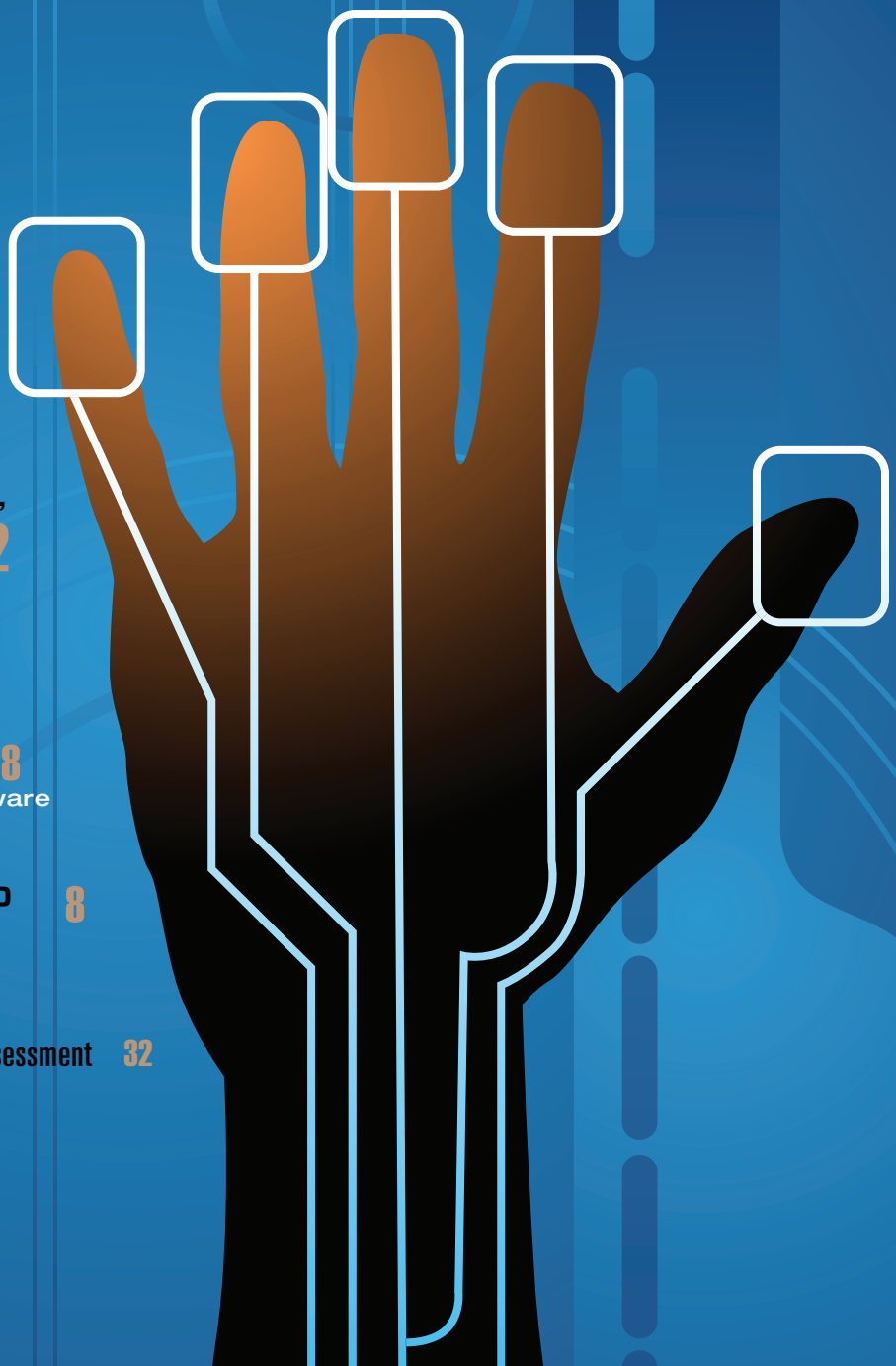
network centric Security

August 2008

WHERE PHYSICAL SECURITY & IT WORLDS CONVERGE

FEW FINGERS IN THE MIX

Biometrics stars in niches, not network 12



UNCOMMON PLATFORMS 18

Can IP video management software be the same, but different?

MASS NOTIFICATION MEETS IP 8

Here comes NFPA 72

PLUS

Converging Physical and Cyber Risk Assessment 32

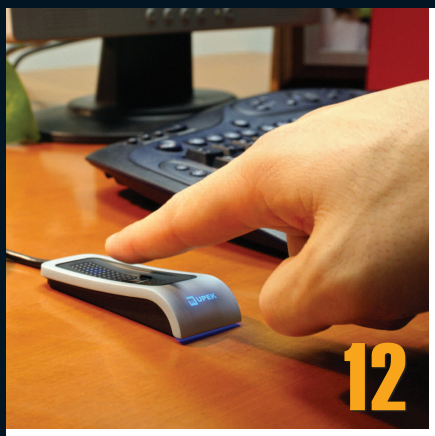
August 2008 Supplement to *Security Products*

network centric Security
WHERE PHYSICAL SECURITY & IT WORLDS CONVERGE

Content

AUGUST 2008 VOLUME 2 NO. 4

features



FEW FINGERS IN THE MIX

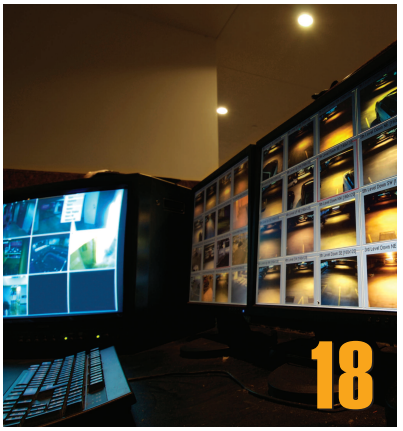
By Sharon J. Watson

Biometric technology is no longer the stuff of science fiction or high-tech thrillers. The technology for using a person's unique biological markers to offer irrefutable proof of identity or presence in a specific place at a specific time is functional, marketable and increasingly sophisticated. That's the good news for biometrics fans. The sobering side of the story is that commercial enterprise users apparently are finding only limited uses for the technology.

UNCOMMON PLATFORMS

By Steven Titch

Can IP video software be the same, but different? End users, while seeking surveillance solutions that can integrate a broad range of cameras and edge devices, balk at platforms perceived as too generic. So video system suppliers are jockeying to differentiate themselves in new ways: by touting the superiority of their underlying technology, by playing to specific strengths in IT networking, by offering a tighter knit with other platforms, such as access control systems and analytics, or any combination of these methods.



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.

Casinos Bet on the LAN

by Steven Titch, Editor

The casino business is the only industry outside the military and defense sectors in which physical security gets as much—if not more—attention as any other business process, and it's showing us how IT is beginning to influence the security procurement process.

Harrah's Entertainment; Las Vegas Sands, owner of the Venetian; and Wynn Resorts have all recently announced top-down IP networking projects that treat security as part of a much larger business process aimed at improving the overall guest experience.

