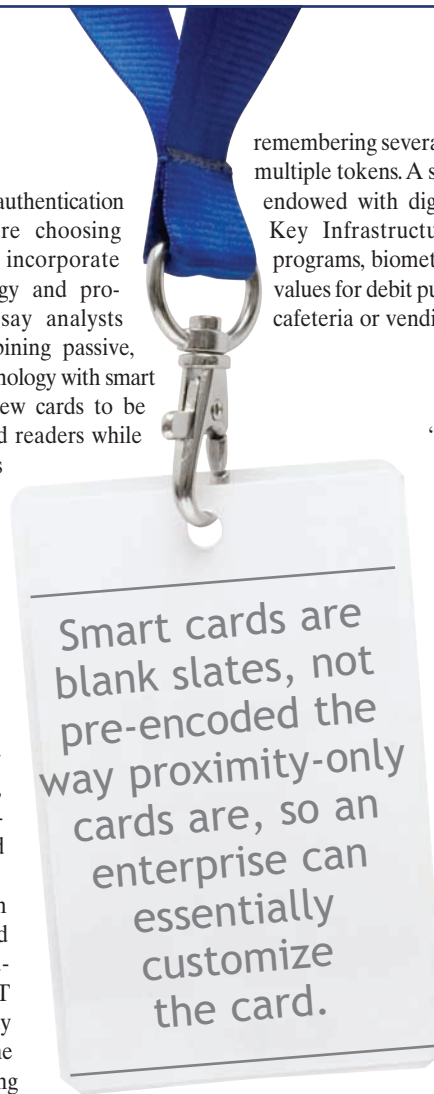
bar codes and magnetic stripes. "It's a shortcut to managing and leveraging all the work that's already been done to verify the identities of employees," says Rob Brandewie, senior vice president, public sector solutions, at ActivIdentity Corp. in Fremont, California.

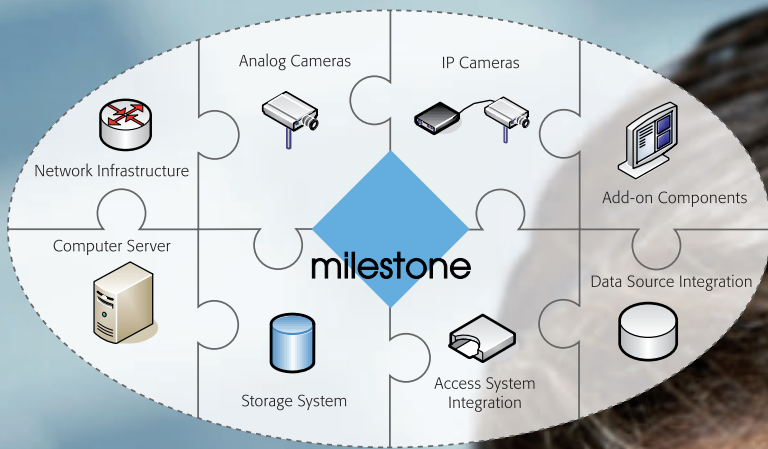
Vendors and analysts agree the price of smart cards has stabilized even though functions have increased, mainly because leading card makers, such as HID Global, now produce cards compatible with ISO 14443, the four-part international standard for contactless smart cards.

"The piece of plastic is commoditized now," says Andy Solterbeck, general manager, commercial enterprise business unit for SafeNet Inc. in Baltimore, Maryland.

That said, some vendors offer innovative smart card features and/or authentication devices designed especially for integrated physical-logical security.

Cryptotex Trust Systems, Owings, Maryland, introduced Mobio last fall.





Are you looking to integrate IP video?

You can video enable your business with a networked security system that works together in one efficient operation. With Milestone Systems IP video software as the core of your platform, you can federate all the elements into one solution: the open platform allows integration with other systems and devices like Access Control, Alarms, Gates, Lighting, Point-Of-Sale, Automatic Teller Machines, and more.

Milestone supports the widest choice in network hardware, too. It's easily scalable and cost-effective to upgrade, proven in performance on more than 24,000 customer installations, sold by authorized partners in 60 countries.

Download a **FREE** 1-camera
XProtect™ license today!
www.milestonesys.com

Circle 202 on card.



The Open Platform IP Video Software

The card-style device, being tested by the U.S. Naval Air Systems Command, converts individual fingerprints into dynamic numbers the company calls "biocodes" using a one-way unique algorithm. The biocodes are valid only for a few seconds, do not repeat and can be used for access to facilities and systems as well as for digital signatures and voice verification.

Smart cards complying with the new Federal Information Processing Standard (FIPS) 201 defining Personal Identity Verification (PIV) requirements must incorporate biometric data. ActivIdentity, Entrust, Lenel Systems, RSA Security, SafeNet and others offer such cards.

IP-LITERATE LOCKS, DOORS AND READERS

As smart cards generally have become standards-based commodities, a similar evolution is under way with card readers and other physical security devices.

"A card reader for the longest time has been a very mechanical device," says Qualcomm's Kelly. That company's inte-

When a physical security device is a network node, multiple devices can be managed and provisioned from the same, single point.

grated authentication solution required readers that could communicate with Qualcomm's logical systems. That's a requirement vendors are beginning to meet by rolling out IP-compliant readers.

And not just readers: Cisco Systems and global security firm Assay Abloy, which owns HID Global, have announced an initiative to make IP-compliant doors and locks.

"When everything becomes a network node, everyone's job gets a lot easier," says Stephen Pineau, CEO of Viscount Systems Inc. in Burnaby, British Columbia.

When a physical security device is a network node, multiple devices can be managed and provisioned from the same, single point. Further, the node can transmit data from a card swipe back to the network,

either activating or de-activating user authorizations. "You can get increasingly sophisticated solutions with that type of convergence," says ActivIdentity's Brandewie.

For instance, Qualcomm's Kelly hopes vendors soon integrate an IP-compliant motion detector and RFID so the combination can continually query and verify the identity of persons in a secure location and send alerts if an unauthorized person is present. "The technology is there; it's a matter of the software putting it together," he says (see box below). ☞

Sharon J. Watson (sjwatson@interaccess.com) is a free-lance journalist based in Sugar Land, Texas.

The Role of Software

With most smart cards and readers becoming commodities, today's key factor in choosing an authentication device is the value added by the software supporting it. Card management software must integrate easily with the enterprise's existing physical access control and identity management systems, including directory and/or human resources applications.

"Customers are looking for solutions that will ease business process flows," says Andy Solterbeck, general manager, commercial enterprise business unit, at SafeNet.

