PULL OUT AND SAVE

SUPPLEMENT TO SECURITY DIRECTOR NEWS
THE BUSINESS NEWSPAPER FOR SECURITY DIRECTORS
SEPTEMBER 2004

AND

SUPPLEMENT TO SECURITY SYSTEMS NEWS
THE BUSINESS NEWSPAPER FOR THE SECURITY SYSTEM INTEGRATOR & INSTALLER
NOVEMBER 2004

PHOTO COURTESY OF MARCH NETWORKS

CONVERGENCE NEW ENTRANTS TECHNOLOGY FUTURE

BUILDING TOMORROW'S SECURITY SOLUTIONS TODAY

Networking issues and developing technology come together to redefine the integrated security market

ObjectVideo

www.objectvideo.com

YOU SET THE RULES. BEFORE THEY CROSS THE LINE.

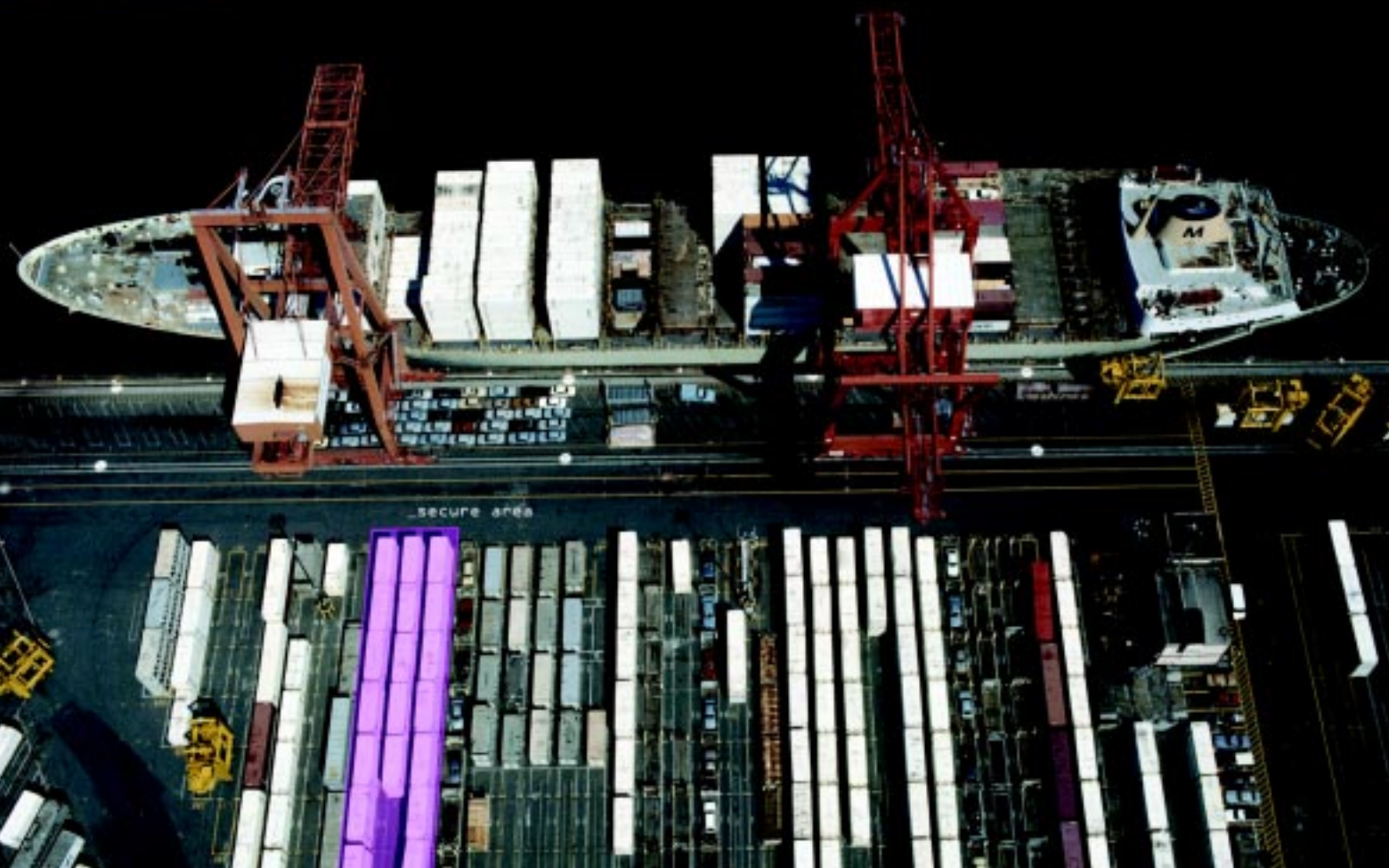
The critical infrastructure you're responsible to protect is a target.

The unpredictable nature of the threat today requires more than conventional means to stop it. You must know what is happening in real-time, be it a perimeter crossing, a vehicle casing a building or an unidentified bag mysteriously left behind.

ObjectVideo's pioneering software intelligently analyzes video from your surveillance system and alerts you when a security breach has happened – **immediately.** It detects, tracks and classifies the potential threat, presenting specific information you use to make a decision.

ObjectVideo VEW turns raw video data into actionable security intelligence. **ObjectVideo Forensics** rapidly identifies anomalies and uncovers valuable information from collected video. Contact us for a demo today.

THE LEADER IN INTELLIGENT VIDEO SURVEILLANCE SOFTWARE.