As described in "Uncommon Platforms," beginning on page 26, the Cisco-Harrah's deal involves the implementation of a large-scale next-generation IP video security infrastructure. But that is only part of the deal. The upgrade will support new "smart services" aimed at enhancing a guest's experience from check-in through check-out. For example, video will monitor the length of lines at valet parking and registration desks. That real-time information will be used to dispatch personnel where needed.

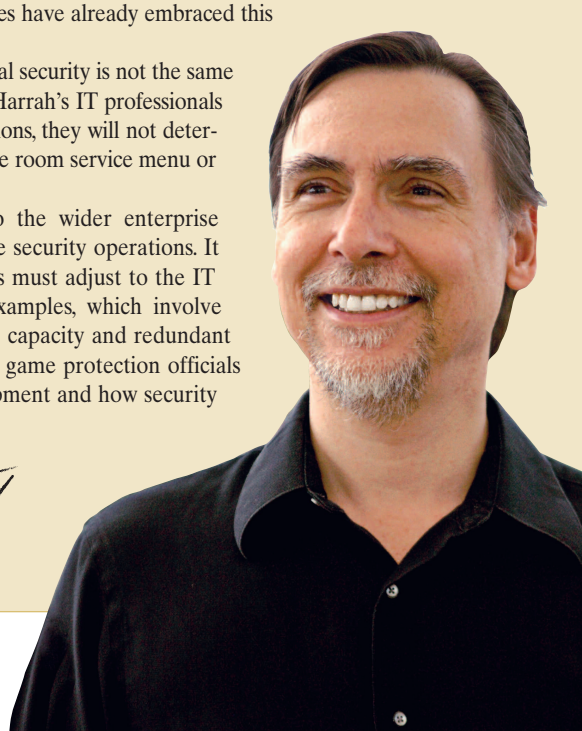
Much of the Harrah's plan is still on paper, and it will be some time before the upgrades are in place and results can be measured. Still, it's a comprehensive template of the IP-based security integration that's already begun.

Hewlett-Packard's ProCurve unit is building a new IP backbone for the Venetian and its new sister property, the Palazzo, that will pull together security, marketing and guest operations. Meanwhile, Honeywell is prime contractor for a similar project for the existing Wynn property and new Encore hotel, set to open at the end of this year.

The general trend toward IP and local area network integration has led many industry observers to say physical security operations will be merged into corporate IT operations, as happened with telecommunications and data processing. Some enterprises have already embraced this notion, but they may be doing so at their peril.

It's subtle, but saying IT should support physical security is not the same as saying IT should run physical security. While Harrah's IT professionals will support guest services and marketing operations, they will not determine the number of VIP check-in desks, select the room service menu or set the point structure for comps.

Without doubt, linking physical security to the wider enterprise network will create more robust and responsive security operations. It is the future, and physical security professionals must adjust to the IT environment. Yet, if we look at the Vegas examples, which involve thousands of surveillance cameras, high storage capacity and redundant servers and CPUs, it's clear casino security and game protection officials retained a powerful voice in the choice of equipment and how security applications will run.



Mass Notification Meets IP

by Steven Titch

There was a time you could set your watch by it. Throughout the Cold War years, every Friday at 1 p.m., towns across America tested their air raid sirens. It was an exercise in basic mass notification.

Mechanized sirens and large public address systems—so-called "great voice" platforms—remain the model in many communities today, in most cases for natural emergencies such as tornadoes and tsunamis. And fire drills are still *de rigeur* in schools and offices.

But as modern threats take in more than large cataclysms that require evacuation or movement of a large group of people, emergency planners and responders are looking at the flexibility and pervasiveness of IP networks as a robust vehicle for mass notification.

The National Fire Protection Association is accepting comments on a revision of NFPA 72, the section of the national fire alarm code that covers the integration of mass notification and fire alarm systems. The new code, known as Chapter 12, would set the procedures that would allow emergency responders to supercede the fire alarm system to give priority to mass notification and emergency communications. Comments are due Aug. 29.

The revision, which would become part of NPFA 72 in 2010, is not controversial. On the contrary, responders and manufacturers welcome the addition and are preparing for the introduction of a number of mass notifications systems and components that will use IP.

UFC 4-021-01

Chapter 12 will essentially merge current NFPA standards with the Department of Defense's Universal Facilities Criteria 4-021-01 document, which lays out the military's specification for IP mass notification, says Wayne D. Moore, chairman of the Chapter 12 working group and principal with Hughes Associates, Baltimore, which specializes in fire protection design and consulting. In an emergency, mass notification will be allowed to take over a fire alarm system with appropriate risk analysis, Moore says.

"Will it be for announcement of class changes? No. In the case of a shooter? Yes," he says.

While emergency planners have been wrestling with modernizing mass notification systems since 9/11, recent incidents, such as the shootings at Virginia Tech, where responders could not collect accurate information and relay proper instructions to students, teachers and university employees, helped galvanize action.

IP-based mass notification gives responders the ability to use different methods—"great voice,"

NFPA 72 Chapter 12 will define eight major tasks IP-based mass notification systems must handle.

They are:

- Recorded messages
- Live messaging
- Fast messaging
- Visual display
- Strobe control
- Local event log
- Local diagnostics displays
- Relay local diagnostics to a control center

> ‘Open protocol is the future of mass notification’
>
> —Jim Mongeau, Space Age Electronics

e-mail, text messaging and video—to promulgate instructions, says John Weaver, marketing manager at Gamewell-FCI, Northford, Conn., a unit of Honeywell that makes fire control systems. At the same time, responders can target specific groups with specific messages, he says. For example, in case of a shooter on campus, responders can focus on targeting and evacuating one building, relaying special instructions to its occupants. Meanwhile, people in other buildings can be told they are not under threat and be advised to stay where they are.

“A fire alarm system, because it’s robust, survivable and subject to scheduled maintenance, is ideal to communicate events to the occupants of a building,” Weaver says.

So far, the military has done the most deployment of these integrated systems, he adds, but there is a lot of interest from the private sector.

“NFPA has been around 47 years. They want to make sure mass notification works to those standards,” says Jim Mongeau, director of business development at Space Age Electronics, Hudson, Mass., which is launching a new division, Lifeguard Networks, to supply ancillary devices for fire alarm systems using IP and open protocols.

ANY IP DEVICE

While the fire alarms and panel serve as the primary means to both gather and disperse information, the broader significance of NFPA 72 is that it can turn any IP-enabled device into a tool for mass notification. As long as the device is IP-addressable, it can be controlled from a central point, Mongeau says. At an airport, for example, threat coordinators can take control of electronic signage and video monitors that display departures and arrivals. In addition to text messages, graphical information can be displayed, such as maps and directions to the nearest exit.

Still, one challenge remains: cellular phone networks, which quickly reach capacity during an emergency. Digitize Inc., Lake Hopatcong, N.J., supplies specialized 35-Mb/s IP wireless mesh networks that support emergency communications and mass notification. Using the wireless network, an organization can create one large hub for emergency communications with battery back-up, says Abraham Brecher, president of the company.