In particular, they want streamlined credential life cycle management. Most prospective customers find it a cumbersome, paper-intensive process today to activate and de-activate authentication devices, say vendors. The goal is automating the process so that one keyboard entry easily sets up authentication and authorization or cancels access across all physical and logical systems, including Web and virtual private network (VPN) ports, for a terminated employee.

To accomplish this, most card management systems act as bridges, conduits or gateways between and among physical and network access points and identification management systems that contain rules for provisioning and authorizing users. Built on standards-based, open architectures, vendors say their card management systems easily integrate with an enterprise's existing systems.

For instance, Lenel System's "credentialing agent" uses its

applications programming interfaces (APIs) to automatically query other enterprise databases when it is encoding smart cards. It also connects to existing physical access control databases. "You don't need all the data to be in a central repository," says Eric Larsen, senior product manager at Lenel.

Similarly, ActivIdentity offers open APIs and software development kits to integrate its card management system with other enterprise applications.

"Ours are plug-and-play connectors," says David Ting, chief technology officer at Imprivata. That company's solution maps user identities from various databases, then pushes an intelligent agent to desktops and devices that manages authentication.

Entrust's IdentityGuard is designed to be installed as part of an enterprise web infrastructure and uses standard web services for integration.

Oracle offers "connectors" between its identity management solution and physical access control systems. "Tying the physical system into HR improves the utility of the physical system," says John Heimann, director, security program management at Oracle.

That company's philosophy, says Heimann, is that authorization rules can be built into a human resources database and shared with a physical control system, so that when a card is revoked at the database level, all the physical security devices will automatically deny access to facilities or data.

— Sharon J. Watson

TAMRON
New eyes for industry



Tamron's on Duty — Tamron High Performance Vari-Focal Lens Series delivers high-quality monitoring images



f=3.0-8mm F/1.0



f=2.8-12mm F/1.4

High Resolution Vari-Focal Lens Series

1/3 2.8-12mm F/1.4
1/3 3.0-8mm F/1.0

All models in Tamron's high-performance, high-resolution lens series feature Tamron's independently developed Multi-Coating. The use of improved ND filters and aspherical lenses in these lenses — built on Tamron's 20 years of experience and performance in the development and manufacture of Vari-Focal lenses — puts Tamron at the leading edge of today's optical technology. Rely on Tamron's advanced optical technology for high-quality monitoring images.

Model lineup: 13VG2812ASII-SQ f=2.8-12mm F/1.4, 13VG308AS f=3.0-8mm F/1.0

www.tamron.com

Circle 205 on card.

and CSO at eFunds in Scottsdale, Arizona.

Jones himself is a rare breed, a CSO who has racked up years of experience in the traditional security field yet also has strong, firsthand knowledge of computing. After getting his degree in computer science at West Point, he spent ten years in Army intelligence.

Mastering Convergence

Some enterprises are mastering the art and science of convergence. The City of Vancouver, British Columbia, is one of them.

The city has moved its surveillance video archiving from magnetic tape to a storage area network (SAN) with 3.5-terabyte hard disk capacity. That should save the city some \$500,000 in storage costs over the next 5 years. Also, by training its security officers in IT policies, the city has seen a 90 percent reduction in violations of those policies.

For his leadership in the initiative, the city's CSO, Dave Tyson, received the first annual Excellence in Security Convergence Award from the Alliance for Enterprise Security Risk Management (AESRM) last fall. AESRM was created in 2005 through an alliance among ASIS International, the Information Systems Audit and Control Association (ISACA) and the International Systems Security Association (ISSA).

David Kent, vice president of security for Genzyme Corporation, and Dave Morrow, CISM, chief security and privacy officer for EDS, were the two other finalists for the award. AESRM received 33 entries.

Tyson, with an MBA focused on digital security management, is now readying a book on the subject, *Security Convergence & Managing Enterprise Security Risk*, due out this year.

— John W. Verity

His broad background, Jones says, "prepares me to take on both roles without short-shrifting either one. I understand camera placement, access control, dead-space analysis, fire and flood."

He's the first to admit that he's hardly a world-class computer programmer, but his IT training gives him a good leg up. "The best technologist can't BS me, and neither can the best physical guys," he says.

Most CSOs have come up through the ranks of physical security and therefore lack much immediate experience with and knowledge of IT technologies and issues. But reality is forcing them to catch up, if only to better manage the specialists they have reporting to them, whether directly or via a dotted-line relationship.

Further, physical security's video cameras and badge readers are connecting to their control points and monitoring stations—as well as to enterprise directories, identity management systems and human resources databases—via corporate networks that also carry Web traffic, email, internal data, even telephone calls. Because it's generally

professional with experience at Visa International, Fidelity Brokerage Co. and Bankers Trust. But two minds, he says, are almost always better than one, especially when it comes to identifying security holes in IT systems before they're exploited by bad-acting insiders or outside attackers.

If handled well, the natural tension between IT and security can be channeled into creative solutions. IT people, says Archer, tend to draw up a system design in a way that works right for the organization and then deploy it. The security department's goal, on the other hand, is to demonstrate gaps in the design that make it insecure. In the end, a good security organization and good IT organization can elevate each other's performance.

PICK-UP STICKS

"Think of it as a house of pick-up sticks," Archer says. "Security's always trying to pull one stick out and make the whole thing fall down. It's important to have people with different focuses."

"You don't necessarily need one indi-

Even as it uses ever-more sophisticated technology to battle would-be cyber-criminals, IT security must cope with serious new challenges that occur in the physical realm.

IT departments that operate those networks, video surveillance traffic may not always be given the priority it requires.

"These are turf wars that really have to go away," says Vance's O'Hara.

Meanwhile, even as it uses ever-more sophisticated technology to battle would-be cyber-criminals, IT security must cope with serious new challenges that occur in the physical realm. Sensitive information is getting loaded into all kinds of mobile devices, for instance—mainly laptops but also cell-phones and PDAs—and when one of them gets lost, stolen or misplaced, IT may fall short in critical skills in the areas of forensics and managing chain-of-custody.

THE BEST OF BOTH MINDS

"They have such different mindsets," says Jerry L. Archer, a longtime security

vidual [to run security] as long as you get the existing individuals to work together seamlessly," agrees Jones at eFunds.

Still, enterprises need formal policies and procedures that foster regular and constructive communications and collaboration between the two groups, all with the goal of driving "an overarching, holistic strategy that leaves no gaps in your security posture," he says.

Without such a strategy jointly hammered out and agreed to, Jones warns, "there may be too much ego and one area will get neglected."

