



network *centric* Security

February 2008

WHERE PHYSICAL SECURITY & IT WORLDS CONVERGE

Clear Vision

RFID emerges as a powerful security tool

14

IP = INTEROPERABILITY (AND OTHER MYTHS)

WATCH OUT FOR ASSUMPTIONS
ABOUT NETWORK VIDEO

20

A PLACE IN THE NEW RESALE MACHINE

WHAT'S NEXT FOR CHANNEL PARTNERSHIPS?

26

EDITORIAL

Editor

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

Art Director

Dale Chinn

Publisher

Russell Lindsay
rlindsay@1105media.com

Associate Publisher/Editor-in-Chief

Security Products

Ralph C. Jensen
rjensen@1105media.com

SALES

District Sales Manager

AK, AZ, HI, ID, MT, NV, NM, OR, UT, WA, WY

Barbara Blake
972-887-6718
bblake@1105media.com

District Sales Manager

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

District Sales Manager

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

District Sales Manager

Northeast, AR, CO, LA, MO, OK, Canada
Randy Easton
678-401-5543
reaston@1105media.com

District Sales Manager

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

District Sales Manager

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

District Sales Manager

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

1105 Media

5151 Beltline Road, 10th Floor
Dallas, TX 75254

Editorial services provided by

Expert Editorial Inc.
www.experteditorial.net



CLEAR VISION

By Sharon J. Watson

From monitoring facilities to locating personnel in an emergency to deterring fraud and theft, vendors, analysts and a growing body of users say RFID is a potentially powerful security tool.

IP = INTEROPERABILITY (AND OTHER MYTHS)

By John W. Verity

Assumptions, hype and pitfalls to watch out for in the transition to digital network video.



A PLACE IN THE NEW RESALE MACHINE

By Frank Barbetta

Security companies see their marketplace in the next two years characterized by an accelerated pace of IT networks supplanting traditional analog systems and physical solutions business. This will disrupt what until now has been a linear and straightforward supply chain.

departments

6 Enter

RFID presents an opportunity for CSOs to lead the adoption of a practical, affordable means of increasing corporate security that leverages corporate IT strategy.

8 Innovate

Congress enters 2008 poised to pick up the pace on legislation that will affect corporate security and policy protocols regarding electronically stored information.

30 Launch

New applications, strategies and solutions.

32 Exit

In an excerpt from its new report, the Security Executive Council provides a glimpse of its extensive hotline benchmarking data.



The RFID Opportunity

by Steven Titch, Editor

Radio frequency identification (RFID) may not be the first technology associated with the job of CSO. In fact, throw out “RFID” to a technology analyst in a word association test and the likely comeback would be “Wal-Mart.”

True, Wal-Mart has probably the highest profile among RFID users. The big-box retailer has been using RFID chips embedded on shipping pallets and bulk packaging for more than a year to track products from assembly line to store shelf, successfully reducing inventory, transportation and distribution costs. Its methods have been adopted by many others.

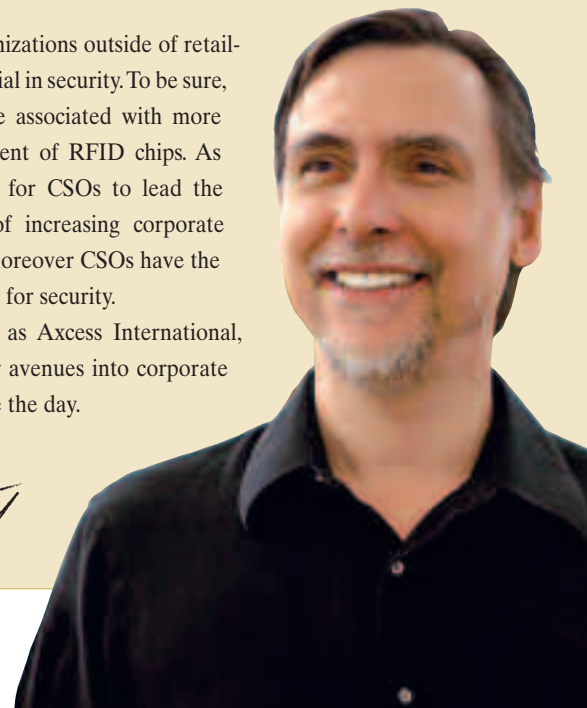
As Sharon J. Watson writes in “Clear Vision” beginning on page 24, some savvy companies see enormous security benefits from RFID, precisely because of its networkability.

For starters, at least in a virtual way, RFID increases visibility. The most seasoned CSO will tell you there are places cameras can’t go or are not effective. An RFID chip embedded in an employee or visitor badge can alert a security officer if an individual ventures into an unauthorized area. Since RFID can fit into a network-centric scheme, a signal can not only trigger an instant message, a page or other wireless alert, but activate video surveillance, if available, and move the image to a larger display screen in a control room, and document the incident in a compliant way.

For assets and property, embedded RFID is a way of battling theft, not only from inventory, but of office property. Again, through networking, RFID can stop someone walking off with a laptop by triggering an alarm at the door, and, again as part of assuring documentation, photographing the attempted theft.

What’s surprising, however, is how few organizations outside of retailing and logistics have jumped on RFID’s potential in security. To be sure, there are privacy issues, but those tend to be associated with more invasive measures, such as subdermal placement of RFID chips. As a technology, RFID presents an opportunity for CSOs to lead the adoption of a practical, affordable means of increasing corporate security that leverages corporate IT strategy. Moreover CSOs have the expertise required to successfully deploy RFID for security.