INTRODUCTION

Building Tomorrow's Security Solutions Today — Networking issues and developing technology come together to redefine the integrated security market.

This white paper will provide you with valuable information on the changes that are coming to our industry as we move from an analog-based world to a fully digital format. Our industry is not alone in this migration—the world as a whole and every industry is involved in the digital revolution.

The ability to capture data—whether it's voice, audio or video continues to expand. We can move these faster and farther without corruption and in larger pieces. With all of this comes a variety of systems to store, access and manipulate this information whenever it's needed.

This white paper is your first consolidated snapshot of what's coming and how each segment of our industry is responding to this. In February, TechSec Solutions, an event brought to you by the publishers of *Security Director News* and *Security Systems News*, will provide attendees with an even more detailed and constructive look at this changing market. We'll bring experts to the table to discuss in detail the technologies that are both available today and those in development that will unquestionably change the way we do business.

The more you know about and understand the changing face of the market, the better you will be able to evolve your business for the future and support your customers.

We look forward to seeing you at TechSec Solutions Feb. 27 - March 1 where you can get a clear vision of the future of our industry.

Respectfully,
Carol Enman, Publisher
Andrea Gural, Editor, *Security Director News*
Chelsie Woods, Editor, *Security Systems News*

SOURCES

"Building Tomorrow's Security Solutions Today" was written by Joanne Friedrick and contributed to by Andrea Gural, Chelsie Woods and the industry sources listed here, who shared information and insight on the industry today and its future.

Alan Lipton, chief technology officer and director, research and development, ObjectVideo
Allan Griebenow, president and chief executive officer, Axcess
Arpad Toth, senior technologist, GTSI and chairman of InteGuard Physical Security Alliance
Barry Walker, chief executive officer, CoVi Technologies
Bill Jacobs, manager, security, technology and systems
Bill Spence, director of marketing, IR Recognition Systems
Carey Boethel, vice president, electronic security systems Division, NetVersant Solutions
Carter Griffin, chief executive officer, Brivo Systems
Dennis McCallam, technology fellow, information technology sector, Northrop Grumman
Doug Cram, vice president, sales and marketing, AWID
Edward Hester, vice president, durable goods division, The Freedonia Group
Eli Gorovici, chief executive officer, DVTel
Eric Maurice, director, eTrust Security Management Solutions, Computer Associates
Frances Zelazny, director, corporate communications, Identix
Frank Abram, vice president, Panasonic Security Systems
Frank LaPlante, vice president, NetBotz
Fredrik Nilsson, general manager, Axis Communications
Glenn Hirsh, enterprise architect, GTSI
Hap Patterson, vice president, advanced research, Tyco Safety Products
Holly Sacks, vice president, marketing, HID Corp.
Jim Coleman, president, Operational Security Systems
Jim Scott, president, IR Security and Safety Solutions
Joe Freeman, principal, J.P. Freeman Co.
John Cassise, director, national accounts, Amag
John Kronick, managing director, North American Security Practice, GE IT Solutions
Jonathan Hollander, chief executive officer and chief architect, Vigilo Security International
Juan Cabezas, senior vice president, global marketing and strategic alliances, GE Security
Marc Abbagnaro, vice president, physical security, Anixter
Marty Guay, regional vice president, Securitas Security Systems USA
Nobu Kawaski, senior marketing manager, IP video monitoring group, Sony Electronics
Peter Strom, chief operating officer, March Networks
Phil Libin, president, CoreStreet
Ray Shilling, NVS Group, video division, Canon USA
Reg Foulkes, chief technical officer, CSC Global Security Solutions
Richard Baggot, vice president, electronic security and currency systems group, Diebold
Rudy Prokupets, chief technology officer and vice president, research and development, Lenel Systems International
Scott Oliver, senior vice president, Pacom Systems
Stephen Pineau, president and chief executive officer, Viscount Communications
Wes Eller, manager, security systems division, Deere & Co.
Yvonne Hao, vice president, global marketing, Honeywell Security

Convergence Comes at a Cost...

A MUCH LOWER COST, Where This:

MESH Servers

- Eliminate "Wiegand" card/elevator controllers
- Redundant servers; RAID 1-5 hard drive redundancy
- Redundant LAN LOOP device redundancy
- Redundant intelligent UPS
- IP addressable voice panels for guard stations/entrances
- Digital Elevator control, Alarm I/O

MESH RFID Readers

- Addressable readers "daisy chain" on CAT5
- Built-in I/O activates door strikes and exit devices
- Polling diagnostics of reader/cable status

MESH Software

- WEB Based programming, partitions globally or by site
- SQL database with unlimited users, cards, parameters

Replaces All of This and MORE!

MESH is a System Like No Other.

Modular and expandable, it eliminates the need for controllers by using intelligent 485 addressable proximity readers connected directly to com ports and routers on MESH servers. MESH servers turn your access control system into a truly IT compatible set of devices. Please call now to learn how MESH helps you converge security and IT.

Incredible Savings:

- Save on Hardware: Controllers replaced by MESH servers and panels.
- Save on Wiring: Cat 5 cable with built-in reader I/O.
- Save on Service: No masses of controllers to maintain
- Save on Software: Built-in Web based software, no multi-user license fees.

About Viscount:

Viscount was an R&D subsidiary of *Verizon Communications Telus* affiliate from 1969-1997.
We develop technologies that converge computer telephony and building control to provide revolutionary functional and cost benefits.