In the end, he says, "convergence does make life easier. I have to worry less about coordination and buyoff among other security organizations."

Rhonda MacLean, a security consultant and former CSO of Bank of America, says



WHEN'S WORLDS CONVERGE

HOW SECURITY CAN WORK IN HARMONY WITH IT

By John W. Verity

Quarterly operations dispersed more globally than ever. Third-party outsourcing increasing exposure to new risks in new locales. Stolen laptops containing millions of customer records. Value shifting from hard assets to information, brand names and other intellectual property. The Wild Wild Web bringing more sophisticated attacks each day. Sarbanes-Oxley regulations looming over every activity.



Add to all this the usual budget pressures, and the challenge of keeping the global enterprise secure looks stiffer than ever. CEOs and their boards are scrambling to respond, with much of their energy focusing on what has come to be known as convergence: getting the traditional corporate, or physical, security department to team up and coordinate better with security specialists in the corporate IT division.

Identified as a trend only a few years ago, convergence has since become top-of-mind for a growing number of chief security officers (CSOs) and chief risk officers (CROs). According to an annual survey by PricewaterhouseCoopers, the portion of global corporations that had in some way integrated physical security and IT security has doubled in the past three years, from 29 percent in 2003 to 58 percent in 2006. Even more dramatic during that same time has been the near quadrupling of companies reporting they have both security groups reporting to the same executive, from 11 percent to 40 percent.

EASIER SAID THAN DONE

Unfortunately, as many companies have been discovering the hard way, successfully achieving convergence is easier said than done. Differing mentalities, reluctance among executives to surrender turf, inexperience, a lack of knowledge are among the many barriers. And, implemented improperly, convergence can actually make a company less secure than it was before.

“Convergence is definitely happening,” says Ray O’Hara, senior vice president at Vance International Inc., an Oakton, Virginia-based security consultancy and unit of Garda World

The chief security officer, the traditional head of physical security, often has years of previous experience in law enforcement, the military or intelligence. IT security people? They’re techno-geeks, and proud of it.

Security Corp. in Montreal, Quebec. “It’s just not happening overnight. Both sides still have a lot to learn from each other.”

Indeed, could any two groups be of more different mindsets? The chief security officer, the traditional head of physical security, often has years of experience in law

enforcement, the military or intelligence. IT security people? They’re techno-geeks, and proud of it. Where the CSO may have gotten to where he or she is by acting as an authoritarian, IT people often have a libertarian bent.

Their toolsets are light-years apart, too. Corporate security’s arsenal is heavy on the hardware: badges, cameras, good old-fashioned barbed-wire fences and even guards wearing guns. IT, in contrast, operates in a mostly virtual realm: hushed, darkened control rooms lit by flickering screens, arcane acronyms and soft, squishy tools like firewalls and packet sniffers. Where traditional security tries to identify, block and nab warm bodies, IT does battle with anonymous hackers and hoards of hijacked “zombie” computers.

With CSOs generally lacking in IT-specific experience and technical expertise, bridging the gap between these two groups calls for special attention.

“There’s a lot of misunderstanding out there,” says Larry Ponemon, chairman and founder of the Ponemon Institute in Elk Rapids, Michigan, which tracks corporate

security and privacy issues. “I hate to say it, but CSOs can be a little close-minded—old dogs aren’t always ready to learn new tricks.”

AN HOLISTIC SECURITY STRATEGY

But try they must, experts say, even if there’s no single formula for converging two disparate security disciplines into a seamless whole. The ultimate goal should be to create “an holistic security strategy,” but that has to be done in a way that fits each company’s specific culture and the talent it has available to it, says Kim Jones, senior vice-president

Insider Threats: A Management Disconnect?

Respondents reporting one or more insider-related security breaches within their company	78%
Respondents reporting lack of resources as a primary contributing factor to poor data security	93%
Respondents reporting lack of accountability as a primary contributing factor to poor data security	81%
Respondents who view insider threats as serious	89%
Respondents who think CEOs have the same perception	49%

Source: Ponemon Institute

Respondents Rank the Top Three Threats to Data Integrity

1. Missed or failed security patches on critical applications
2. Accidental or malicious insider misuse of sensitive or confidential data
3. Virus, malware and spyware infections

Source: Ponemon Institute

RFID & BIOMETRICS ACCESS CONTROL SYSTEM

Long Range Reader for Vehicle Control



- 2.45 GHz Long range reader (10 ft - 34 ft)
- Multiple Tags Identification (30 tags / sec)
- Directional Antenna for multiple lanes vehicles access
- 26bit Wiegand and RS232 Output Format
- Life Time Active Tags with Replaceable Battery CR2025
- Indoor / Outdoor installation
- * FCC, CE and RoHS Compliance

Finger Biometric Devices



- Standalone / Wiegand 26bit or higher output format
- Up to 4000 finger print users, 2 templates per user
- 4000 users for finger only mode support
- Card / Pin / Finger combination or any individual operation
- External reader port for Anti-passback
- Scratch proof optical sensor with high protection from ESD
- RS422, TCP/IP connectivity
- * UL, FCC, CE and RoHS Compliance

Proximity Readers / Cards



- 4"12"18" proximity readers
- Life time warranty
- Full vandal proof
- Indoor/Outdoor use
- Wiegand 26bit or higher / ABA Track II / RS232 output
- Reverse power polarity protection
- * UL, FCC, CE and RoHS Compliance

Standalone Proximity Reader



- Built-in 4" proximity reader and 512 users' capacity / 256 event buffer
- 2 TR output for door lock and 3 input for sensors
- RS485 (Max 255 units connectivity), 99 ports for TCP/IP support
- Indoor / Outdoor use and vandal proof
- Life Time Warranty and incredible low cost access control solution
- Event and alarm logs monitoring Software (Free of charge)
- * UL, FCC, CE and RoHS Compliance

Seamless CCTV Integrated Access Control S/W



- Displays event, alarm logs with graphic map and video clip files
- 30 fps real time video image / channel up to 16 cameras
- Web remote monitoring and control
- Web camera / 6 channel Web server / DVR integration
- PTZ settings and multiple monitors are available
- Add-on Software for Elevator control and ID badge printing

Two minds are almost always better than one, especially when it comes to identifying security holes in IT systems before they're exploited by bad-acting insiders or outside attackers. If handled well, the natural tension between IT and physical security can be channeled into creative solutions.

she advises clients to create and nurture "a culture of trust between physical and cyber-security guys. They need to talk or be together a lot. It's really important that the two disciplines work together in an end-to-end process, that there is leadership that makes sure all the dots get connected."