At this point, RFID system vendors, such as Axxess International, Reva Systems and ThingMagic are looking for avenues into corporate organizations. RFID is one way CSOs can seize the day.





Congress and Courts Confront ESI

by Steven Titch

Congress enters 2008 poised to pick up the pace on legislation that stands to affect corporate security and policy protocols regarding electronically stored information (ESI). Meanwhile, in the courts, new procedures regarding the discovery, submission and authentication of ESI are expected to see their first real-world tests.

The U.S. Senate strengthened identity theft and identity fraud laws in a unanimous voice vote in mid-November. The bill, the Identity Theft Enforcement and Restitution Act of 2007, among other provisions, imposes requirements for privacy and security on enterprises that maintain personally identifiable information in electronic or digital form on 10,000 or more U.S. citizens (see box). That bill now moves to the House of Representatives for consideration.

The House also passed the Internet Spyware and Protection (I-SPY) Act, which strengthens penalties against phishing and planting spyware for malicious purposes. The Senate is expected to take up the legislation this year.

For the most part, however, bills that got attention in 2007 represented low-hanging fruit that addressed voter concerns over identity theft and protection of personal data. "Threatening to damage computers; threatening to obtain information to use for extortion—there's no constituency to protest that," says Stephen Wu, a partner in the law firm of Cooke Kobrick and Wu LLP, which specializes in legal matters pertaining to information security.

The coming year may see Congress tackle more controversial legislation, including the Personal Data Privacy and Security Act of 2007, which would create civil and criminal liability for companies that do not adequately protect personal information on employees and customers. Among other provisions, the act would require enterprises to conduct risk assessments of potential security breaches, adopt risk management and control policies and procedures, ensure employee training and supervision for implementation of data security programs.

Specific parameters, however, are still up for debate. These include the question of how large a breach triggers a notification requirement, and what responsibilities the organization that suffered the breach would have toward consumers and partners, Wu says. For example, if a company loses credit card data—even if the cause is theft, not negligence—it still might have to bear the banks' cost of replacing the credit cards of consumers at risk.

"All this might mean more costs," Wu says.

IT data privacy act also calls for companies to notify any U.S. resident of a breach where it is "reasonably believed" that personal information was accessed or acquired. The "reasonable belief" phrase, observers say, will be a significant part of the debate about the bill's language. From the perspective of

Pending Congressional Legislation

S. 495 PERSONAL DATA PRIVACY AND SECURITY ACT OF 2007

Sponsor: Sen. Patrick Leahy (D-VT)

Status: Senate Judiciary Committee has recommended placement on Senate calendar

▶ Imposes a fine and/or prison term of up to five years for intentionally and willfully concealing a security breach involving sensitive personally identifiable information that causes economic damage to one or more persons.

▶ Defines "sensitive personally identifiable information" to include an individual's name in combination with his or her social security number, home address, date of birth, biometrics data or financial account information.

▶ Imposes requirements for a personal data privacy and security program on business entities that maintain sensitive personally identifiable information in electronic or digital form on 10,000 or more U.S. persons.

▶ Requires a business entity that is subject to data privacy and security requirements to: (1) implement a comprehensive personal data privacy and security program to ensure the privacy, security and confidentiality of sensitive personally identifying information and to protect against breaches of and unauthorized access to such information; (2) conduct risk assessments of potential security breaches; (3) adopt risk management and control policies and procedures; (4) ensure employee training and supervision for implementation of data security programs; and (5) undertake vulnerability testing and monitoring of personal data privacy and security programs.

▶ Requires any agency or business entity with sensitive personally identifiable information to notify without unreasonable delay any U.S. resident of a security breach in which such resident's information has been, or is reasonably believed to have been, accessed or acquired.

▶ Requires any business entity or agency that is required to provide notification to more than 5,000 individuals of a security breach to notify all consumer reporting agencies.

S. 2168 IDENTITY THEFT ENFORCEMENT AND RESTITUTION ACT OF 2007

Sponsor: Sen. Patrick Leahy (D-VT)

Status: Passed Senate by voice vote Nov. 15, 2007; awaits action in the House.

▶ Authorizes criminal restitution orders in identity theft cases to compensate victims for the time spent to remediate the intended or actual harm incurred;

▶ Expands identity theft and aggravated identity theft crimes to include offenses against organizations (currently, only individuals are protected); include conspiracy to commit a felony with the definition of "felony violation" for purposes of aggravated identity theft crimes;

▶ Eliminates the requirement that damage to a victim's computer aggregate at least \$5,000 before a prosecution can be brought for unauthorized access to a computer;

▶ Makes it a felony, during any one-year period, to damage 10 or more protected computers used by or for the federal government or a financial institution;

▶ Expands the definition of "cyber-extortion" to include a demand for money in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.

H.R. 1525 INTERNET SPYWARE AND PROTECTION ACT OF 2007 (I-SPY)

Sponsor: Rep. Zoe Lofgren (D-CA)

Status: Passed House by voice vote May 22, 2007. Awaits action in Senate

▶ Amends the federal criminal code to impose a fine and/or prison term of up to five years for intentionally accessing a protected computer without authorization to install a program and intentionally use that program in furtherance of another federal criminal offense.

▶ Imposes a fine and/or prison term of up to two years if such unauthorized access of a protected computer is for the purpose of obtaining or transmitting personal information with intent to defraud or injure a person or cause damage to a protected computer; or intentionally impairing the security protection of a protected computer with the intent to defraud or injure a person or damage such computer.