As Chapter 12 approaches the end of its comment period, excitement about its potential is becoming more palpable. “The first pass will be out here real soon,” Mongeau says of the code. “It’s great to be involved in an open protocol. Open protocol is the future of mass notification.”

FEW FINGERS IN THE MIX

BIOMETRICS STARS IN NICHES, NOT NETWORK

By Sharon J. Watson

Biometric technology is no longer the stuff of science fiction or high-tech thrillers. The technology for using a person's unique biological markers to offer irrefutable proof of identity or presence in a specific place at a specific time is functional, marketable and increasingly sophisticated.

"Biometric systems are available now. Fingerprint and iris systems are reliable," says Jonathan Keith, project manager for Milwaukee, Wis.-based Johnson Controls.

That's the good news for biometrics fans.

The sobering side of the story is that commercial enterprise users apparently are finding only limited uses for the technology. The reasons are intertwined, say analysts and a variety of security industry vendors.

First, biometric systems still cost more than password, token and card technologies. Second, biometric technology does not always work the way users expect. Higher costs combined with unmet expectations are keeping biometrics from playing a larger role in the converged physical/logical security world. Instead, the technology is proving useful in important but less integrated functions.

"The places where biometrics works are not where people expected it to go," says William Kennedy, product marketing manager for Pelco in Clovis, Calif.

THE COST PROBLEM

While the biometric vendor universe has consolidated through mergers and acquisition, innovation continues in types of biometric "templates." Enterprises and their system integrators may choose among fingerprint capture, palm geometry, voiceprint recognition, iris scans, facial recognition and even vein pattern recognition systems.

In a typical biometric system, a user supplies physiological data, such as a fingerprint, which is then stored as a complex mathematical template in a local reader, on a smart card, on a central database or in some combination. When the user presents his finger for scanning, the live data is compared against the stored template.

The security and convenience of biometrics seem obvious; however, the expense of achieving these benefits often comes as a surprise.

"There's a huge perceived cost problem with the equipment," says Steve Van Till, president and CEO of Brivo Systems, based in Bethesda, Md. He and others in the industry say many users are very interested in biometrics until they compare the

price tags of biometric scanners and biometrics-embedded smart cards with those of proximity cards and readers.

Sometimes biometrics may supply more security than is actually needed, vendors say.

"If you're not gaining a high security benefit, you haven't proven the economics of installing biometrics," says Damon Dageenakis, product marketing manager, physical access control readers for HID Global, based in Irvine, Calif. "You must look at the context in which you will use the technology."

MANAGING EXPECTATIONS

Managing what users expect to gain by deploying biometrics—security, convenience or both—is a critical challenge for the technology, say industry observers.

"Expectations for biometrics are still not set correctly," says Kennedy, who works with access control systems at Pelco and formerly marketed palm geometry biometric systems for Ingersoll Rand.

Most end users don't perceive the key benefit of biometrics as added security but rather convenience, he says. Then, if biometric tools are not convenient, users are dissatisfied. Kennedy says Pelco "constantly" finds biometric readers installed but disabled at client sites because they did not work as expected.

Users often expect to eliminate or reduce other security measures with biometrics. That's not always the case. "The value of biometrics is in combining factors of authentication," Van Till says. "If you give up an access card in favor of a fingerprint, you haven't necessarily made things more secure."

Practical problems also plague user expectations. Users see biometrics working seamlessly in film and on television. However, while the technology is constantly improving, false rejects are still common. A scab, scar or new ring may trick a reader. Workers in heavy industries may not have very legible fingerprints.

"Biometrics is not quite a science yet; there's still a lot of art that goes into it," says Larry Lien, vice president of product management for Proximex, a physical security information management systems vendor based in Sunnyvale, Calif. "Biometrics must get to the point where the accuracy is there."

Lien and others say clients are interested in multimodal forms of biometrics, in which multiple physiological markers are compared for a positive identity. However, costs often disqualify these systems for many companies today.

FRONT DOOR BACKLOG

One place that it's rare to find biometrics is at the main entrance of an enterprise or building. False rejections at these entrances easily can cause a traffic backup. Even if the biometric system works perfectly, each person still needs to stop and do something, whether it's be scanned or swipe a card and wait for a match.

"The biometrics system then becomes a barrier to me doing my work," Kennedy says.

Part of the issue is the speed of matching a user and a stored template. Most vendors

Consumer-driven Biometrics?

When discussing biometrics, privacy issues or the comfort level of iris scanning versus a fingerprint read usually get mentioned first. However, many security solutions vendors noted it's often individuals within an enterprise who first ask about biometrics.

"They're drawn to its Star Trek quality," says Steve Van Till at Brivo Systems.

The current cost of enterprise-based biometrics often forces those curious users back to earth. Yet, consumer biometric applications—including many launched in the Asia-Pacific region—could wind up driving widespread adoption of biometrics.

According to *World Financial Biometrics Markets,* released by Frost & Sullivan in May, biometrically enabled ATMs have become immensely popular in Japan and have been widely adopted in India, Latin America and the Middle East. The consultants expect revenue from biometric solutions sold globally to financial institutions to jump from $117.3 million in 2006 to $2.07 billion by 2013.

Not all consumer-oriented biometric applications are in the Pacific Rim.

UPEK Inc., based in Emeryville, Calif., has its biometric technology embedded in a range of notebook PCs made by Dell, Gateway, IBM/Lenovo and Toshiba, among others.

UPEK's biometric processing engine incorporates algorithms for RSA Security's SecurID one-time password solution—which has an installed base of more than 25 million. Companies using SecurID can then have RSA enable seed records in any UPEK-equipped device. After that, the same finger swipe that activates a mobile device simultaneously triggers the processor to generate a unique RSA SecurID "tokencode"—without using a physical token.

With this integration, an enterprise could secure its mobile devices as well as have a two-factor authentication process for signing employees into the corporate network and accessing devices, Web-based applications and portals. Multiple seeds in a single device can enable it to access different devices or applications.

UPEK also sells its Eikon Digital Privacy Manager through such outlets as Amazon.com.

The device, retailing for around $57, enables a consumer to log onto a PC with a fingerprint read—and also to log into various Web sites that require user IDs and passwords, again using a fingerprint read.

"We're starting to see more customer adoption," says Bill Bockwoldt, director of marketing, software and services for UPEK. Amazon consumer reviews for the product are largely positive.

Microsoft and APC also sell fingerprint readers direct to consumers.

—Sharon J. Watson

and observers note that "one-to-many" matches, in which templates are stored either in a reader or in a network database, are inherently slow because of the data volumes involved.

A more efficient current approach is a "one-to-one" match. A user's biometric template is stored on a smart card; the biometrics reader then reads the card template, compares it to the real-time data captured in a scan and makes a match. Even this approach takes time and requires more costly cards and readers.

BIOMETRIC BUSINESS CASES

Issues like these are pushing biometrics into security applications in which a relatively small volume of users need to access very sensitive or valuable data, materials or merchandise. Locations include server rooms, data centers, secure areas, vaults and storage facilities.