Organizational issues, such as whether IT security should report directly to the CSO, matter less than regular meetings. "I see it in terms of risk management, which involves security, business continuity and privacy," she says. "Sharing and strategizing and tactical planning are a must."

O'Hara at Vance takes the call for regular communications and collaboration a major step further. In this age of globalization, he says, security touches many corporate functions, and the CSO interested in full convergence may want to bring more voices to the table than physical and IT security.

For example, manufacturing is often outsourced to offshore producers, the corporation's value is held largely in the form of easily purloined intellectual property and supply chains have been stretched out to involve many different partners operating in myriad locations. In such cases, "information,

in all its forms, is probably more important to the company than who's coming over the fence," says O'Hara.

Therefore, the CSO and chief information security officer (CISO) should get together with "supply-chain people, manufacturing, sales people and brand managers, for all of them have a stake in managing the enterprise risk factor," he says.

What makes this wider conversation about security so critical, O'Hara says, is the growing complexity of the environments in which most large companies now find themselves doing business.

Take the common problem of tamping down gray market sales. It's not unusual for authorized distributors to order more goods than they can legitimately sell and then quietly unload the excess into unauthorized channels. To crack down on such activity, which can affect the value of a brand, profit margins and relationships with key partners, a producer will often respond by being more aggressive in enforcing the contracts it has with the offending distributors. That will likely call for the security department to nail down certain investigative documentation. But as

the gray market activity gets shut down, the company may see a decline in overall sales volume. Therefore, O'Hara says, it's advisable to give the sales department - among others - a say in resolving what turns out to be largely a security issue.

CSOs can benefit from not only improved familiarity with IT but with business issues as a whole, says Tom Cavanagh, a senior research associate in Global Corporate Citizenship at The Conference Board in New York City, a management consulting firm.

"It would be helpful to have an MBA and management experience so you know how to contribute to business value," he says. "Most security guys know how to run a checkpoint or clear a building, but they're at sea with broader business concerns."

And instead of viewing security merely in terms of defense, business managers ought to see it as an enabler that can help them take advantage of opportunities without incurring undue risk. As Cavanagh sums it up, "Don't tell me no, tell me how."☞

John W. Verity (john@jverity.com) is a freelance writer based in South Orange, New Jersey.

The Information Life Cycle

A major factor underlying the drive for better-integrated security strategies is the notion of the "information life cycle."

This cycle begins the moment a document is created, say, on a PC, and stretches to cover its editing process, its distribution to an intended audience, its storage in a long-term archive, its disposal in a shredder. A comprehensive security plan will include policies for protecting different classes of documents at each stage of their life cycles, no matter if they're stored on a data center's hard drive or in a salesperson's laptop, printed on paper, displayed on a screen, sent over a network or copied to CD-ROM or memory stick. The format, physical or logical, doesn't matter. It's all a matter of information security.

The Most Advanced IP Video Surveillance Solution. **Period.**

Megapixel and Universal Camera Support



Intelligent Video Delivery



Advanced Content Analytics



Multiple Video Clients



IP Video Wall Matrix Switch



Open Systems Integration



OnSSI. Connecting the Dots.

Visit us at ISC West, Booth #8075

Circle 208 on card.



OnSSI

Intelligent IP Video Surveillance and Delivery



Video Rides — the Bus —

CALIFORNIA'S Foothill TRANSIT DEPLOYS NETWORKED SURVEILLANCE SYSTEM

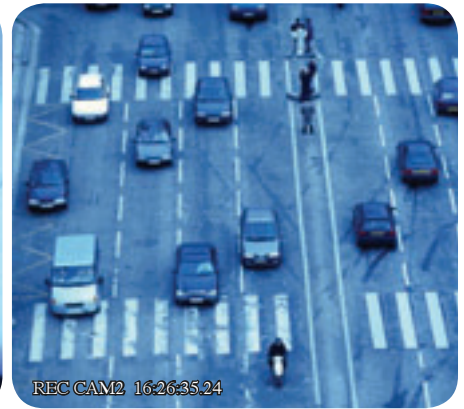
By Phil Britt

Foothill Transit, the second-largest fixed-route bus system in Los Angeles County, California, is installing an Internet Protocol (IP) networked video system from Verint Systems Inc. of Melville, New York, that manages cameras and DVRs throughout its fleet, using Ethernet networks, high-speed wireless connections and video analytics.

The American Public Transportation

Authority (APTA) estimates more than 14 million people use public transportation each weekday. State and local transit authorities around the country are investing in video surveillance to proactively address security threats, promote optimal response in emergency situations and mitigate the risk of liability claims through more comprehensive incident investigation.





Take It All In. Remember Everything. The Seagate SV35 Series Video Surveillance Drive.

Empower your video surveillance systems with the Seagate® SV35 Series® drive—the first hard drive engineered and optimized for video surveillance applications:

- Records multiple data streams
- Stores months of footage
- Capacities up to 750 GB
- Runs 24x7xPracticallyForever

Hard drives are replacing tape as the industry's storage medium of choice. Smart move. The SV35 Series drive turns that smart move into a stroke of genius with unsurpassed capacity, performance and reliability.

Visit spp.seagate.com to become a Seagate Partner Program member and learn why the SV35 Series drive is a must for your next surveillance project.



Get more security-focused storage information by visiting specials.seagate.com/frames/ncm



“Video will be everywhere in the next 10 years,” says Joe Freeman, an independent security analyst based in Newton, Connecticut. “It’s being used increasingly in train stations, on school buses around the country and also for pedestrian traffic. What we’re looking at is protection of the public wherever they are.”

“SMART BUS”

For Foothill Transit, its video system is a critical element of its “smart bus” program designed to give better service to its almost 15 million customers per year in the San Gabriel and Pomona Valleys.

Foothill’s fleet of 314 buses covers a route system of 327 square miles. With increasing congestion on the roads and highways its vehicles travel, it became critical that Foothill Transit increase the efficiency of its fleet operations, including its surveillance capabilities, according to Doran Barnes, Foothill Transit’s executive director.

Barnes says the bus company chose IP video for its ease of use: the open platform permits easy networking within the video system as well as integration with other security applications that use the protocol.

“The video [surveillance] system is part of our ‘smart bus’ program, which includes global positioning systems, vehicle locator technology, global positioning equipment [and] automating of dispatchers and coach operators,” he says.

Working with an outside consultant, Foothill Transit began by conducting a needs assessment in late 2004. Selecting a solution took nearly two years as the agency identified its needs, sought contractors, made its purchase decision and began installation. Implementation started in November 2006 and is expected to be completed by the

end of the first quarter of 2007.