HR. 2290 CYBER-SECURITY ENHANCEMENT ACT OF 2007

Sponsor: Rep. Adam Schiff (D-CA)

Status: Referred to House Judiciary Committee

▶ Amends the federal criminal code to: prohibit accessing a protected computer to obtain a unique identification number, address or routing code, or access device; revise the definition of "protected computer" to include computers affecting interstate or foreign commerce or communication.

▶ Expands the definition of "racketeering" to include computer fraud; redefine the crime of computer-related extortion to include threats to access without authorization (or to exceed authorized access of) a protected computer; impose criminal penalties for conspiracy to commit computer fraud.

▶ Imposes criminal penalties for damaging 10 or more protected computers during any one-year period.

S. 2213 CYBER CRIME ACT OF 2007

Sponsor: Sen. Orrin Hatch (R-UT)

Status: Referred to Senate Judiciary Committee

Amends a loophole in current law to make conspiracy to commit extortion through a threat of damage or impairment of a computer a crime.

the security process, it is likely to create greater demand for standards on internal corporate data classification as enterprises deal with identifying which information assets are stored where.

Two technology trends, however, raise compliance concerns over the way information can be catalogued and how access to it can be controlled. The first trend, virtualization, has led to IT environments where information is housed across multiple storage

hardware, which appear to the user to be one large repository. The second is the decreasing size and cost of high-capacity storage devices, such as flash drives, which can be used to illegally copy data or simply be stolen outright.

Meanwhile, several versions of identity theft, cybersecurity and anti-spyware legislation are moving through the Senate and the House and could possibly be combined at some point. In general, the bills, which contain a number of overlapping provisions,



Stephen Wu

make it a felony to conspire to attack a computer network, or hack one with the purpose of stealing information.

E-DISCOVERY

In the courts, the new year likely will see wider application of new federal rules that have standardized e-discovery procedures in state courts. These new rules became effective December 1, 2006, but given that it takes an average of 18 months for most civil actions to reach trial, Wu reckons 2008 will be a watershed year as attorneys and judges gain first-hand experience with the new rules.

The rules establish a chain of methods that attorneys can use to get ESI from an organization. Many are basic. For example, they allow litigants to request data in specific formats, such as TIFF, JPEG and PDF. Overall, Wu says, the rules have both benefits and drawbacks. On the upside, they create higher standards for the authentication and validation of the data than an affidavit or testimony from a CSO or CISO; they call on courts to push plaintiffs and defendants to demonstrate objectively that the information represents what they claim it does.

The downside, however, is that e-discovery could be used as a tactic to overburden opposing litigants—or worse, win sanctions against them—by forcing them to slog through voluminous records, Wu says.

Either way, the procedures mark the beginnings of a “sea-change in the way litigation is conducted,” Wu says. Discovery data will increase geometrically. “Vast quantities of information will overwhelm the paper-based paradigm. All courts will have to come to grips with ESI.”

Since 2001 Brussels Airport has relied on IndigoVision's IP Video for CCTV Surveillance



7 Years - Field Proven
700+ Cameras
40 Workstations
1 Integrated Solution

IP Video and Alarm Management
www.indigovision.com



Circle 406 on card.



feature

Clear Vision

RFID EMERGES AS A POWERFUL SECURITY TOOL

By Sharon J. Watson

A large German manufacturer wanted to reduce its operating and data storage costs while increasing the security efficiencies of the several hundred video surveillance cameras it uses to monitor a huge production facility.

To accomplish this, the firm placed radio frequency identification (RFID) tags on all the assets passing through the facility. The tags use WiFi-based Active RFID technology from AeroScout Inc., in Redwood City, Calif.

RF “exciters” placed at strategic doorways throughout the facility signal any tags entering their coverage area. The tags respond immediately, enabling the network to precisely locate the tag. Once located, a local video camera begins recording in the tag’s area, so that cameras now record only when and where an asset is physically present.

“Whenever a tag is on an asset, you have complete visibility of it,” says Amir Ben-Assa, industry solutions marketing director for AeroScout.

Visibility—of something or someone and whether they are or are not where they are supposed to be in space or time—is RFID’s key attribute for security. The technology uses tags—a microchip combined with a tiny antenna—and readers to enable companies to track the location of products, tools, personnel and activities.

Tom Schuster, CEO of Reva Systems, based in Chelmsford, Mass., says the technology gives security personnel a multifaceted, comprehensive view of the critical assets they must monitor. “RFID enables you to see individual items alone, as they come together with other items, and as they change,” he says.

From monitoring facilities to locating personnel in an emergency to deterring fraud and theft, vendors, analysts and a growing body of users say RFID is a potentially powerful security tool.

KEEPING PERSONNEL VISIBLE

Placing RFID tags on employee, guest or contractor ID badges enables companies to define and enforce restricted areas and equipment and control access to them.

Occidental Petroleum Corp. uses Axxess International’s Active Tag RFID solution for hands-free access control at the company’s Elk Hills Reserve field in California. Occidental has used more than 14,000 tags to monitor employees and on-site contractors since December 2005. The system also gives the company time and attendance records required for safety reporting as well as a reliable locator system in case of emergency.