Some of the same access problems occur in these locations. But fewer users means greater tolerance for slower access times; the enterprise is so concerned about protecting the asset that it's willing to spend the money on sophisticated readers. Plus there's the "cool factor."

"The end user accepts the inconvenience as being part of the elite," Kennedy says.

Many observers say IT departments and computer manufacturers are driving biometric adoption. Laptops increasingly have built-in fingerprint readers, and the technology is finding its way into cell phones and other small mobile devices.

"It's cheaper to add a fingerprint reader to a laptop than to install fingerprint readers at every door," Van Till says.

Such readers can use the PC's or laptop's processing power and cost only a few dollars per unit, versus hundreds for biometric readers. And some industries have either the security needs or resources to deploy biometrics, Lien says.

"Business applications have to drive the technology," he says. "Biometrics has to be part of the standard operating solution and workflow across systems and the environment." He notes a security application for biometrics may not always be the best value driver.

BIO-TIME

In fact, time and attendance applications are the most commonly cited uses for biometric technology.

"There's an immediate return for large and small companies and manufacturers when they implement biometrics in time and attendance systems," Dageenakis says. He and other vendors point out that business enterprises are willing to pay for additional biometric readers at entry points and throughout work sites because of the benefits gained from increased timekeeping accuracy.

Biometrics also is useful in industries with many compliance regulations to meet because biometric data is considered "non-repudiable." That is, outside of a spy movie, it's difficult for someone to claim their finger or iris was stolen and used to enter a restricted database or work center.

In these situations, enterprises either issue biometrics-embedded smart cards to the employees requiring special access, or use a separate system of biometric readers at the locations, say vendors. It's rare to find a single access control system incorporating both the general population and the high-security biometric locations.

Nor is it common to find biometric data used as a trigger for video surveillance or other security applications. One reason may be that tying biometrics into some legacy card readers often requires that complex, highly secure biometrical algorithms be translated into much simpler Wiegand electronic signals the legacy systems can interpret.

Still, the potential and wish for integration is there. Lien says some of Proximex's customers are interested in combining more video with biometrics, such as a finger swipe matched to a video image.

"You need to leverage existing systems to enhance biometrics," he says. "It's another source of information."

Sharon J. Watson *is a freelance writer based in Sugar Land, Texas. She can be reached at sjwatson@experteditorial.net*

Eastern Promises?

When the U.S. government issued the FIPS 201 standard requiring biometrics to be embedded on all federal personal identity verification cards, many vendors and analysts expected to see biometric technology costs fall and its adoption soar. Similar hopes surfaced about the Transportation Worker Identity Card (TWIC), another set of federal standards for ID cards to be used at U.S. ports.

Yet in a news story last autumn, a General Services Administration executive estimated less than 1 percent of federal employees and contractors had PIV cards meeting FIPS requirements laid out in Homeland Security Presidential Directive 12.

Meanwhile, TWIC, another unfunded mandate, boasts of a robust technological standard—but one that may not be compatible with access control systems now in use at many U.S. ports. Many vendors are waiting to see how the standard shakes out before manufacturing readers compatible with it.

In short, say security vendors, the federal experiments with biometrics aren't doing much to drive the technology into commercial sectors…yet.

That may change, with national ID card projects incorporating biometrics either under way or planned in India, Malaysia, Japan and China.

Consultants Frost & Sullivan and Acuity Market Intelligence separately predict Asia-Pacific government and consumer-oriented biometric projects will account for the bulk of biometric revenues in the next decade, surpassing figures from both the United States and Europe. If so, biometrics would join the list of technologies, like mobile-based media, that Asia-Pacific businesses and consumers have effectively tested for the rest of the world.

—Sharon J. Watson

UNCOMMON PLATFORMS

CAN YOU BE THE SAME, BUT DIFFERENT?

By Steven Titch

The shift to the use of IP networks for video surveillance, as well as the enterprise-wide integration of other security applications over IP backbones, has substantially increased the choices large end users have for software platforms that control video surveillance networks.

Common platforms, however, force manufacturers to move away from the proprietary models of the past. Interoperability is in; vendor lock-in is out.

While seeking surveillance solutions that can integrate a broad range of cameras and edge devices, end users balk at platforms perceived as too generic. So video system suppliers are jockeying to differentiate themselves in new ways: by touting the superiority of their underlying technology, by playing to specific strengths in IT networking, by offering a tighter knit with other platforms, such as access control systems and analytics, or any combination of these methods.

The result has been a dramatic increase in the impact management software has on the purchase of a large-scale video surveillance system.

With analog, the purchase was all about the cameras. The management software was there to manage cameras and DVRs and do little else. The IP era changed that. Suddenly, cameras are nearly incidental and video management software—especially its compatibility and interoperability with other nodes on the enterprise network—is central.

Moreover, with video surveillance now an enterprise network application, IT departments are extremely involved in system review and selection. The high degree of IT influence has led software and networking companies like Cisco Systems, Milestone Systems and Genetec to leverage their expertise in IT—as well as familiarity among CIOs and IT managers—to push into the video security market.

Long-time suppliers of proprietary solutions, such as Pelco, Mobotix and Verint, are fighting back, introducing their own IP-based platforms that work across various cameras and encoders, while trying to maximize their existing advantage as established CCTV vendors with strong reputations as one-stop suppliers.

> ‘With markets changing fast, it’s not smart to be dependent on one vendor.’
>
> —Eric Fullerton, Milestone Systems

“It’s a trend across the industry,” says Mark Kirstein, president and co-founder of MultiMedia Intelligence, a market research firm. “Legacy vendors have more of the pieces pulled together. IP vendors are pushing hard on the other side, with no analog or legacy business to protect.”

Video surveillance management software essentially ports DVR and NVR functionality onto a PC or server, moving video control out of an isolated, vendor-specific CCTV silo into an environment where it can process, control and direct multiple feeds from multiple cameras, DVRs and NVRs located anywhere in the world, exploiting the scale made possible by IP networking.

Nearly all IP video software can be counted on to control thousands of cameras and to automatically discover and assimilate new cameras when they are added (sometimes drivers are required). All the traditional DVR and NVR functions are there: pan-tilt-zoom, video wall, search and analysis. IP-compatibility means the software can handle multiple feeds from different cameras using different compression algorithms. All can transmit live and stored video to other PCs and to thin clients like cell phones and PDAs.

So as vendors attempt to differentiate by stressing core background strengths and a unique organization of feature sets, apples-to-apples comparisons fall short.

No vendor has the “right” approach—or even claims to. Depending on user requirements, size and legacy equipment, some IP video solutions will work better than others. That’s why it’s important for end users to be aware of the respective strengths of the many vendors and how they are leveraging them to succeed (see chart, pages 22-23).

STRENGTH AND POSITIONING

The biggest and most important difference among vendors is their starting point. Companies like Pelco Inc., Clovis, Calif., and Verint Systems Inc., Melville, N.Y., are examples of legacy vendors whose traditional strength has been integrated CCTV systems. Milestone, in Brøndby, Denmark, and On-Net Surveillance Systems Inc. (OnSSI), Suffern, N.Y., are typical of a growing, aggressive corps of suppliers whose core strength is IP networking and software.