Call Toll Free 1-800-476-3774

E-mail us at sales@viscount.com or visit us at www.viscount.com

viscount
We Control Doors

"Now, because of the IT influence, we see global platforms linked through IT systems."
— Yvonne Hao, Honeywell Security

If there is an "it" topic among security industry participants these days, it would have to be IT. The convergence of traditional security systems with the IT network has given rise to a host of issues from how this will work and who has control to what the impact will be on integrators' business and manufacturers' products.

Of course, the debate over how best to work with the IT department isn't limited to the security sector. A recent survey from Deloitte Consulting LLP and IDG Research Services showed only 10 percent of companies say their enterprises have been "extremely successful" at aligning IT and business efforts. Yet, 96 percent of them predicted a "significant" or "moderate" positive impact if IT spending were planned and measured against corporate priorities.

The ineffective communications between the business side and the IT side represented a significant or moderate challenge for 65 percent of respondents.

So if security personnel are having a difficult time finding common ground with the IT department, as the Deloitte/IDG research shows, they aren't alone.

"It's a strange evolutionary process," says Frank LaPlante, vice president-marketing for NetBotz. Calling IT and physical security "two separate islands," LaPlante says the move toward digital, IP-based systems has driven the migration of security onto the existing IT infrastructure.

While the needs of corporations differ based on the organization's size and nature of its operations, there is little doubt that the economies of consolidating the security functions onto an enterprise network has been a major driver of that migration.

For global technology firm Cisco Systems, putting the security system on the network was the company's "only logical decision" in order for comprehensive security management at Cisco locations around the globe, said Bill Jacobs, Cisco's manager-security, technology and systems. "Our goal was to have one centralized security database of information, linked and synchronized to the human resources database so that security administration was minimized and information was current," he said.

Smaller player Deere & Co., which has run its access control system for 55 different locations on the corporate network since 1997, also sees the economies of scale and cost-savings in using one infrastructure for many different systems. To operate without a server at each location would require a minimum of five people on site, according to Wes Eller, manager-security systems division, Deere & Co.

The real buzz, according to Carey Boethel, vice president, electronic security systems division-NetVersant Solutions, is total "operational convergence between physical and cyber security controls." For example, if a person doesn't use their access control card to enter the building, and they use their password to try to log onto their computer, the system sends up a red flag because the person logging on may not be the appropriate user.

Taken a step further, true convergence is the melding of security functions within an organization, using the tools of security in other applications. For example, video surveillance systems used by Club Car, a division of Ingersoll-Rand that manufactures golf, utility and transportation vehicles, are also being used so that potential buyers of Club Car's used vehicles can view vehicles at remote sites.

"We are just looking at technology within organizations and how it can help businesses. It's convergence for efficiency."
— Jim Scott

"We are just looking at technology within organizations and how it can help businesses," said Jim Scott, president of IR Security and Safety Solutions. "It's convergence for efficiency."

But marrying two applications or departments for efficiency doesn't always breed cooperation, particularly given the sensitive nature of security information.

"The co-dependence is starting to be there and its making

links between transactions on the physical side and the IT side," Boethel said. "Now you have two disparate groups seeing the value of working together, although it's not there yet. There are a lot of territory battles."

TURF JOUSTING

A large part of the debate has been over who owns, or runs, the network. At Cisco, a compromise of sorts occurred when the company migrated its access control functions onto the corporate network. Early on, Jacobs said, he had ownership and management responsibilities of all the servers, but the company "transferred the responsibility of management of the hardware (infrastructure) and the operating system/virus protection to IT. I own the application and the relationship with the manufacturer of updates and future business enhancements."

To hear some say it, the most common result of this tug of war is IT personnel often taking the lead as the two sides begin to work together, said Eli Gorovici, chief executive officer of DVTel. "It's on the network, so the IT people take charge," he explains.

Yet Gorovici says businesses need to bring security into the organization, such as into a multi-source intelligent management system, he says, rather than viewing it as a separate function.

"We must remember that the operation of physical security protection systems demands very high reliability, security and trust relative to commercial-grade IT systems."
— Arpad Toth

Arpad Toth, senior technologist with IT integrator GTSI, agreed. But Toth, who is also chairman of InteGuard Physical Security Alliance, a group of physical and IT companies that have teamed up to provide physical security solutions, also cautioned about the high-maintenance nature of the two disparate disciplines.

"We must remember that the operation of physical security protection systems demands very high reliability, security and trust relative to commercial-grade IT systems," Toth said. "Integration of hardware and software resources will happen mostly at the backend of the IT and security systems, for example, matrix switcher, data storage, trunk and feeder lines, servers, switchers, routers."

BANDWIDTH AS A BARRIER

Different parts of the infrastructure will provide different barriers to marrying the two discplines, but one of the major issues between security and IT include bandwidth, said Peter Strom, chief operating officer, March Networks. Security is now transmitting over a mission-critical network; and security of the network itself, which is exposed to more viruses and attacks as more information goes up onto it, he said.

That high bandwidth usage by physical security systems, such as for surveillance, will initially limit their place on the network, according to Glenn Hirsh, enterprise architect, with GTSI. "I believe you will see simple integration of systems such as magnetic badges or common access cards into network systems for tighter security and, as organizations become more aware of the possibility of integrating physical and network security, the scope will then grow."

FOLLOW THE LEADER

Many in the industry say they believe security needs to be an active, vital participant as the two departments come together. And maybe even take the lead role.