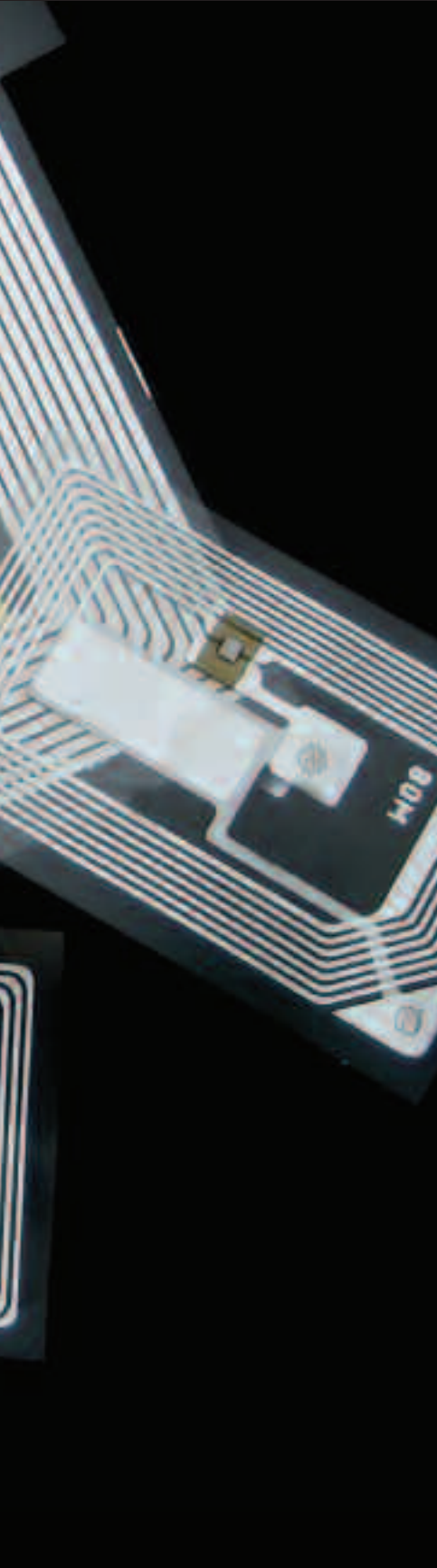
“The badge looks a lot like a proximity card but has a long range,” says Allan Griebenow, president and CEO of Axxess, based in Carrollton, Texas.

The Port of Barbados also uses an Axxess personnel monitoring solution that is exception-based. If a person’s RFID tag registers them as being out of place, an email, page or wireless alert is automatically sent. “That increases the productivity of security personnel,” Griebenow says.

CHAIN OF CUSTODY

RFID tags also can associate specified users to specific pieces of RFID-tagged equipment, such as keyboards, factory or medical tools, vehicles, even filing cabinets and the documents within them. The tags can offer a record of who touched what when.

University Medical Center in Tucson, Ariz., uses AeroScout’s WiFi-enabled active RFID tags with its Philips Asset Tracking Solution to monitor the location of thousands of medical devices. The tracking, with Web-based location tools, enables the



RFID: Ready for the Corporate Network

Just three or four years ago, most RFID applications were stand-alone implementations based on proprietary tags and readers. Their goal was to comply with mandates from Wal-Mart or the Department of Defense that required their suppliers to tag pallets.

In a short time, the industry has come a long way from “slap and ship” RFID to embracing standards that help ensure interoperability among RFID components within enterprise network applications. The maturing of RFID makes it even more effective as a security and business tool.

“It’s actionable data from RFID readers that gives the technology greater value in an enterprise,” says Tom Schuster, CEO of Reva Systems in Chelmsford, Mass.

STANDARDS FOR SHARING

Most compliance-driven RFID applications aren’t designed to share data. That’s changing, as new generations of RFID support networking protocols such as Transmission Control Protocol/Internet Protocol (TCP/IP) and 802.11 WiFi standards.

That makes it possible to effectively use WiFi network access points to read tag data. AeroScout Inc., Redwood City, Calif., makes WiFi-enabled RFID tags that communicate with access points from major vendors like Cisco Systems, Aruba, Trapeze and others.

Using WiFi access points allows RFID to be deployed without RFID readers, though most vendors say they expect to see a mix of increasingly intelligent network-based read-

ers as well as access points used for gathering RFID data.

In addition, leading vendors comply with standards from EPCglobal, an international RFID standards body. Key standards are the Generation 2 UHF protocol for transmitting data, the Electronic Product Code (EPC) standard and EPC Information System (EPCIS) standard, designed to let disparate business applications share EPC data gleaned by RFID readers.

INTERPRETING THE DATA

Even standards-based data from readers must be aggregated and filtered for use in Enterprise Resource Planning (ERP) or other enterprise applications. This data massaging is typically done today in a layer of middleware. Middleware also enables users to set rules for alerts triggered by tag movements or additional data from sensors embedded in RFID tags.

Reva System’s Tag Acquisition Processor (TAP), a firmware device that collects and interprets standard data streams from RFID readers, can give users multiple perspectives on the same tag reads. A logistics expert might dissect the efficiency of the product’s manufacturing flow, while a security expert examines how often the product passes doors and windows that should be secured.

RFID is most successful when it’s implemented to solve more than one problem, say vendors and analysts.

“Get a partner who understands the business problem you’re trying to solve,” says Schuster.

hospital to quickly locate critical equipment across nine floors comprising about one million square feet. Faster location means better patient care. It also tells administrators who the last user was, in case the device is damaged or lost. That means

point. If a delivery customer says an item is missing, the specific item can be traced back to individual cameras at each step so that Sony can verify whether it shipped.

“This was a project that had to stand on its own legs as an RFID application and

A growing body of users says RFID is a potentially powerful security tool.

units can be held accountable for damages.

To verify its shipments of consumer electronics products, Sony Logistics Europe is using an RFID deployment from Reva Systems.