Milestone’s XProtect is built completely around IP and interoperability. The company does not manufacture any video surveillance hardware, choosing instead to develop drivers for a wide range of IP cameras and edge devices. The technology approach plays to common IT procurement methods, where CIOs and CISOs often look to integrators to bring together best-of-breed products, says Eric Fullerton, president of the company’s U.S. office.

“With markets changing fast, it’s not

smart to be dependent on one vendor. You can't always expect one vendor to give you what you need," he says.

Jeff Knapp, vice president of marketing at OnSSI, agrees. The company had been rebranding XProtect until this spring, when it introduced Ocularis, its own IP video management platform. "Users are looking at a different kind of integration. It's become an intuitive market reflecting what security operators want to do on an immediate basis," he says. "There's a need for networking best-of-breed."

Executives at Verint and Pelco, however, say there is still a great deal of interest in a single integrated solution from one vendor. "There are multiple definitions of 'wide open,' especially in this space," says Mariann McDonagh, vice president of global marketing at Verint. "This is a funky space. You pick your solution from a Chinese menu, but you don't build [systems] one piece at a time."

Verint's Nextiva software, she says, has anchored installations involving 750 cameras and 17 video platforms from diverse manufacturers.

"We want to be the de facto video management platform," McDonagh says.

Pelco moved into the IP space following its 2007 acquisition by France's Schneider Electric, which then folded Integral Technologies' DigitalSentry IP software platform into the Pelco product line.

"In moving toward an open architecture, taking components and building them into a solution, we want to allow customers to make choices," says Rob Morello, senior product manager of digital systems.

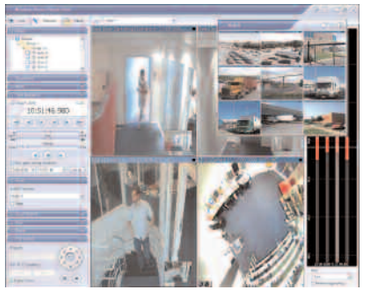
While customers want a variety of components from different players, Morello says they also appreciate the comfort level that comes from working through a turnkey vendor.

"Customers like to have one throat to choke," he says. "[Best-of-breed] integrators can deliver value, but it comes with liability."

Milestone's Fullerton, on the other hand, says turnkey players tend to give best-of-breed a bad rap.

"If we had that attitude, we wouldn't be where we are today," he says. "We take responsibility. We go a long way to solving any problem."

From the user perspective, companies like Pelco and Verint, along with IndigoVision, LenSec, March Networks, Mobotix and VideoInsight, can go a long way toward putting together a surveillance solution.



Milestone System's XProtect software

But they may work best for buyers with an enterprise network in place, substantial legacy gear and perhaps an existing relationship with either the vendor or one of its major integrators or resellers. They can get you cameras and NVRs, but might be more limited when it comes to the supply of other IT components.

Users less dependent on legacy CCTV equipment, and who are committed to maximizing value of their IP networking assets, are likely to gravitate toward vendors with a strong software and IT story. On the other hand, these projects will require more attention, investigation and evaluation, both from the purchasing organization and the system integrator angling for the bid. Companies like Milestone, OnSSI and Genetec, along with 3VR, Avigilon, DVTel, Exacq Technologies and Telindus, can make recommendations and can even provide a fair number of components, but they will be looking for far more input from customers.

APPLICATIONS INTEGRATION

Cisco Systems is trying to provide the best of both worlds. When it comes to brand equity in IT networking, few rival the San Jose, Calif., company. Yet, while Cisco is

The Importance of APIs and SDKs

Almost all IP video surveillance management software vendors provide application programming interfaces and software development kits. Those that don't, such as On-Net Surveillance Systems Inc. (OnSSI), which introduced its Ocularis platform in March, plan to have them available by the end of the year.

APIs allow other manufacturers to make their cameras, NVRs, access control systems, alarm systems and other security hardware and software compatible with the video management platform. They are generally available free.

Verint, for example, has supplied open APIs to Orsus (analytics) and AirVisual (PDA software).

"We want to play as well with all these other solutions," says Mariann McDonagh, vice president of global marketing. "That's where the value is."

SDKs allow end users or system integrators to design customized applications that can work off the vendor's platform. SDKs generally use software building blocks like Microsoft's ActiveX and .NET framework.

Ed Thompson, chief technology officer for DVTel, Ridgefield Park, N.J., sees the use of the .NET framework as a key advantage of his company's iSOC management software.

"It has a huge support library, all trusted and qualified," he says. The .NET infrastructure offers much more scale and stability and faster development time, particularly with Vista, Microsoft's new operating system, says Thompson. ".NET's robust, and Microsoft supports it. Microsoft invested thousands of man-years. Our applications ride on top of it."

—Steven Titch

Software Solutions for IP Video Surveillance Systems

Company	Product	Background strength	Manufactures additional video hardware?	Turnkey integrated functions	Operating system(s)	Encoding and compression	Pricing model(s)	Integrator certification required?	Open APIs?	SDK
3VR	SmartRecorder	Software	Yes	Analytics, case management, enterprise management, facial recognition, health reporting, license plate recognition, POS	Windows	H.264, M-JPEG	Per-camera/client license	Yes	Yes	Yes
Avigilon	Avigilon Control Center	Software	Yes	Access control, license plate recognition, storage (Steelbox)	Windows	JPEG 2000 (wavelet)	Pe-camera/client license	Yes	Yes	Yes
Cisco	Video Surveillance Stream Manager	IP networking	Yes	Access control, analytics, POS, TITO (casino app)	Windows (client), Linux (server)	H.264, M-JPEG, MPEG-4	Per-camera license or project configuration and number of cameras	Yes	Yes	Yes
DVTel	iSOC/Latitude NVMS	Software	Yes	Access control, analytics, data mining, visualization	Windows	H.264, JPEG, MPEG-4	Project configuration and number of cameras	Yes	Yes	Yes
EVT	Vertex	Software	No	Alarm management	Windows	H.263, H.264, M-JPEG, MPEG-2, MPEG-4	System core license, per-camera license, or per system	Yes	Yes	Yes
Exacq Technologies	exacqVision	Software	Yes	Access control, analytics, iSCSI storage, POS	Windows, Linux, Mac (client); Windows, Linux (server)	H.264, M-JPEG, MPEG-4	Per-camera/client license	No	Yes	3Q
Genetec	Omnicast	Software	No	Access control, analytics, fence detection, license plate recognition, POS	Windows	H.264, MPEG-2, MPEG-4, M-JPEG, wavelet	Per-camera license	Yes	Yes	Yes
IndigoVision	Control Center	Cameras and CCTV systems	Yes	Alarm management, analytics	Windows	H.264, MPEG-4	Based on camera resolution rate	Yes	Yes	Yes
LenSec	No trade name	Software	No	None, but integrates third-party applications on project basis	Windows, Linux	H.264, M-JPEG, MPEG-2, MPEG-4	Per-camera or bundled into project cost	N/A; sells direct	Yes	Yes
March Networks	VideoSphere Intelligent Video Management	Cameras and CCTV systems	Yes	Access control, alarm management, analytics, business intelligence, POS/ATM, transaction integration	Windows, Linux	MPEG-4	Per-camera and per-server licenses	Yes	Yes	Yes
Milestone Systems	XProtect	Software	No	License plate recognition, POS	Windows	H.264, JPEG, M-JPEG, MxPEG	Per-camera license	Yes	Yes	Yes
Mobotix	MxControlCenter	Cameras and CCTV systems	Yes	Analytics, bidirectional audio	Windows, Linux, Mac	M-JPEG, MPEG-4, MxPEG	Included in price of camera(s)	Yes	Yes	Yes
OnSSI	Ocularis	Software	Yes	Access control, analytics, environmental detection, fire panels, phones, POS	Windows	H.263, JPEG 2000 (for still pictures), M-JPEG, MPEG-4, MxPEG (for Mobotix cameras), wavelet	Per-camera license	Yes	Planned	Planned
Pelco	DigitalSentry	Cameras and CCTV systems	Yes	Access control, analytics, bar code scanning, POS/ATM, storage (IBM), truck scales	Windows	IVEX, M-JPEG, MPEG-4	Per-camera license	Yes	Yes	Yes
Telindus	CellStack Integration Suite	Software	Yes	Access control, analytics, biometrics, fire and intruder detection	Windows; proprietary embedded OS in high-end NVR	H.264, M-JPEG, MPEG-2, MPEG-4, MxPEG (proprietary)	Per-camera stream and operator location	Yes	Yes	Yes
Verint	Nextiva	Cameras and CCTV systems	Yes	Alarm management, analytics, storage (EMC)	Windows	JPEG, MPEG-4	Per-camera license	Yes	Yes	Yes
VideoInsight	No trade name	Cameras and CCTV systems	No	Access control, POS	Windows	H.264, M-JPEG, MPEG, wavelet	Per-camera license or bundled into project	Yes	Yes	Yes