BETTER IMAGES

Foothill wanted to avoid the grainy, black-and-white, poor quality video common in many convenience stores. These cameras might serve as a deterrent in some cases – just knowing one is under surveillance can prevent some crimes – but are far too poor in quality to use in many litigation cases.

Agency officials sought a system that first and foremost offered a user-friendly search

however, Buchko says, “Verint offered a better value proposition.”

The Verint system itself is a component of Orbital’s OrbCad system, which includes computer-aided dispatch, automatic vehicle location systems and related technologies for monitoring and control of fleet resources in real-time. Foothill Transit is one of about 20 transportation systems with the OrbCad system. Other Orbital customers include Los Angeles County, Tri-Met in Portland, Oregon, and the Denver Regional Transportation District.

GROWING USE

The video system for Foothill Transit is one of only a handful that Orbital has installed so far, but several more could be forthcoming, says Buchko. “It’s in all the requests for proposals we get now,” he says.

The main reason for the increased interest in digital video surveillance systems, Buchko says, is 9/11 and the July 2005 bombings of the London transit system. Installation of security cameras is one of the

APTA’s suggestions for

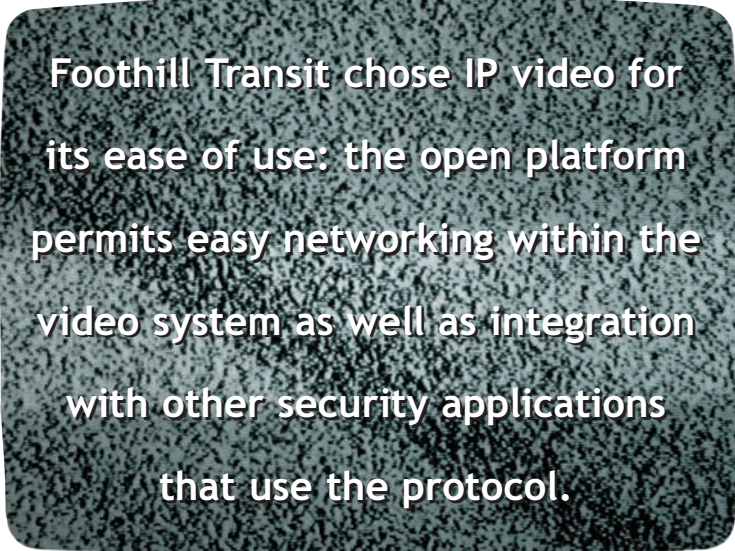
low-cost ways to deter terrorism.

Another reason to add video systems to bus fleets is protection from legal liability, says Freeman.

According to the Federal Transit Administration, there were 6,802 collisions involving buses in 2004, the last year for which full statistics are available. Data reported includes about 560 of the largest transit agencies. The more accurately such events can be documented, the more public agencies can protect themselves in today’s litigious society.

“There’s been a huge increase in parents’ lawsuits [for school bus incidents],” Freeman says.

Also, if the contractors who operate the buses can keep their initial insurance



Foothill Transit chose IP video for its ease of use: the open platform permits easy networking within the video system as well as integration with other security applications that use the protocol.

function. Also important was the ability to provide quality video in low-light conditions, such as overcast days, and at night.

Foothill looked at packaged offerings (video, GPS and other components) from three contractors, including the eventual contract winner, Orbital Sciences Corp.’s Transportation Management Division based in Dulles, Virginia. Orbital offered the Nextiva video system from Verint.

Orbital had another video technology option, according to Chris Buchko, the company’s program manager, but had no bias toward either. Orbital previously had installed a similar networked video system for the Los Angeles County Metropolitan Transit Authority. For Foothill Transit,

and liability costs lower, Foothill Transit benefits by receiving lower contractor fees, say system officials.

SAFETY DRIVE

Safety was another concern, according to Barnes. The video, which is linked to a g-force sensor on each bus, can show near-misses as well as actual accidents, so it can be used to help in safety training.

"We have a strong commitment to safety," Barnes says. The APTA recognized Foothill Transit in 2001 with its "Bus Safety Gold Award," dubbing the transit agency the safest of its size. The Greater Los

Any time a driver exceeds a certain g-force, the video is tagged so that the five minutes before and five minutes after the event are locked on the removable drive and can't be recorded over until reviewed by Foothill officials.

Angeles chapter of the National Safety Council gave Foothill Transit first place awards for the agency's safety programs in 1995, 1996, 1997, 1998 and 2001.

Foothill also wanted to ensure efficient operations for its transit system. "We needed the technology to maintain the effectiveness of our system," says Barnes.

The video system provides a comprehensive picture of activity in and around each vehicle. Each bus has six cameras, all mounted inside the vehicle. One is focused on the bus operator and front door. One mounted on the windshield looks out the front window; another in front looks to the back of the bus. One near the rear

door and two more in the back of the bus look outside.

The cameras are hardwired via Ethernet connections to a digital video recorder on each bus. The recorders store information on internal removable drives locked in cabinets on each vehicle accessible only by authorized personnel, says George Karbowski, Foothill Transit director of operations.

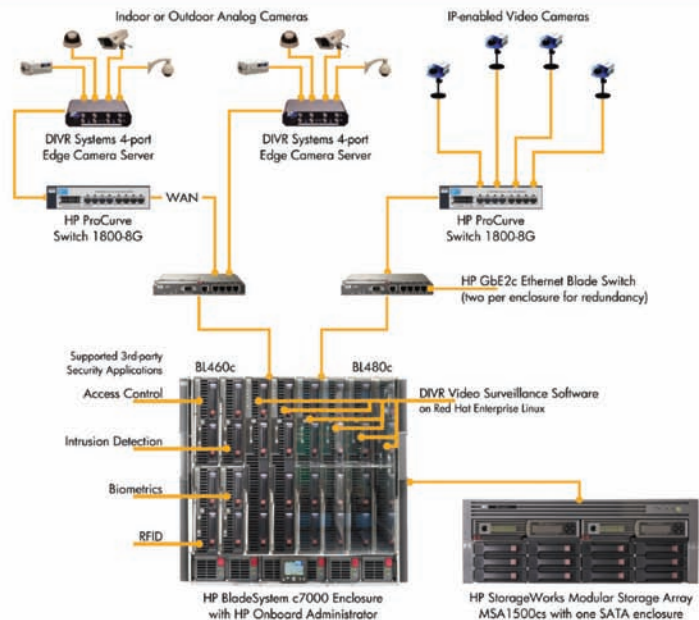
The recorders store seven to eight days of video before the removable drive needs to be changed or recorded over. The recordings themselves are "snapshots" of actual events, unless automatically tagged by the g-force monitoring system or tagged by the operator himself as the result of "internal incidents" such as fights or vandalism.