In a large distribution warehouse in Holland, Sony labels individual goods with RFID tags. An automated MPEG4 video surveillance system records the tag reads during item picking, packing, pallet wrapping and truck loading. Further, the tag data is burned into the video stream at each

bring security results,” says Schuster at Reva Systems.

“Loss prevention is key throughout the supply chain and retail,” says Dimitri Desmons, director of RFID marketing for Impinj, Inc. in Seattle, Wash. A luxury goods manufacturer is using Impinj chips to deter counterfeiting. By incorporating an RFID tag into its product packaging, would-be counterfeiters would have to duplicate the tag to get away with duplicating the product.

CUSTOM IS COMMON

While RFID’s security applications are easily categorized into tracking personnel and assets, companies are unlikely to find pre-packaged RFID solutions from vendors.

“There is no off-the-shelf RFID,” says Ravi Pappu, co-founder and head of the advanced development group for Thing-Magic in Cambridge, Mass. Further, he notes that even the widespread standardization of RFID components doesn’t guarantee plug-and-play applications. “There’s some black magic that goes on to make an RFID system work,” he says.

Some vendors offer RFID solutions for specific industries they claim can be deployed relatively quickly for applications with well-defined limits, such as complying with a larger trading partner’s RFID tag requirements. T3Ci and BEA Systems offer a solution combining RFID tags, readers and analytics.

Impinj and a group of allied vendors

are offering semi-packaged “functionality” for pharmaceutical, media/entertainment, apparel, food safety and other vertical market applications. The supporting companies include epcSolutions, GlobeRanger, InSync Software, OATSystems, Omnitrol Networks, Scout Software, Systech International, Tacit Solutions, Vue Technology and Reva Systems.

Packaging vendors could offer additional near-ready-made RFID applications. Pliant Corp., a Schaumburg, Ill.-based stretch film manufacturer, has partnered with PowerID in Petah Tikva, Israel, to create tamperproof stretch film. The solution involves electrically connecting a PowerID battery-assisted RFID tag to a wire wrapped with the stretch film around a shipping pallet. Cutting the film ensures the wire is cut too, thereby breaking the circuit and making the tag unreadable.

“This is a solution for valuable or sensitive shipments,” says Jeff Middlesworth,

principal development engineer at Pliant, noting that customers must be willing to balance the added security with the cost of the tag.

SECURING BUSINESS BENEFITS

RFID applications easily cross security and business lines, with applications designed for process improvement leading to more security and vice versa.

Schuster cites a Reva Systems client that uses RFID tags to automate inventory counts when loading and wrapping pallets to improve security. Automating the reads meant the company could stack the goods higher on pallets because personnel no longer had to physically reach items to count them. In turn, the higher pallet stacks led to less handling, more efficiently packed trucks and fewer truck runs.

Capitalizing on the fact that RFID used for security can solve business issues too can help make the business case for RFID

Privacy and Personnel Matters

A potential drawback to using RFID to monitor personnel is running afoul of current or proposed privacy laws. However, RFID proponents point out the safety benefits of RFID-based badges are an excellent counter to privacy issues, at least in an emergency.

“Knowing who exactly was in the facility, where they were, and whether they exited can be the difference between life and death,” says Daniel P. Mullen, president of AIM Global, in written comments to *Network-Centric Security*.

ThingMagic, which makes chips and software for RFID tags, learned this firsthand when its personnel evacuated their building in December 2006 because of a fire. In the chaos, it wasn't clear if everyone had gotten out. The company's programmers rigged a simple system using a Google Maps API and tag reads to locate employees.

“In those kinds of situations, people really want to be found,” says Ravi Pappu, co-founder and head of the advanced development group for ThingMagic. “The notion of privacy invasion went away.”

Those Terrific Tags

Tags—microchips and antennas—are the heart of RFID, containing data about an object or person being monitored. The tags come in three varieties: passive, semi-passive and active.

Passive tags are the least expensive, because they have no power source of their own. To transmit, these tags must reflect power from a reader. The drawback is that readers must be very close to the tag. By contrast, semi-passive RFID tags have a small power source, like a battery, to boost their signal to a reader.

Active RFID tags, the most expensive option, have an embedded power source so they can transmit signals independent of readers. This transmission capability makes Active RFID tags ideal for real-time location systems (RTLS) and for use with sensors. The tags can answer queries or send an alert when a sensor threshold is reached.

“Powered RFID changes the spectrum of security,” says Allan Griebenow, CEO of Axxess International, in Carrollton, Texas. Griebenow says active RFID provides greater flexibility and accuracy for security and business requirements. “You can rely on the tag read,” he says.

Stimulating an active RFID tag to reveal its data or location is a key function. Axxess's technology “wakes up” a tag with hidden antennas. AeroScout's “exciter” tools accomplish a similar function over a WiFi network.

Almost anything can be tagged via RFID. In November, Axxess introduced DOT, a battery-powered wireless computer as small as a grain of rice. Its first user will deploy it with personnel, assets and vehicles.

RFID tags also can be combined with sensors that can measure temperature changes, motion, humidity, chemicals, even the presence of combustible gases. Active RFID and sensors could provide another array of powerful security tools.

security applications.

“For high value items with a street value, [real-time location systems] or tamper-resistant asset tagging can provide a real ROI [return on investment] if losses are significant,” according to Daniel P. Mullen, president, AIM Global, an RFID industry group. In a written reply to queries, Mullen also noted that security might be the only business case for protecting data on laptops and removable media.