> ‘There are multiple definitions of “wide open,” especially in this space.’
>
> —Mariann McDonagh, Verint

renowned for its support of interoperability and common standards (having written many of them), its traditional strength has been network hardware rather than software. However, it clearly sees the future of video surveillance as IP, hence its multimillion-dollar push into the surveillance segment, punctuated by its purchases of Broadware Technologies and SyPixx Networks in 2006.

Desktop interface on Pelco’s DigitalSentry system

The investment bore fruit this May when Cisco announced a 10-year deal with Harrah’s Entertainment Inc., the world’s largest casino operator. Among other networking innovations, the transaction involves the implementation of a large-scale next-generation security and surveillance infrastructure.

Cisco’s IP software serves as “a point of interoperability for entire systems, analytics, encoders and access control,” says Dennis Charlebois, director of product marketing for Cisco. “[It integrates] our systems and others into one nice application. It can manage and parcel out functions at the edge, at the server and at the application level.”

The Harrah’s deal is a template for how users want to turn video security into a network application that runs in tandem with other components and applications. In this case, interoperability is not limited to CCTV integration with access control and alarms, but with a much larger guest management system.

While Cisco might best articulate the strategy, nearly all software vendors are touting some level of turnkey applications integration.

“We’re on the verge of something transformative,” says Stephen Russell, CEO and founder of 3VR, in San Francisco.

Russell sees today’s video management software ultimately morphing into a central point for the enterprise to manage security processes across the global organization, combining access control, alarm management, analytics, storage and, depending on the customer’s vertical segment, ATMs, point-of-sale systems, ticket-in/ticket-out kiosks in casinos and much more.

Nearly all vendors have taken their first steps toward applications integration. For many of the legacy companies, it’s key to their future. The most common function is access control. Of the 17 vendors examined for this article, 10 offered an access management platform, either their own or through an OEM arrangement. Genetec, of St. Laurent, Quebec, which was selling an access control platform before it introduced its Omnicast video software, touts its experience. Pelco considers its partnership with AMAG Technology, which will allow it to link video management to access control and building automation functions, as critical to its turnkey strategy.

CODECS AND COMPRESSION

To really command the attention of IT departments, surveillance management software vendors must address video encoding, storage and analytics.

These are the functions that prompt the most contention between IT departments and security operations because of conflicting priorities. Different video encoding algorithms such as MPEG-4, M-JPEG and the emerging H.264 standard place different levels of demand on network and storage capacity. Simply put, the higher the resolution and faster the frame rate, the more bandwidth and storage capacity the surveillance network consumes. Security and compliance officers want as much data as they can get. IT directors want efficient network use.

MPEG-4 and M-JPEG, the most common legacy encoding schemes, are bandwidth-intensive. Thus IT managers usually demand frame rates be scaled back, usually in inverse proportion to the camera resolution. While most networks can tolerate MPEG-4 at 10 to 25 fps, M-JPEG streams generally need to be 5 fps or less.

Users see H.264 as a potential middle ground. Studies by Edinburgh, U.K.-based IndigoVision have shown that compared to MPEG-4, H.264 can achieve typical savings of between 20 percent and 25 percent in bandwidth usage and in excess of 50 percent during periods when there is no movement in the frame.

“H.264 is the most popular. And because it’s standard, it’s cheaper,” says Patrice Belmonte, director of marketing at Genetec.

“But is it ready?” counters Iain Wadds,

Compression Conversion

As a differentiator, VideoInsight touts a “transcoding” technique that it says makes storage and retransmission that much more efficient. According to James Whitcomb, the company’s chief technology officer, VideoInsight’s software can, for example, convert an MPEG-4 video stream into an AVI file, a format that can be used with popular video client software, including Windows Media Player. A 150-kilobyte MPEG-4 file can be converted to a 10-kilobyte AVI file, Whitcomb says, making it much easier for it to be transmitted and viewed on a handheld device.

head of pre-sales consultancy at Telindus, Cambridge, U.K., which does not support the algorithm.

Meanwhile, a handful of vendors, including Avigilon, Genetec, OnSSI and VideoInsight, are looking at leading-edge wavelet compression encoding schemes—JPEG 2000 for still frames and a variety of nonstandard formats for moving images. Wavelet compression, they say, is the only technology that can allow security departments to get all the advantages from digital high-definition and megapixel video without overtaxing the undergirding IT networks.

JPEG 2000, explains Pierre Parkinson, vice president of marketing and business development for Avigilon, of Vancouver, B.C., which promises HD "out of the box," uses on-board camera intelligence processing to record large amounts of data and then selectively transmit data. Avigilon's Control Center software can be set so a 16 megapixel camera transmits one frame per second at the full 16 megapixels, and the other 29 frames at one megapixel. It can also send portions of a single image at full resolution, where a person might be moving, for example, rather than the whole picture.

A few manufacturers offer proprietary encoding techniques, a holdover from the legacy era. Mobotix, for example, offers its own proprietary MxPEG algorithm with its cameras.