Rudy Prokupets, chief technology officer and vice president-research and development at Lenel Systems International, agrees there is no separation between physical and logical security any longer. "People live in both spaces," he says, "you have convergence and can use it (the network) for whatever you need."

But the question remains: who in an organization is leading the charge for this consolidated approach?

"Security helps IT people do it (run the network) securely," said Reg Foulkes, chief technical officer, CSC's Global Security Solutions, which is becoming more important as companies need to comply with the information security measures laid down in Sarbanes-Oxley Act and other regulations. But other rules, such as privacy laws, in one country may be in direct conflict with information access laws in another, such as Canada's privacy law versus the U.S. Patriot Act.

"It impacts how we engineer and do convergence on the IT network," Foulkes explains.

Perhaps the most important facet in the fight over control over a network infrastructure is where corporate management grants the purchasing power, a decision that affects not only the end user but also the vendor community of integrators and product suppliers looking to tailor their offering to today's new customer base.

The end user used to be the security department, "but now we're seeing more influence from the IT director," said Yvonne Hao, vice president-global marketing for Honeywell Security, which also affects on what level decisions are made. "Now, because of the IT influence, we see global platforms linked through IT systems," she said.

The best customers, said IR's Jim Scott, have been a team that is grounded in the security department but also has input from finance, IT and human resources.

Alan Lipton, chief technology officer and director-research and development at ObjectVideo, agrees the IT decision-makers are gaining ground when it comes to purchasing power within the security space. "It's a different class of buyer," Lipton says, going from security's traditional one-stop shopping view to IT people "who want different components and plug-and-play—the best of all worlds."

But to properly tailor a new offering, vendors need

Continued on page 15

"I think there is an increasingly keen awareness that technology can have an impact on the bottom line."
— Carey Boethel, NetVersant Solutions

Key among the factors driving growth in the security market, according to a November 2003 report published by Frost & Sullivan, is the shift toward integrated security technologies. The report notes that digital surveillance, remote monitoring and advances in software integration have resulted in increased offerings.

Add to this increased residential demand aided by new construction activity, commercial growth prodded by companies' liability concerns and anticipated government spending on security, and the outlook is a healthy one.

In fact, the Frost & Sullivan report shows U.S. commercial end-user revenues of $14.15 billion in 2002 will reach $29.36 billion in 2009. Revenue numbers for the government end-user market were recorded at $7.49 billion in 2002 and $16 billion in 2009, and residential revenues at $1.72 billion and $3.21 billion for 2002 and 2009, respectively.

In its report on electronic security products, The Freedonia Group projected 8.7-percent growth in demand per year through 2008 to $15.5 billion. Looking at specific technologies, the report projects double-digit annual growth for both access control and CCTV systems.

Slower demand will come from alarms and electronic article surveillance, the report notes, but adds "smart labels based on radio frequency identification technology will represent a growth segment within the EAS market."

Edward Hester, vice president-durable goods division at Freedonia, says smart cards have thrived in Europe but have done less well in the United States, so far. Biometrics, however, has a great deal of potential, Hester says, "and has had for some time. It's just had trouble getting its footing."

He says without large companies with a lot of resources promoting biometrics, it won't explode the way digital CCTV has.

INTEGRATORS, END USERS SEE THE SHIFT

Perhaps one of the biggest developments in the security market is the use of IP-based technology. More and more manufacturers today are providing products in this niche market, with the end user and systems integrator fueling demand.

"Adoption of IP cameras for automated intelligent video surveillance has grown substantially," notes Arpad Toth, senior technologist, GTSI Corp. and chairman, InteGuard Physical Security Alliance. "Overall, we anticipate triple-digit growth rates in the new generation digital video surveillance systems for at least the next three years."

Bill Jacobs, senior manager-security, technology and systems for Cisco Systems, says Cisco is embracing digital camera technology as a way to protect the company's capital investment. The company, he says, has some IP cameras in use and will continue to migrate to them as the analog cameras' life span expires.

"We have converted all 2,600 analog cameras over to digital, utilizing encoders," says Jacobs. "All of our video is stored on network video recorders and SANs. We can monitor any camera in real-time in any of our 300 worldwide locations with three mouse clicks."

Despite the newness of the techology, systems integrator Vigilo Security International says a majority of its camera sales are for IP cameras. "Although 80 percent of our sales are in IP (cameras), it's not necessarily the norm," said Jonathan Hollander, chief executive officer and chief architect at Vigilo Security. "But why not have a camera anyone can see (the video from) if they're supposed to?"

The adoption of new technology is not just limited to IP cameras, but touches on other facets of the market, as well. Biometrics and access control systems are going through an evolution of their own, with greater capabilities that make these systems more efficient and enable users to track visitors, collect data and manage a host of other functions.

"We're seeing people adopting more technology related to identity management and authentication," said Reg Foulkes, chief technical officer for CSC's Global Security Solutions. "It might be a biometric or, if it's not as important for security purposes, other credentialing."

The reason companies are embracing this technology is the greater demand placed on properly securing a premise. Manpower alone is too costly and requires too many people, says Marty Guay, regional vice president,

Securitas Security Systems USA.

Yet, he adds, "technology is a tool for the people in an organization. It doesn't totally replace people."

Guay says the old challenges related to security still exist—theft, workplace violence—but new ones have emerged as well, such as keeping people from bringing things into the workplace.

On the biometrics side, it's innovation that is making detection accuracy higher, while helping to drive down costs.