“Considering the potential embarrassment and legal/financial penalties for data loss these days, the ROI is fairly easy to calculate,” he wrote. ☞

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



IP=Interoperability (and Other Myths)

WATCH OUT FOR ASSUMPTIONS ABOUT NETWORK VIDEO

By John W. Verity

Who'd of thought something as humble as the Internet Protocol (IP) could roil the video surveillance market so?

IP-based cameras, networks and other gear promise not only to drive down hardware, installation, operations and maintenance costs—they also will greatly improve video imagery, make possible innovative new surveillance techniques and facilitate video's integration with other security systems and with IT in general.

IP brings video into the information technology mainstream, enabling cameras and other hardware to take advantage of the mass-market's economies of scale. With IP, standard Ethernet-based networks treat video imagery as just another type of data—albeit a rich and somewhat bulky one—that can be recorded, analyzed and

viewed anywhere on the Internet with something as compact as a handheld phone or PDA—a big help for first responders.

For all its promise, however, IP isn't magic. Just because two products employ IP and its fellow traveler, Ethernet, it does not mean that they will immediately be able to work together in any useful way. Yet, many customers expect that kind of plug-and-play facility. They equate "IP" with "open architecture" and assume it will enable them to mix and match hardware devices and software regardless of brand. In fact, while adopting IP certainly is a big step towards creating an open architecture for all kinds of security systems, including

video, it doesn't solve all problems of interoperability. For now, some open architectures are more open than others.

NO SHAME IN CONFUSION

Actually, customers can be excused for being confused right now. The video surveillance market is growing fast, and the change from analog to digital is nothing short of radical. Moore's Law, which states that computer processing power doubles every 18 months, enables digital products to evolve extremely rapidly. That puts some major market positions at stake.

So, while smaller manufacturers are open to accusations of overselling IP video's ad-

vantages, the larger, analog-centric makers are not above poo-h-pooing the new technology as overly complex, relatively expensive and less than rock-solid. Typical of the doubts they've been heard to raise: Would you trust something as critical as physical security to a PC-based server that might have viruses or need rebooting once a day?

"IP networking has excellent potential," states Steve Surfaro, group manager and strategic technical liaison at Panasonic, a leading maker of analog gear. "Is it unstoppable? Absolutely. But there will be a gradual progression. Analog will always be there, even if gets relegated to entry-level products."

So far, digital technology has had its biggest impact at the head-end, in the equipment that records and displays video signals. The shift to digital recording has shifted innovation almost entirely to software, which has not always been the strongest suit for the established providers. GE, Bosch, Panasonic, Honeywell and Pelco, among others, have responded mainly in two ways: moving to acquire makers of digital gear and software, and striving to innovate more in the area of cameras. Increasingly, intelligence is being built into cameras themselves, a move that is directly facilitated by IP.

SMART CAMERAS

While continuing to sell a full line of analog cameras and digital encoding/decoding equipment, Bosch Security Systems is growing its line of intelligent IP-based cameras. They can perform the kinds of analytics that have usually run in centralized servers: analyzing traffic patterns, detecting loiterers, and noticing objects that get left behind as someone leaves a scene. "The beauty of this is that the camera decides by itself to report what it sees," says Bob Banerjee, product marketing manager for IP video products at Bosch. "The distribution of intelligence means a fundamentally different total cost of ownership. You can have a camera in Outer Mongolia. This is a world where not everyone has high band-

width networks."

Bosch, Banerjee states, is determined to drive down the price of its intelligent cameras to the range of \$200 to \$300 per unit and "bring analytics to the masses."

PRICING AND QUALITY

Panasonic is actively innovating in IP cameras, too. It is fleshing out a line of Ether-

net-ready cameras while adding IP encoding to certain analog models. The latter, says Surfaro, still have some advantages in low-light surveillance, for instance, though digital technology is fast-improving there, too. Certain situations, he says, are still tackled best with a combination of analog and digital cameras.

Panasonic is putting special emphasis on

exacqVision®

Advanced IP Video Surveillance Solutions

- Smart Solutions: NVR, IP software, hybrid systems
 - Powerful monitoring features included
 - Megapixel IP cameras and analog cameras
 - Open integration with other systems
- Simple, cost-efficient IP camera licensing
 - One easy to use, powerful interface

exacq Technologies www.exacq.com • 317.845.5710

Entire line is completely Scalable

Circle 410 on card.

Just because two products employ IP and Ethernet, it does not mean that they will immediately be able to work together in any useful way.

improving image quality because it sees that as a key differentiator versus the many consumer-class IP cameras now flooding the surveillance market. High-resolution images from cameras that have multi-megapixel sensors will be a big help with the coming wave of new image-processing and analytic techniques. "Pricing is a serious problem as the industry moves to IP," Surfaro says. "Other makers are not investing in image quality as much as adding IP transport." By tapping its heritage in broadcast video, Panasonic hopes to distinguish itself from the pack.

Panasonic is also readying a line of surveillance monitors that use the same High Definition Multimedia Interface (HDMI) used in home television setups. This will help the company to ride the consumer market cost curve.

Another company with a strong analog legacy is Pelco. "We continue to sell a lot of analog products," says Rob Morello, product marketing manager for digital systems. "Enterprise customers are all looking for IP. But a lot of these customers don't want to do forklift upgrades, and their analog equipment is not fully depreciated." Pelco's answer has been to bring out a matrix digital decoder that enables IP cameras to operate as an extension to analog networks. It's selling this directly to customers and also plans to sign up other manufacturers to resell it.