The video is integrated with the g-force monitoring system on each vehicle. Any

Network-Integrated Video Surveillance on HP BladeSystem



Clearly superior surveillance technologies from HP, Blade Network Technologies®, and DIVR Systems, Inc.



Rising security concerns are accelerating the need for enhanced, proactive network-integrated digital video surveillance solutions that take advantage of the latest computer, network, and storage technologies. But doing so without negating investments in legacy analog surveillance systems has been a serious challenge—until now. To learn more about moving to the next-generation of video surveillance or to tailor a solution for your organization, contact your HP representative, visit www.divrsystems.com or call (661) 393-5546 extension 4.



HP BladeSystem
Solution Builder



© 2006 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Mobile fleets are a little trickier than stationary locations because they require good, stable wireless connections for real-time monitoring.

time a driver exceeds a certain g-force, the video is tagged so that the five minutes before and five minutes after the event are locked on the removable drive and can't be recorded over until reviewed by Foothill officials. In the event of an accident or near-accident, this makes it easy to locate video that shows exactly what was going on inside and outside the vehicle at the time of the incident.

If there are any incidents, the tagged

video is downloaded in one-minute bursts via a 1 megabit per second (Mb/s) wireless connection when the bus pulls into Foothill Transit's dispatch area.

Because installation of all units wasn't to be completed until early in 2007, it's still too soon to determine actual benefits, according to Barnes. But he expects the system to produce lower long-term costs for the agency because contractors will limit their own liability costs and have

better proof of innocence in the event of a dispute.

There are no immediate plans to make real-time, live video available directly from the cameras to the corporate office, though Buchko says that would be the next logical step. ☞

Phil Britt (spenterprises@wowway.com) is a free-lance writer based in South Holland, Illinois.

En Route to Digital Video

Even before the events of 9/11, legal liability, vandalism, crime deterrence and investigation were all valid reasons for installing video surveillance equipment. Now the rise in the use of these systems is as much due to the technology as it is to the need for better surveillance.

"With IP, it's become possible to connect all security devices to the same IT backbone," says Joe Freeman, a security analyst. "This does it in a way that maximizes efficiency."

Traditional video technology, common in convenience stores and other locations, requires the cumbersome process of reviewing hours of video tape.

Digital video surveillance systems, however, work much like the popular TiVo consumer devices, enabling a business or public agency to monitor remote locations from anywhere, anytime. Mobile fleets are a little trickier than stationary locations because they require good, stable wireless connections for real-time monitoring. More common is the system that Foothill Transit uses, where fleet vehicles pull into a central location to transmit video wirelessly or to change a removable drive.

With a digital remote surveillance system, there is no need to change video tapes – the removable drives can be recorded over if nothing needs to be saved. Digital systems also provide crystal-clear picture quality and a digital stamping system that enables a viewer to quickly go to an exact time on the

recording, rather than spending hours trying to first find the correct video tape, then the right spot on the tape.

In addition to Foothill Transit, Verint's systems are used by 10 government agencies, 20 seaports, 25 cities, 55 major airports and numerous mass transit systems and U.S. banks. The company's transit customers include Valley Transit Authority, Santa Clara, California; Ft. Worth Transit Authority; Montreal Metro; London Underground; the Long Island Railroad and JFK AirTrain in New York; and the Los Angeles, Dulles and Orlando international airports.

The Verint DVRs can send images to multiple monitors on a rail car or bus, giving operators real-time visibility to activities throughout the vehicle. Verint provides video monitors from 5 to 15 inches that include the ability to handle changing light conditions and are designed to handle the motion in a fleet environment.

Users can plug the removable hard drives into a docking station or transmit selected video via a wireless local area network or digital cellular.

Verint solutions support Vehicle Area Network communications over Ethernet, RS-232/485, J1708, CAN and IBIS, with options for both 802.11 and GSM/GPRS wireless communications. Verint solutions also support high-speed communications through railroad trains via the Verint Train Video Network and analog communications for retrofitted trains via the Verint Train Video Coupler.

— **Phil Britt**



defuse **DISASTER**

CPM delivers a training experience unlike any other. Learn to defuse any disaster that rears its ugly head.

Sessions include:

- Pandemic Influenza: The State of the Threat
 - Establishing Mission-Critical Employee Programs
 - Data Security in a Distributed World
 - Disaster Simulation Exercise
- And many more!

Register Now!

www.ContingencyPlanningExpo.com



The Mirage • Las Vegas, NV • May 22 – 24, 2007

Circle 210 on card.



Applications, Strategies, Solutions



1 Axis Video Server Blade

Axis Communications has unveiled a video server blade and rack solution for professional surveillance installations. The combination is designed for use in any professional security application that requires the conversion of analog video to digital. The Axis 291 1U Video Server Rack holds up to three interchangeable Axis blade video servers and includes a built-in gigabit switch. The Axis 243Q Blade Video Server is specially designed for the Axis 291 1U rack. It converts video signals from up to four analog cameras into full frame rate, de-interlaced digital video that can be viewed via an IP network.

www.axis.com

2 Tamron IP Camera Lenses

Tamron has introduced a line of improved high-resolution vari-focal lenses for IP cameras. The new models 13VM2812ASII and 13VG2812ASII have improved mechanical constructions to optimize optical performance. Each employs aspherical elements to provide clear, high-contrast images over the entire focal length range.

www.tamron.com





3 DIVR Client Monitoring Station



DIVR Systems' thin client monitoring station (TCMS) is a Linux-based system dedicated to driving LCD panels to display live video surveillance images. Used in conjunction with DIVR's IP video surveillance solution, it can also support IP-based camera applications compatible with the Firefox web browser. www.divrsystems.com

4 Lantronix IntelliBox

Lantronix's IntelliBox I/O 2100 with EventTrak technology provides a new level of control over remote industrial equipment. With secure access, the IntelliBox proactively monitors and controls remote digital input/output, dry contact and RS232 or RS422/485-based industrial equipment. When an event occurs, IntelliBox responds with user-defined policies. This provides an unprecedented level of flexibility to monitor and manage industrial I/O devices.