Toth, of GTSI Corp., predicts that the next generation of piezoelectric fingerprint recognition will take a leading role in this market, while iris recognition systems have become smaller and more practical for PC logical access.

Northrop Grumman's Dennis McCallam, technology fellow for the information technology sector, says combining cyber and security with various systems enables companies to do more than ever before. Therefore it's important to aggregate information to get the big picture, which can be achieved by layering security devices, such as biometrics, onto the network and analyzing data.

The combining of video surveillance and access control marks a big shift because of digital technology and networks.
— Fredrik Nilsson

While Diebold has been installing biometric-related systems for years, Richard Baggot, vice president-electronic security and currency systems group, says still less than 10 percent of access control is biometric.

What is selling well, he says, is a product developed two years ago that uses a biometric control on a bank vault gate or door. It does away with having someone using a second key to open a safe deposit box. "It's quick and it's efficient." In addition, explains Baggot, it is an example of products growing beyond "the typical security environment and growing into a non-typical application."

SUPPLIERS GIVE THEIR TAKE

Given the numbers cited earlier, it's not hard to understand how those participating in the security industry remain bullish on the move to digital systems, as well as the growing applications for smart cards, RFID technology and biometrics.

Ray Shilling of Canon USA's NVS Group, video division, calls the ability to capture, process, transmit and store secure data in digital formats "the most prominent feature of the physical security industry of the future."

He says once in the digital realm, the industry will expand in breadth and depth, especially in software development. It's a good news-bad news scenario for end users, he says, with the positive being more choices and the bad side being confusion over all the options.

"Technologies, such as night vision, retinal scanners, motion detection and tracking, radiation sensors and the like can be put to work," Shilling says, "adding virtual-cybersecurity guards to our workforce."

GE Security's Juan Cabezas, senior vice-president global marketing and strategic alliances, says the intelligence being added to cameras is allowing for all sorts of innovation, including the possibility of cameras doing facial recognition without being tied to a central server.

Remote monitoring, brought about by IP camera technology, will be critical in the future, says Nobu Kawaski, senior marketing manager for Sony Electronics' IP Video Monitoring Group.

Police departments will employ the technology to monitor incidents in schools and public places, he says, while others will use mobile PCs to remotely monitor events.

But despite the newfound growth in the IP security market, this area still has a few obstacles to overcome—namely bandwidth and price point.

IP cameras are "still in early stages," with bandwidth usage being the biggest concern in their implementation, said Peter Strom, chief operating officer of March Networks. "Most companies aren't willing to make the investment for bandwidth."

For some, it's not investing in the technology that is the problem but a lack of know-how.

"The traditional integrator has had a hard time keeping up with technology. More often than not, we are interfacing with the end user along with the integrator, " he said. While Strom says this can cause some friction over who owns the customers, in most cases the manufacturer and integrator see the advantages of working together on a solution.

The combining of video surveillance and access control marks a big market shift because of digital technology and networks, says Fredrik Nilsson, general manager of Axis Communications. With digital security systems employing the same networks used by IT departments, Nilsson says it opens the way for IT distributors and integrators to enter the market and build systems for customers.

But by the same token, he says, the improved functionality and affordability of video surveillance systems allows security to enter new markets, such as small offices and homes.

"I think there is an increasingly keen awareness that technology can have an impact on the bottom line," says Carey Boethel, vice president -electronic security systems division, NetVersant Solutions Inc. "But corporate security directors haven't always had the opportunity or the wherewithal to do (cost) analysis. Now they have an audience at the C (corporate) level and run the department."

Continued on page 10

Finally, a consolidated vision from the most credible publisher in Security

TechSec SOLUTIONS

Security's shift to IP, wireless, software and networking technologies

The shift toward integrated security technologies is the key factor driving growth in the Security market. Moving from an analog-based industry to a digital-based industry is dramatically affecting Integrators' business, Manufacturers' products, and End-Users' options.

TechSec Solutions will offer the most comprehensive and in-depth discussion on major changes such as:

- How emerging intelligent products and systems capture, move and store data
- How IT managers and Security managers work together and who controls budgets
- Which new technology provides creative networking solutions and drives decisions

Bringing together integrators, installers, manufacturers, security directors, and IT personnel, TechSec Solutions will give you the tools to develop your business strategies for today and tomorrow.

For Conference Information
www.techsecsol.com

Zanne Tenney Augur, Conference Manager
(207) 846 0600, ext 227
zaugur@unitedpublications.com

Organized by the most trusted and respected publisher in the Security industry

SECURITY SYSTEMS NEWS

SECURITY DIRECTOR NEWS

February 27–March 1, 2005
The Ritz-Carlton
Sarasota, Florida

The Ritz-Carlton, Sarasota is the area's premier destination for meetings and conferences. The resort offers groups a luxurious location with private beach retreat on Lido Key and is in close proximity St. Armands shopping district and various downtown diversions.

Frank Abram, vice president at Panasonic Security Systems, says providing "door-to-desktop" solutions make such security applicable for access control and IT.

Frances Zelazny, director of corporate communications for Identix, says biometrics is being looked at to help solve the identity issues raised within organizations for monitoring people as well as at borders and other checkpoints. It can also be used for doing background checks.

In the case of access control, says Bill Spence, director of marketing for IR Recognition Systems, the goal has always been tracking people, but until biometrics took off, "we've only dealt with tokens of people," he says, such as cards.