FEW OTHER CCTV STANDARDS

Morello says that as a whole, the IP surveillance market is still short on industry standards. Unfortunately, Pelco is not a big enough business to dictate standards, especially in the face of the much larger consumer and PC markets. That provides an opportunity for Pelco and other companies to select a few standards—for digital video compression, for instance—and throw their weight behind them as a way to help securi-

ty systems integrators. "We will provide free APIs to others," says Morello.



Eric Fullerton

ty systems integrators. "We will provide free APIs to others," says Morello. Among those others are Milestone Systems and OnSSI, which make PC-based video management software. By necessity, each has had to work hard in educating the marketplace about the benefits of IP networking and digital video. "We believe we are making the video server industry more horizontal," says Milestone's Eric Fullerton, chief sales and marketing officer. Old-line analog vendors, he says, have traditionally been vertically integrated, making everything from cameras to storage systems. "IP is enabling the decoupling of hardware from software."

Milestone, he says, has designed its software to be open to many different suppliers' gear, including more than 35 brands of camera. "We aim to provide more choice in best-of-breed hardware, applications, and storage." Certain competitors, he says, have tried to "create vertically-integrated stacks of technology" that often include proprietary cameras. "We want to help people bust out of proprietary jail."

Gadi Piran, president of OnSSI, offers a similar story about open architecture, claim-

ing his company's NVR software works with some 300 IP cameras, across a broad range of quality, features, and pricing. He notes that for each type of camera, OnSSI may have to develop specialized software to handle control functions such as pan, tilt, and zoom, but the actual video images it records arrive in one of only a few fairly well-accepted standards.

CISCO LENDS ITS WEIGHT

If there's any company whose name is synonymous with IP, it's Cisco Systems, the leader in IP-based networking gear. And Cisco has made it very clear that it has serious plans in the area of IP-based video and in all forms of physical security. If nothing else, IP-based video will help drive demand for Cisco's network routers and switches, which are and will be the core of its business.

Cisco's vision of video surveillance networks is modeled on what it has accomplished in IP telephony: The IP network is not simply plumbing, a means merely of moving bits from here to there; it also provides a range of technical services and serves, in essence, as a platform on which other companies and customers themselves can build applications. Unplug a Cisco IP telephone in your company's office in California and reconnect it in the Paris branch office, for instance, and the company network will automatically detect the change and act accordingly. Your calls will be forwarded to Paris and all of your directory services and other information will be available exactly as if you were in the home office. Equally important, since the network recognizes the device as a

Glossary

API (Application Program Interface): a set of routines, protocols and tools for building software applications. (Webopedia)

HDMI (High-Definition Multimedia Interface): A licensable audio/video connector interface for transmitting uncompressed, digital streams. HDMI connects digital audio/video sources, such as a set-top box, a HD DVD Disc player, or a PC to a compatible digital audio device and/or video monitor. (Wikipedia)

iSCSI: A protocol that allows clients to send SCSI (Small Computer System Interface) commands to SCSI storage devices on remote servers. It is a popular Storage Area Network (SAN) protocol.

Plug in to the future of CCTV

Bosch IP Network Video



Warning: Avoid the perils of CCTV.
IP video networking. With Bosch's IP Network Video line you can leap into new markets plus migrate existing systems without sacrificing investments in analog products. Simple to install, Bosch IP allows your customers to store video in one location and then view it from anywhere in the world. And network reliability is no longer a concern thanks to our exclusive technology. Ready to take the first step? Contact us today – we have the solutions, support and expertise that will take you into the future of CCTV.

CCTV: 866-CCTVREP
Bosch: 800-289-0096
www.boschsecurity.us



BOSCH
Invented for life

phone, it will prioritize any traffic headed its way to make sure the audio they're carrying suffers no degradation because of packet delays.



Bob Beliles

It should be the same with video, says Bob Beliles, senior manager of physical security market management at Cisco: "Once the network is a video platform, it will be much easier and faster for integrators and dealers to install new systems. Developers will be able to add more features and networks will be much easier to scale."

This will require makers of edge devices such as cameras to embrace certain standards, "but that's the beauty of standards," Beliles says. "Anyone can implement them. And if they do, any vendor's product will communicate with any other vendor's product."

The alternative is the maddening process of developing interfaces to help different products interoperate. Says Dennis Charlebois, Cisco's director of product management for physical security: "In our experience, easily 19 of 20 companies will say they do something [as defined in a technical spec] when actually they do not. This creates a lot of pressure and wastes a lot of money." Building to a set of standards will assure everyone of some level of basic interoperability. Says Charlebois: "The challenge will be in getting something out there that people will adopt. We must collaborate with others to establish standards."

INSTALLED BASE TO PROTECT

As Cisco sees it, the first standards to get in place will be at the edge, inside cameras. Following that is middleware, the software that integrates video with other security systems with analytics and perhaps even CRM systems. Other standards will be needed to deliver video for viewing on desktop workstations and mobile devices.

Cisco's hardly ignoring the sizeable number of customers still using analog networks and cameras. Its acquisition of SyPix Networks brought it software and hardware technologies that enable analog video networks to IP-based setups. "This enables us to provide a hybrid environment," Beliles says.

Whether Cisco can successfully leverage its unsurpassed networking know-how into the security market remains to be seen. And how well old-line providers can navigate the technical and economic changes wrought by IP is another big question mark. Perhaps the only sure bet is that eventually, and probably sooner than later, IP will dominate video surveillance as it has just about every other field on which it has set its sights. ■

John W. Verity is a free-lance writer based in South Orange, N.J. He can be reached at john@jverity.com.