EventTrak technology allows end users to program the device server to respond to external events automatically, such as by rebooting or reconfiguring attached equipment. It will also log events as detected and repaired through automated reporting and email notification.

www.lantronix.com



5 OnSSI Partners with S2

On-Net Surveillance Systems (OnSSI) has formed a strategic partnership with S2 Security Corp. for the integration of OnSSI's surveillance NVR and intelligent video delivery platform with S2's Netbox integrated physical security management system. With the integrated S2 and OnSSI system, video surveillance will correspond to events detected by a range of physical security devices, including access control, alarm monitoring and temperature monitoring. Because the system will attach video to each unauthorized access attempt or perimeter security breach, it will eliminate the need to search for and match video content to security exceptions.

www.onssi.com www.s2sys.com



6 RF Logics Biometrics Access Control

RF Logics' LX007 series offers a built-in controller with TCP/IP communication support for door access control and time and attendance logging. The device operates in 125 KHz or 13.56 MHz modes. The controller can register up to 4,000 fingerprint users and can store up to 10,000 IDs and 20,000 event transactions. Isolated I/O definitions given to each ID enable fully customizable features such as disability access. In addition to hardware upgrades, the new LX series features intuitive, easy-to-use management software integrated with web browser connectivity.

www.RFLogics.com

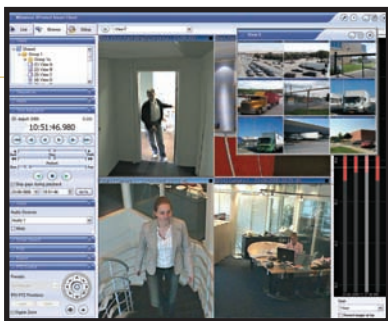




7 Trango Wireless Network Ring

Trango Broadband Wireless' HD Mesh is a self-healing, high-capacity wireless network ring ideal for transmitting IP-based broadband video and data. The highly secure ring incorporates multiple backhaul frequency options including 5.3/5.8 GHz unlicensed and the 4.9 GHz licensed bands for public safety, first responders and homeland security. Up to 45 Mb/s throughput; up to 40-mile range; includes a 6-port router and built-in 802.11a/b/g hotspot.

www.trangobroadband.com



8 Milestone XProtect Corporate

Milestone Systems has launched XProtect Corporate, a premium IP video surveillance solution with centralized management designed for large multi-site and multiple server installations. The solution offers centralized management of IP cameras, servers and other devices from different vendors with an extremely flexible rule system driven by schedules and events. Its distributed server architecture allows unlimited recording and archiving of video data. The software also features an application program interface for integration with third-party systems. Full-fledged client access provides live view, playback and video evidence export with smart search and analysis, all operated through a multiple computer-monitor interface.

www.milestonesys.com

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.

exacqVision Pro exacqVision IP

Advanced IP Video Surveillance Solutions



- Software Packages
- Hybrid Systems (analog and IP)
- NVR Systems

Entire line is completely Scalable

exacq
Technologies

317.845.5710

www.exacq.com

Need wireless IP video?

My security command center is here.

I need surveillance cameras here.

No problem, call Trango! Your source for wireless IP video solutions.



IP Video & Data Network *Self-healing Broadband Backbone Ring*

- » Full-motion video @ up to 30 fps
- » Up to 45 Mbps, up to 40-mile range
- » Frequency options: 2.4 GHz, 4.9 GHz, 5.3 GHz, 5.4 GHz, 5.8 GHz, 900 MHz
- » Built in 802.11a/b/g hotspot

Remote Video & Data Applications

- » Homeland Security
- » First responder video & data connection
- » Municipality video & data connection
- » Parking lot surveillance
- » Freeway and city traffic monitoring
- » Port/harbor/airport security monitoring
- » Public safety parks monitoring
- » Construction site monitoring
- » Industrial/plant surveillance
- » Campus/complex monitoring
- » Railroad monitoring
- » Military installation perimeter security



NTSC/PAL Video

- #### *Analog Wireless Video Systems*
- » Full-motion video @ 30 fps (2.4 & 5.8 GHz)
 - » 1 to 7 mile systems available
 - » Video, audio and data transmission
 - » Control fixed and pan/tilt/zoom cameras
 - » Multiple channels for maximum flexibility

For wireless security solutions, visit:

www.trangobroadband.com/SECURITY

or email: SECURITY@trangobroadband.com

WWW.TRANGOBROADBAND.COM

Trango Broadband Wireless
A division of Trango Systems, Inc.

San Diego, CA
+1 (858) 653-3900
SECURITY@trangobroadband.com

Circle 212 on card.

Made in the U.S.A.





Getting the CEO's Attention

by Joseph P. Freeman, Sc.D.



One of the most difficult challenges for today's security users is getting senior management to pay attention to the serious issues affecting the continuity of a well-managed enterprise.

Anyone with physical security experience knows that the challenge of attention-getting is now more serious than ever. Management was once comfortable with guard services patrolling a facility's sensitive areas after closing time, and since everyone else was trusted, that was the security program. Meanwhile, PCs, modems, routers, servers, coax and fiber became powerful information conductors in the organization, and management invested lots of money in IT resources without too much immediate concern for security of the "sensitive" areas they had created in the virtual world.

As the trust factor declined, knowing who was where, accessing what asset, looking at what information, became more difficult to determine. Yet all the while, the security management function continued to be a little like the sales chart—unless the trend line turned down, management paid little attention. So how do we capture management's interest in something that protects life, assets and even cash, yet is so difficult to evaluate that it draws little interest? Here are some tips for the chief security officer to consider—especially when it's time to invest corporate funds in program upgrades.

COMPLIANCE

There are lots of regulations to deal with today, from state and local mandates to the Securities and Exchange Commission (SEC) and Sarbanes-Oxley. If the security budget needs new funding to comply with new "regs," the CSO should call for a meeting to inform the corporate finance committee of the investment requirements. The message here is that compliance is not an option. It protects the firm against legal as well as physical attack.

ACCURATE RISK ASSESSMENT

Risk assessment is not an exact science. Nevertheless, it affects the premiums that organizations pay to their insurance carriers. Yet communication between CSOs and insurance carriers is often limited. If CSOs are brought into the risk assessment process, there could be significant savings in more coordination between the presence of threats and the methods of countering them.

IT USE

Management often overlooks the security department as a major user of company information technology. Yet today it can be clearly documented that strategic integration of security and IT can produce significant savings in security department operating costs while simultaneously raising enterprise protection levels. After all, wasn't productivity the whole spending rationale for the IT department? Security is not just guards and mechanical locks any more.

cont. on p. 34



EX96000 Series

**8-port 100Base Fast Ethernet
and 1-port Gigabit Hardened
Managed Switches**

Ethernet Connectivity Everywhere



EX9224SF Series

**24-port 100Base-FX with up to 2-port
Gigabit Hardened Managed Switches**

Circle 213 on card.