In a post-Sept. 11, world, Spence adds, biometrics has emerged as a high-security application. "What was good enough before isn't good enough now," Spence says. And with budgets finally coming into line with planning, he says, "biometrics has made the jump over the chasm from early adopters to mainstream."

John Cassise, director of national accounts at Amag, agrees the focus these days is on the credentialing process. Cards are bridging the gap between physical and IT security, he says, because a single card can handle the passwords needed for everything from doors to IT networks to e-mail.

Computer Associates' Eric Maurice, director eTrust Security Management Solutions, says the common credential not only provides more security but also more accountability with usage being tracked from a single reference point. This segues into the use of such information for auditing purposes, Maurice explains. If you get IT and security to share information, he says, security improves because you can detect patterns.

What you get in the end, Maurice notes, is better efficiency, lower cost, increased flexibility, improved security and even the ability to meet regulatory obligations, such as those set under the Sarbanes-Oxley Act.

It's about using information, not putting up higher fences, says Alan Lipton, chief technology officer and director-research and development at ObjectVideo. The challenge with physical security, he says, "is you're always fighting to keep up with the bad guys. And whatever defenses you put up, they can get around them."

The future is also about the battle between proprietary vs. open systems, and an industry currently without standards that is now moving toward regulations and best practices.

"Our industry is under increased pressure from IT to use open standards," said Jim Coleman, president of Operational Security Systems, although most companies haven't embraced it.

Coleman said security products will eventually succumb to the commoditization that has entered the computer industry "when you no longer provide the features that people are asking for."

Toth, from GTSI Corp., said the industry still has a way to go when it comes to standards.

"Currently there is no single standard that would provide secure, reliable and trusted solutions to large enterprises or to the government," said Toth. He said GTSI, through its InteGuard Alliance partners, has taken the first significant step toward bringing the physical security industry leaders together to create a fully open, interoperable, secure, reliable and trusted end-to-end physical security system."

RFID IS ON THE WAY

Another area grabbing attention is electronic article surveillance and RFID, either as integrated technologies with existing security and access systems or as standalone systems.

Hap Patterson, vice president-advanced research for Tyco Safety Products, says EAS is being used in conjunction with video and POS systems to get a better sense for what happens when an alarm goes off.

Further integration with PDAs or cell phones can provide information remotely. "The cost of computing has come down to the point where it's inexpensive. People want to see what their EAS systems are doing and once you set that computing infrastructure in place," Patterson says, "people want to get that data."

Common credentials not only provide more security but also more accountability with usage being tracked from a single reference point.
— Eric Maurice

The biggest challenge for RFID, notes Patterson, is making sure the technology isn't overhyped. While it has many applications, overselling its abilities can be as dangerous as not promoting it at all.

Allan Griebenow, president and chief executive officer of Axcess, says RFID has been successfully applied to the problems of supply chain pilferage, vehicle access control and asset management such as tracking laptops within a company.

"We also see active RFID in physical security, especially tracking personnel in a facility," says Griebenow. The technology can provide the ability to identify intruders because they aren't wearing an RFID tag.

RFID can be tied to biometrics as well, Griebenow says, with biometric information being preloaded at an access point via RFID notification so the information is waiting as the person arrives. With the biggest drawback to biometrics being its processing time, Griebenow says the use of RFID can make biometrics more employable. ❖

MARCH networks

Banking on Video Security?

March Networks' industry-leading video security systems help financial institutions of all sizes remain safe and secure.

With advanced recording and management capabilities – including ATM transaction monitoring, high capacity storage and powerful IP networking features – our DVRs are providing banks around the globe with the performance and reliability they demand.

Backed by an international network of certified security resellers, our systems and software also excel in retail, government, commercial, transit and first responder installations.

Contact us today to see how our line-up of Linux-based DVRs gets overwhelming approval from both security and IT teams.

www.marchnetworks.com
1.800.563.5564

THE CHOICE OF SECURITY AND IT PROFESSIONALS WORLDWIDE

NEW ENTRANTS

"The need for servers, complex control software and large capacity memory is the key to future systems development and expansion."
—Frank Abram, Panasonic Security Systems

They are company names that are spoken of every day—IBM, Microsoft, Cisco Systems—though not typically in the context of the physical security industry.

Yet, as security continues its migration toward a network-based platform, it seems only logical, in some minds at least, that these giants in the IT world would find the security industry an attractive market.

"I think there are many players who haven't sold security before but will get into this industry," said Carter Griffin, chief executive officer of Brivo Systems. "It will be good for the industry, provide growth for the industry, but it will be very dynamic change, as well."

Contributing to that dynamism, many say, is the entrance of non-traditional security companies. "Everything is zeroes and ones—it's all digital," explained Joe Freeman, who heads the research firm J.P. Freeman Co. "We're drifting more and more to an IT world."

As security makes this transition, Freeman said, it becomes increasingly likely that companies already conversant in IT will see an opportunity.

While some companies made their entrance into the security industry by design, others simply found the synergies between their current offerings and those also applicable to security appealing.

"We came to the (security) market by coincidence" having provided video surveillance for a client that initially needed wireless Internet connections, said Jonathan Hollander, chief executive officer and chief architect, Vigilo Security International.

Systems integrator NetVersant also found a "natural fit" between security and its business in other low-voltage applications, such as cabling, telephony, and wireless, centering its offering around the idea that wire and cable is the common denominator between these areas and electronic security, said Carey Boethel, vice president-electronic security systems division, for NetVersant Solutions.