"MPEG-4 requires processing power, video compression and storage," says Peter McKee, director of sales for the Kaiserslautern, Germany-based company. MxPEG can feed 40 high-resolution camera streams to a single PC, he says.

> 'Customers like to have one throat to choke. [Best-of-breed] integrators can deliver value, but it comes with liability.'
>
> —Rob Morello, Pelco

Analysts such as Kirstein, even as they question whether H.264 is suitable for HD, are skeptical about the long-term viability of proprietary codecs.

"Interoperability is a lot more important," he says. "You're not going to get away with a proprietary codec."

STORAGE AND ANALYTICS

At least four vendors—March Networks, Telindus, Verint and Pelco—emphasize their ties with storage companies.

Telindus has an OEM agreement with Steelbox Networks, which provides a storage system geared for surveillance applications. Verint partners with EMC, and Pelco works with IBM. March Networks, Ottawa, Ontario, has a deal with Sun Microsystems.

"As the industry goes to an all-IP platform, storage requirements are going up," says Peter Strom, CEO of March Networks. "The Sun platform is extremely compelling from a [total cost of ownership] perspective. It's open and scalable and uses Windows or Linux." The relationship has helped March Networks win customers in the retailing, transportation, financial and banking industries.

Analytics provides another point of differentiation. Although products are available from companies such as IQinVision, Orsus and ioimage, analytics packages are increasingly being integrated into video management software. Even Milestone, which started out as the quintessential application-agnostic video software platform, added a license plate recognition feature this spring.

PRICING

Finally, pricing approaches vary among vendors, although gradually manufacturers are moving toward a model based on a license fee paid per camera.

"Per-camera license is the only model that makes sense," Kirstein says. "It's the only way vendors can have a sustained revenue stream." Any resistance stems more from the perception inherent in the legacy market than from outright vendor strategies, he adds. "The perception has always been that hardware has more value than software—even when it was software in a hardware box."

Cisco, DVTel, EVT, IndigoVision, LenSec, Mobotix and VideoInsight offer pricing schemes based on factors other than number of cameras. In some cases, the software cost is bundled into the cost of the project, an approach used by Cisco, VideoInsight, LenSec and EVT. Only Mobotix rolls the cost of the software into the cost of the camera itself—and boasts it will give away control software free for use with non-Mobotix cameras.

Analysts such as Kirstein see the per-camera license model winning. But that does not mean the future belongs solely to the software specialists. Still, as procurement processes become more tied to IT networking requirements, it will be legacy players—and their channels—that will have to adapt more readily.

"The speed of innovation is so fast," Milestone's Fullerton says. "You're not going to know what the user wants tomorrow."

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

You Go Right, I'll Go Left

The deal between March Networks and Sun Microsystems provides insight into the way the two companies are piggybacking on each other's supply channels to get in front of new customers. Sun, which faces diverse competition in the IT space from Cisco, IBM, HP and Microsoft, can position March Networks' video surveillance package as a sweetener to its base of IT customers. At the same time, March Networks gets access to Sun's value-added reseller channel. March Networks reciprocates, getting Sun in front of traditional security system buyers through its own network of integrators.

Applications, Strategies, & Solutions

1 Chilean Casino Project

Enjoy Group has chosen IndigoVision's IP video system to provide a complete digital video surveillance solution for all nine of its casinos in Chile. The first 500-camera system has been completed at the casino complex in Coquimbo. Once complete, the entire project will have upgraded more than 2,500 cameras to digital IP-CCTV surveillance. Installation is being managed by Bitelco Diebold LTDA, with the storage solution supplied by Intransa. Each of the CCTV cameras will be connected to an IndigoVision 8000 transmitter/receiver that converts the analog feed to DVD-quality, 4SIF, 30 fps digital video for transmission over the IP network. The casino security staff will use Control Center, IndigoVision's IP video and alarm management software, to view live and recorded video from any camera in the system.

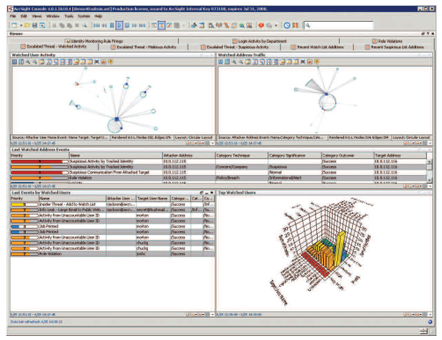
2 Mini-Dome Camera

IQinVision has unveiled Alliance, a mini-dome camera system that promises unsurpassed megapixel lens optics, on-board SD card storage and an integrated tracking shroud that automatically aligns the camera and lens. It features a three-axis gimbal, full Power-over-Ethernet capability, alarm I/O connections and dual analog video outputs—one for public view monitors and another for field-of-view and focus adjustments. Alliance offers 64 simultaneous, independent video streams and H.264 compression. Resolution ranges from VGA to high-definition 2-megapixel quality.

3 Video Flicker Reduction

Pixim's V3.2 firmware with Enhanced Flicker Reduction mode overcomes video sampling issues that can diminish camera performance, including fluorescent light flicker, fluorescent color roll and frequency-modulated LED "blackout." These issues all are caused by differences between the video field capture frequency, which is set by global standards bodies, and the local AC power frequency, which varies by geographic location. The firmware for Pixim's Orca chipsets began shipping to camera companies in May, and the first Pixim-powered cameras with EFR are expected to reach the market in the third quarter of 2008.

4 Software Links ID and Event Management



ArcSight has introduced IdentityView, a solution for increasing the value of identity management technologies. ArcSight IdentityView connects the user- and role-management functions of ID management products with the broad activity monitoring and correlation functions of security information and event management products. IdentityView is uniquely designed to work with identity and access management systems from a variety of vendors to improve security and compliance by understanding who is on the network and what actions they are taking. IdentityView includes pre-built capabilities for correlating multiple user identities to a single identity key. Using that master identity key, IdentityView collects all of a user's activity information and analyzes it to determine if the user is performing unauthorized activities. IdentityView also includes specialized connectors for leading identity and access management solutions, including those from Oracle and Microsoft.

5 UK Biometric Deal

Sagem Sécurité has won a contract from the U.K. Home Office to supply the biometric management system for U.K. visa applicants and the biometric management subsystem for the Biometric Residents Permit project. These automated fingerprint identification systems will provide the means to track the immigration status of foreign nationals through the production of biometric cards. The systems are designed to process more than 5,200 requests per hour for a database of 16 million.

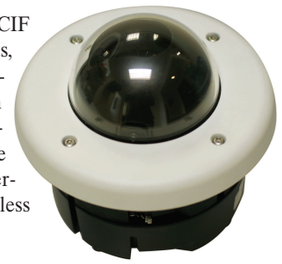
Information in this section has been supplied by the respective vendors. *Network-Centric Security* magazine does not accept responsibility for the timing, content or accuracy of the product data or for the quality or accuracy of the photos.