EtherWAN

EtherWAN Systems, Inc.

4570 E. Eisenhower Circle Anaheim, CA 92807

Tel : (714) 779-3800

Fax : (714) 779-3806

E-mail : info@etherwan.com

www.etherwan.com

The CSO needs to show management a technology plan with budget requirements in order to secure the funding for a highly productive technology-based enterprise security process.

ENTERPRISE "SENSITIVITY"

Banks, insurance companies, chip manufacturers, nuclear power stations, defense suppliers and the like have traditionally been regarded as "sensitive" enterprises with particularly strong security programs and well-trained CSOs. But 9/11, wars in Iraq and Afghanistan, insecure southern borders, unprotected seaports and a generally more nervous world now make everything "sensitive." As a matter of good governance, every CSO should be sending regular reports throughout the organization about new risks and the importance of extra care in dealing with "sensitive" assets like controls, databases and protected information. Managed well, security should not be secret and totally invisible, but routinely reinforced to remain in every employee's mind.

EMPLOYEE AWARENESS AND PARTICIPATION

Every employee has a stake in a productive firm and a safe working environment. How about a short, friendly security awareness bulletin sent by email once a month? During World War II, President Franklin Roosevelt had signs installed in front of every post office in America. Slogans like "Loose lips sink ships" reminded the citizens that information has value. It might not be the CSO's most polished professional discipline, but the employee communications department can help. In addition to getting employees on board the security program, it would also create management awareness and very possibly pave the way for a requested meeting.

PRODUCTIVITY AND COST CONTROL

Two of the most magical words to senior managers are cost reduction. Jack Welch produced earnings increases

of 5 percent for years largely through cost reductions. Departments in all enterprises are annually asked to recommend cost reductions to improve corporate productivity and earnings. The security department now has a big one available in the form of security/IT convergence. It's more involved than people think, and the fastest way to understand it is through a membership in the Open Security Exchange. OSE resources can help CSOs create a comprehensive management presentation for funding to modernize a firm's security program while showing how costs can be reduced. The savings are significant, so a grasp of return on investment (ROI), technology and teamwork with IT managers are musts before asking for the meeting.

LIFE SAFETY AND ASSET PROTECTION

Security and protection will be more vital as growth in the global marketplace is accompanied by new international tensions. If management doesn't understand the subject, help them gently along. While it's true that security contributes nothing to sales, it does prevent possible interruptions to sales. And it definitely contributes to earnings when all the technologies now available are used in conjunction with good security management prac-

tices. Your work is no less important than the human resources, legal and facility departments.

Getting face time with senior management can be difficult when the subject is poorly understood and regarded as unexciting. Many senior managers fail to see how a sound security business process can contribute to shareholder value—until its protective design is clearly juxtaposed with the rising risk premium that every enterprise in the industrialized world now pays for asset replacement and legal vulnerability.

Your claim on management time can address all or any of the topics above. Threats are present 24/7/365, employee awareness is important and management should know how you protect them and what they can do to help you stay current, if not on the cutting edge. On Wall Street they say "buy on the rumor and sell on the news." You may have to buy the meeting by publicizing new threats in order to sell the funding for new protections. However you do it, getting that meeting is a major responsibility. ☺

Joe Freeman (info@jpfreeman.com) is CEO of J.P. Freeman Co. and J.P. Freeman Labs (www.jpfreeman.com), providing research, consulting and product testing services. New 2007 Reports include: Intelligent Video & Smart Cameras, IP & Network Video and the Convergent Systems market.

LINKS A navigational guide to **advertisers** & companies mentioned in *Network-Centric Security*

ActivIdentity Corp.actividentity.com	Milestone Systemsmilestonesys.com
AvaLANavalanwireless.com	Motorolamotorola.com
Axis Communicationsaxis.com	Novellnovell.com
Boschboschsecurity.us	onSSIonssi.com
Cisco Systemscisco.com	Oracleoracle.com
Cryptolex Trust Systemscryptolex.com	Pelcopelco.com
DIVRdivrsystems.com	Ponemon Instituteponemon.org
DSXdsxinc.com	Qualcommqualcomm.com
Efundsefunds.com	RF Logicsrflogics.com
EDSeds.com	RSA Securityrsa.com
Entrustentrust.com	SafeNetsafenet-inc.com
EtherWanetherwan.com	Seagateseagate.com
Exacq Technologiesexacq.com	Trangotrangobroadband.com
Firetidefiretide.com	Tamrontamron.com
HIDhidcorp.com	Tropos Networkstropos.com
Honeywellhoneywell.com	Vance Internationalvanceglobal.com
Imprivataimprivata.com	Verintverint.com
Inscapeinscapedata.com	Viscount Systemsviscount.com
JPFreeman.comjpfreeman.com	Zebrazebra.com
Lenellenel.com	

THE MOST POWERFUL ACCESS CONTROL ON THE PLANET!



DSX Access Systems, Inc.
Creators of powerful access control systems that are considered to be the finest in the industry.

DSX products are engineered for rock solid stability and ease of operation. WinDSX is capable of monitoring one door or an enterprise wide system of thousands of doors.

Our WinDSX software, coupled with the DSX 1048 state-of-the-industry panels, provide the ultimate in user-friendly operation and service.

When you're ready for the most powerful access control on the planet... there's only one place to call.

- Threat Level Management
- Hot Swap Redundant Comm. Server
- Time Zones Controlled with Linking
- High Level Elevator Control Interface
- Digital Video Recorder Integration Network
- LAN/WAN Compatible
- Integral Photo ID Badging
- Unlimited Access Levels Per Cardholder
- Smart Access & Biometric Integration
- Global Access Level Manager

Quality. Reliability. Integrity.
The Security Professionals'
First Choice.

DSX Access Systems, Inc.

10731 Rockwall Road ▾ Dallas, TX USA 75328-1219
1-888-419-8353 ▾ 214-553-6140 ▾ Fax: 214-553-6147
E-mail: sales@dsxinc.com ▾ www.dsxinc.com

Circle 214 on card.

Easy to install

+

Phenomenal security

+

Same price as prox

+

Genuine HID

=

No brainer



hidcorp.com

Starting access control customers with iCLASS is more than smart. It's obvious. It's as easy to install and use as proximity. Its additional authentication features offer far greater security. Its read/write capability opens the door to new applications as your customers grow. And it costs the same as proximity. That makes everyone look smart.



ACCESS the new prox.

iCLASS

Circle 215 on card.

Please visit us at ISC West, Booth #13051