Another way non-traditional companies are coming into the security space is through strategic partnerships, such as GE Security's partnership with IBM, said Juan Cabezas, senior vice president-global marketing and strategic alliances at GE Security. Frank Abram, vice president at Panasonic Security Systems, said his company is also going the relationship route to combine the expertise of both.

It's not a matter of whether these companies enter security, but how. Abram said it's the result of the networking nature of new security systems generating interest from the IT world. "The need for servers, complex control software and large capacity memory is the key to future systems development and expansion," he said.

Fredrik Nilsson, general manager of Axis Communications, said his company is one that is relatively new to the security surveillance market. "The security market is a conservative market and we on the IT side don't have the long term relationships with security, but we're working on building that," he said.

IT companies also present a new approach to the market, Nilsson said. "In the traditional security market, companies like to do one-vendor solutions," he said. "On the IT side, it's a best-of-breed approach."

Even with the focus on IT eyeing the security space, some don't think a wholesale takeover will happen.

"Everything is zeroes and ones—it's all digital. We're drifting more and more to an IT world."
— Joe Freeman

"I don't see IT companies coming into it," said Pacom Systems' Senior Vice President Scott Oliver. Rather, security companies will become more efficient and will compete with IT resellers coming into security as structured wiring installers. The crossover is happening on the distribution side, he said.

Consolidation, however, is a very real likelihood as the industry changes and matures. As a result, said Rudy Prokupets, chief technology officer and vice president-research and development for Lenel Systems International, the company's goal is develop a platform that can be built on and integrated with rather than acquired.

Allan Griebenow, president and chief executive officer at Axcess, said consolidation is being felt both on the manufacturing and integration side. For integrators, competition is coming from big players with Defense Department contracts, such as Boeing, "large companies that can mix and match technologies," he said. ❖

AXCESS™ RFID = Savings Security Convenience

Vehicle Access

Asset Management

Personnel Access

Wireless Sensing

Supply Chain Management

Yard Management

Personnel Access Control and Tracking
- Complete "Hands-Free" Access
- Visitor Tracking and ID Badging
- Automatic Time and Attendance Recording
- Disaster Mustering

Vehicle Access Control and Tracking
- Automatic "Hands-Free" Rolling Access
- Fleet Management
- Yard Management

Asset Management and Protection
- Complete Asset Visibility
- Automatic Inventory
- Cargo/Pallet Protection

Wireless Sensing
- Temperature and Humidity Monitoring
- Nuclear/Chemical Detection

Integrated Network Video
- Remote Live Viewing
- Surveillance Recording
- Event-Based Incident Investigation

AXCESS' Active RFID and integrated network video products provide powerful, low-cost solutions for automatically tracking, locating & monitoring people, assets and vehicles. Whether riding on your network infrastructure or integrated with existing access control systems, AXCESS' modular design allows for flexibility and ease of installation. AXCESS' ActiveTag™ readers, long range battery powered tags & family of software products combine into a powerful system that scales from stand-alone to enterprise-wide applications. To learn more about our complete line of RFID & network video solutions and where you can get them, call us at 800-588-6080 or visit us online at *www.axcessinc.com*.

1-800-588-6080
www.axcessinc.com

AXCESS™

3208 Commander Drive
Carrollton, Texas 75006
Telephone: 972-407-6080
Fax: 972-407-9085
www.axcessinc.com

"The technology shift we've seen in video has had a profound effect on the use of video."
— Peter Strom, March Networks

Given the ever-changing nature of business these days, it's difficult for even the most well-established, well-funded company to predict its longevity. Mergers take place, the economy rises and falls, events of great magnitude occur.

Still, there are steps that can and must be taken now, those in the industry say, to ensure a place in the future—whatever direction it heads in.

Key among those steps is education—both within an organization and for its partners and end users.

One way to educate yourself, says Ray Shilling of Canon USA's NVS Group, video division, is to master the principles of IP networking.

The DOD, for which CoreStreet provides scalable validation products, has been leading the way in smart cards and identification security.
—Phil Libin

"Enroll in classes, read text books—do whatever it takes, it will be worth it," Shilling says. In addition, he suggests integrators and end users get to know the hardware and software manufacturers. "As our products become more and more complex, this disconnect (between manufacturer and integrator or dealer) becomes more pronounced and must be addressed."

Ultimately, he suggests that the emphasis shift is from focusing on system features to concentrating on ease of set-up, use of the system and customer training and support.

Education also means support, says Bill Spence, director of marketing for IR Recognition Systems, which, in turn, can reduce the risk when introducing a new technology. "The security industry is all about mitigating risk, so if it (a new technology) seems too risky, people may not use it."

With technology changing as quickly as it is, customers haven't the time to do the research necessary to keep up. So, says, Marc Abbagnaro, vice president-physical security at Anixter, customers rely on partners for technology updates and to troubleshoot problems.

The training and technical know-how has to begin with the supplier or integrator, says Abbagnaro, so they can have the conversation with customers about integration, about trends they are seeing and about directions in which they should consider moving.

"You have to be willing to adapt and to shift as the paradigm shifts," he says, such as the move to network-based systems.

The industry, Allan Griebenow, president and chief executive officer at Axcess, needs to take a proactive, rather than reactive, approach. He says this positive approach should come from all sectors, including trade groups and the media.

"We have people educated on legacy technology but who are not ready for IT technology," he says. "We have to educate our industry in the aggregate to be more IT savvy."