6 IP Camera Packages

American Fibertek Inc. (AFI) has introduced six new IP Video Network Enterprise Solution (V'nes) packaged systems for quick set-up in retail stores, fast food restaurants and other establishments with small surveillance footprints. The packages, designed for 8-, 16- and 24-camera configurations, come with AFI's Director servers with dual core Intel processors and 3 GB of memory. AFI's Pilot Management software is pre-installed and can be customized for alarms and reactions. The embedded Commander IP Communication Center provides network switching; environmental, power and bandwidth monitoring; and interfaces with access control and point of sale systems.

7 Megapixel Cameras with Adaptive Technology

DVTel has previewed a new line of IP megapixel cameras designed to achieve 16 CIF (1408 x 1152) resolution with low bandwidth and storage requirements. The cameras, which the company has been demonstrating since May, incorporate MPEG-4 compression, multicasting technologies and DVTel's proprietary adaptive visualization technology (AVT) algorithms at the network edge. The AVT algorithms continuously adapt to changing light and environmental conditions to automatically improve and maintain picture clarity. The technology substantially improves workstation performance, DVTel says, and allows the user to display more megapixel images using less CPU power.



8 Fluidmesh, Pelco Supply Wireless Video

Segro, a U.K. property investment and development company, has installed a Pelco IP video surveillance system at the 60-acre Kings Norton Business Centre in Birmingham, supported by a Fluidmesh 2200 wireless mesh network. Mitie Security Systems installed eight Pelco Spectra IV dome cameras and uses Fluidmesh wireless IP transmission to relay their signals back to an on-site control room. The system minimizes latency while doubling available bandwidth by using two radios simultaneously, one operating in the 2.4 GHz band, and the other in the 5 GHz band. A dedicated Micros DVIP digital recorder records all incoming information and links the system to the Business Watch control room in Slough from where the site is monitored.

Converging Risk Assessments

By Marleah Blades

Just as every business is unique, so too are corporate approaches to physical and logical security convergence. However, as companies develop their convergence models, they should thoroughly consider all business functions or processes that may benefit from it, says John McClurg, vice president of global security for Honeywell.

McClurg, a member of the Security Executive Council, has seen a variety of models as he's researched convergence practices in large organizations, and he's noted that corporations frequently overlook one function that could benefit from convergence: risk assessment.

> 'A converged assessment presents the interdependencies between physical and cyber vulnerability'
>
> —John McClurg, Honeywell

"Classically, your IT risk assessors will go to part of a business, show up one week and then come back and issue a product," McClurg says. "A couple of weeks later your physical team will come, take more of your time, do an assessment and issue a product. It's left to the [assessed department] to correlate the total risk posture."

At Honeywell, McClurg has pulled those two activities together, cross-training risk assessors and sending out teams able to perform a single comprehensive risk analysis comprising both IT and physical security. He's seen a number of benefits from this innovative approach.

A CLEARER RISK PICTURE

"The converged assessment is more likely to present in a coherent manner the interdependencies between physical and cyber vulnerability," McClurg says.

"A good example is the phreakers (telecom hackers) I used to work against when I was in the FBI," he said. "They would exploit a 30-year-old rusty lock with an old-fashioned pick set—a physical world vulnerability. Once that's exploited, the phreaker goes into the central office of a phone company and quickly gathers up manuals, passwords and other equipment that he can take back to his base of operations, and there advance a far more

continued on page 34

sophisticated cyber attack than he would ever have been able to do but for the physical world deficiency."

When IT and physical risk assessments are done separately, the assessed business unit has to put the two assessments side by side and analyze them carefully to discover interdependent vulnerabilities—but this doesn't happen often. A converged assessment draws the lines of interdependency for the business unit, leaving less to the imagination and allowing it to move directly to the mitigation phase.

BETTER AUDIT PERFORMANCE

Because the converged audit provides a clearer risk picture, it helps each business unit prepare more thoroughly for the corporate audit, anticipating which issues might be cited and dealing with them in advance. When one team is responsible for risk assessments, it is also easier to coordinate them with the corporate audit schedule in mind.

"We know where [the audit is] going to go a year in advance," McClurg explains. "And we try to get our assessments pre-positioned six months in advance of the audit so any remediation that needs to be done can be fixed before they come. You see a more robust audit rating and less going to audit committee."

A single converged risk assessment causes less interruption, improving unit productivity.

McClurg says Honeywell also has experienced significant cost savings from using converged risk assessment teams.

"With a team that is cross-trained, you can do more with the same individuals," he says.

SIGNIFICANCE OF INFLUENCE

To begin converging risk assessments in the corporation, you must have a relationship and influence with the heads of other business units and in the executive suite.

"I sit on [Honeywell's] IT Council with the CIO and its Technology Leadership Council with all the CTOs, and I advance those duties as a peer, which conceptually pulls or expands the way you traditionally think of the CSO," McClurg says. "It's a positioning that acknowledges that in this day and age security is not an afterthought but an inextricable, indispensable way of advancing the business, whether it's the technology or the IT or the resiliency piece of the business. The inextricable nature in which security weaves itself into the company justifies the placement of this critical role."

Because of his role in the organization, McClurg has found strong support for converging risk assessments: "I end up not having to do nearly as much pushing as I'd otherwise have to do, because as you educate your peers, they start to recognize the need for certain initiatives, so they're pulling with you instead of being pushed."

Marleah Blades *(mblades@secleader.com) is senior editor for the Security Executive Council, an international professional membership organization for leading senior security executives.*

LINKS

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

3VR	3vr.com
American Fibertek	americanfibertek.com
ArcSight	arcsight.com
ArecontVision	arecontvision.com
AvaLAN Wireless	avalanwireless.com
Avigilon	avigilon.com
Axis Communications	axis.com
Bosch Security Systems	bosch.com
Brivo Systems	brivo.com
CBC America	cbcamerica.com
Cisco Systems	cisco.com
Digital Horizon	1dhs.com
Digitize Inc.	digitize-inc.com
DVTel	dvtel.com
EVT	evt-vms.com
Exacq Technologies	exacq.com
Firetide	firetide.com
Fluidmesh Networks	fluidmesh.com
Gamewell-FCI	gamewell-fci.com
Genetec	genetic.com
HID Global	hidcorp.com
Hirsch Electronics	hirschelectronics.com
Honeywell	honeywell.com
Hughes Associates	haifire.com
IndigoVision	indigovision.com
Ingersoll Rand	ingersollrand.com
ioimage	ioimage.com
IQinVision	iqinvision.com
Johnson Controls	jci.com
LenSec	lensec.com
March Networks	marchnetworks.com
MicroTek Electronics	microtekelectronics.com
Milestone Systems	milestonesys.com
Mobotix	mobotix.com
MultiMedia Intelligence	multimediaintelligence.com
OnSSI	onssi.com
Panasonic Security Systems	panasonic.com/business/security
Pelco	pelco.com
Pixim	pixim.com
Proximex	proximex.com
Sagem Sécurité	sagem-securite.com
Space Age Electronics	1sae.com
StarDot Technologies	stardot.com
Telindus	telindus.com
UPEK	upek.com
Verint Systems	verint.com
VideoInsight	video-insight.com
Zebra Technologies	zebra.com