LEADING THE WAY

The Department of Defense, for which CoreStreet provides scalable validation products, has actually been leading the way in areas such as smart cards and identification security. As a result, Phil Libin, president of CoreStreet, says security companies are looking at the steps the DOD has taken and are using it as a predictor of where things are headed.

CoreStreet has taken the approach of working with customers who have some education, or foundation, on the latest technologies in the security market.

"We've intentionally only dealt with customers with a high level of knowledge" about our technology, "but that's not an extendable market." Down the road, Libin says, "we have to get into the mainstream," going beyond the large government or corporate customers and leverage relationships with systems integrators and systems architects.

"The education piece is critical," says Scott Oliver, senior vice president at Pacom Systems' U.S. operation. Companies can no longer sell in the conventional way, but rather need to make technological training part of the sales piece, he says.

But education isn't just one sided, points out Barry Walker, chief executive officer at CoVi Technologies. To develop the proper educational and support tools, he says, "you have to

PARTNERING FOR THE FUTURE

Partnerships are part of the next wave and, in an increasingly IT-oriented environment, a key to survival, says Axis' Fredrik Nilsson, general manager. "With an IT approach, partnerships are essential," he states. "It's a much more open, community type of approach." And the benefit, Nilsson adds, is through strategic partnerships. Prices often decrease while functionality increases.

"From a sales and marketing point of view, you have to make alliances," says Doug Cram, vice president-sales and marketing for AWID. He said suppliers need to look to their existing market channels, be they OEMs or dealer customers, and reinforce and maintain those relationships.

Service and support also means proactively seeking ways to solve problems, says Holly Sacks, HID Corp.'s vice president of marketing. Sacks points to HID's hard printer testing program that tests HID cards in a variety of printers to ensure improved image quality or durability. "We do this for the benefit of our mutual customers," she says of HID and the printer companies.

Having open and interoperable products that support multiple technologies and multiple applications is another way to build for the future, Sacks says. Such products, she says, protect customers' investments and position companies as good business partners. ❖

listen to both sides of the industry (security and IT) that we talk about. Pay attention to both sides to build great products and then support the heck out of those."

Whether it's education or support, Yvonne Hao, vice president-global marketing for Honeywell Security, says it's important "to understand your customer and do what's right for them."

"The worst thing you can do," she says, "is lose sight of your customers. Despite all the changes and dynamics, we try to stay focused on the fundamentals."

But staying focused on the fundamentals doesn't mean that you shouldn't look to new ideas, Hao says. In fact, she says, companies wanting to ensure their value to customers need to constantly innovate. "To miss new innovations or to stay in stale products is a risk," explains Hao. "We have to be smart about why customers buy from us."

Juan Cabezas, senior vice president-global marketing and strategic alliances at GE Security, is also an advocate of innovation as a means to build for the future. "We will continue to innovate and transfer those solutions to things that improve the business," he says.

Pushing the envelope through continuing research and development, says Alan Lipton, chief technology officer and director-research and development for ObjectVideo, will address the industry's changing needs.

That means, Lipton says, "moving intelligence beyond software into the realm of hardware" by embedding intelligence in cameras or switches and working with other manufacturers to make this happen.

Peter Strom, chief operating officer of March Networks, said a one-time investment in security hardware can be leveraged through the addition of software that makes a security platform into a broader application.

"The technology shift we've seen in video has had a profound effect on the use of video. With the capability to transmit video over a network, there are new uses for video" that go beyond loss prevention and into operations, he said. Companies, Strom says, are viewing it as a management and a marketing tool. ❖

CONVERGENCE

Continued from page 6

to explore where the customer is coming from. According to Jim Coleman, president, Operational Security Systems, the two sides differ on their approach: Security places the higher premium on value, while "IT lives in a world where reliability is important," Coleman said.

They also differ on what they bring to the table. IT has insight into database management, WAN and LAN, "but they don't have stunning insights into security. If you allow them (IT) to dominate decisions, they may not be good decisions from a security standpoint," he said.

On the integrator side, Coleman said he sees that role as a bridge between the security director, who may or may not have an understanding of networking, and the IT department. As integrators, "when you jump into that (IT) domain, you have to know networks and all the buzzwords," he said.

Ray Shilling of Canon USA's NVS Group, video division, said just as security integrators are learning networking skills, "IT firms are also entering the marketplace by hiring security industry experts to expand into new business areas."

Hammering out funding for consolidated corporate security functions can be a significant barrier to implementing such a unified approach, said John Kronick, managing director of the North American Security Practice for GE IT Solutions.

"One of the biggest deterrents to rolling out security over the enterprise network is the hidden cost of the security solution," Kronick said, and who foots the bill hasn't been clearly articulated.

But other technical barriers still remain, said Stephen Pineau, president and chief executive officer, Viscount Communications.

With access control, "the biggest barrier to true convergence between IT and physical security is the Weigand standard that requires controllers," Pineau said. "The future will be in addressable and network readers." ❖

OPEN DOORS WITH:

R10 READERS

2K CARDS

NOW FOR LESS THAN PROX!

www.hidcorp.com

iCLASS by HID

Get more for less while futurizing your business.

iCLASS **R10 readers** and **2K bit cards** still deliver more than Prox, but now at a lower price. Install contactless smart card technology for access control today and open the door to adding future applications such as biometric authentication, cashless vending, and logical access tomorrow.

call (800) 237-7769

HID