WHAT'S NEXT FOR
CHANNEL PARTNERSHIPS?

By Frank Barbetta

A Place in the New Resale Machine

Wisely prepared companies in the resale channel will continue to benefit from the new, emerging climate of security and IT convergence. Along the way, channel executives envision an increase in new partnerships and tighter handshakes on existing relationships among the security industry's manufacturers, distributors, systems integrators and value-added resellers.

Security companies see their marketplace in the next two years characterized by an accelerated pace of digital information technologies (IT) and Internet Protocol (IP) networks converging into and supplanting the traditional analog systems and physical solutions business. This stands to disrupt what has been a linear and straightforward supply chain: Manufacturers sold to distributors. Distributors sold to a network of contractors, installers and dealers.

The entry of companies such as Cisco

Systems, Electronic Data Systems, Hewlett-Packard and IBM, which bring their own structured channel partner networks, has sent tremors through the traditional supply chain. Established contractors now find themselves faced with the task of developing new skill sets to deal with the IT aspects of the job. The good news is that IT companies show signs of reaching out to contractors and installers of video and access-related security systems (see "Changing Channels," *Network-Centric Security*,

August 2007). The downside is that these established players will now be competing with the IT reseller channel and may have to share sub-contracted business with other integrators. On another front, there have been reports of distributors themselves bidding on large security projects in direct competition with their dealer base.

A late 2007 canvassing of manufacturers, distributors, systems integrators and value added resellers (VARs) strongly suggests a consensus toward a positive yet sometimes

disruptive and challenging outlook within the third party channel environment as many participants position themselves for changing times.

Channel businesses may stop short of formal joint ventures and merger and acquisition (M&A) activities, but manufacturers aren't ruling out such developments. French manufacturer Schneider Electric's \$1.54 billion acquisition of Clovis, Calif. video management system vendor Pelco this past October could be a representative pace setter.

In addition, local and regional security companies are closely watching several large diversified electronics vendors and generalist system integrators—such as Cisco Systems, EDS, EMC, Hewlett-Packard, IBM, Science Applications International Corp. (SAIC) and Seagate—that will be showing increased interest in the business over the next 12 to 24 months.

Meanwhile, the overriding imperative among dealers and installers is to avoid stepping on each other's toes in competitive bidding contests and to gauge arguably threatening collisions with the national brand name vendors seeking major contracts that include security criteria. To date, however, security executives surveyed aren't reporting any low-ball or margin-squeezed bids by such large companies. Several security integrators, in fact, see new opportunities when IT vendors pursue multimillion dollar contracts directly with end-users. The way the IT channel works, large chunks of those contracts will filter down to VARs, who end up in a sub-contracting role. The key for a physical security installer or integrator, then, is repositioning the business to be a credible IT VAR.

STRENGTHENING PARTNERSHIPS

Meantime, the relationship equity that security contractors and integrators have built with customers has not escaped the notice of big IT equipment distributors. The convergence trend is motivating them to beef up their security product portfolios and strengthen their integrator partnerships with sales leads and other third party support programs, says Robert Hile, vice president of business development at IT, network systems and broadband integrator Adesta in



Robert Hile

“The IT types of distributors are adding value to spur purchases of all sorts of products,” he added. “They really are doing a good job stepping up to the plate. I don't really see anything that would stop this movement. Traditional distributors of security products aren't reaching out as much.”

Hiles sees an accelerating evolution in the new security IT distribution model. “We'll see more creative ways to help us get business and make money,” he says. “Some companies are putting feet on the street to get deals and bring in the integrators. But the traditional security guys will be the most challenged to maintain their piece of the market share.”

John Gaillard, president of security distribution at value-add distributor Scan-



John Gaillard

Source Inc., Greenville, S.C., agrees. “We are continuing to see the convergence trend move forward as we thought it would,” he says. “IP forecasts are reasonable, and we will see some big shifts in buying habits. There are lots of traditional analog systems being sold, and there are still many applications for that. But more IT integrators are seeing the IP opportunity and the future someday will be 100 percent IP, albeit not overnight.”

According to Gaillard, IT integrators bidding in the traditional security marketplace has now become “a fact of life,” although whether the IT integrators are from software, server, computer system or networking worlds may be somewhat mud-

dled. Video security is the priority for newcomers, he said, with some interest in access control systems likely to follow.

“A full suite of security will be the eventual goal, and the smart ones are looking to IT for all this,” Gaillard maintains. “The pace is being set by end-user bids for computers, telecom and such—with security being added. Some traditional security dealers are struggling with all this and not getting the bigger picture, but the risk is that if they don't migrate, they lose the ability to sell to the customers. For the most part, IT integrators understand what will be happening.”

MORE INTEGRATION

“Where we're going a couple of years down the bend—as so much depends on cost as physical security migrates over to IT—is to better reposition physical security in relation to IT,” said Art



Art Morrison

Morrison, operations manager at value-add distributor ProTech Security, North Canton, Ohio. “The vendors with the best toys will sell the sizzle and show how it can be done. People will find the money because they want good working systems. As cameras get smarter and have more features, as access control gets bigger and as smart analytics increasingly surface, we'll see more integration.”

Morrison said he is looking to public address intercom, speaker and paging systems for mass alerts as another potential up-and-comer for the IT/IP/security convergence mix. He also foresees more competition among smaller companies from both the physical security and IT sides of the fence.

AN INCREASING SKILL MIX

“We're starting to see an increasing mix of security people and IT/networking types getting involved in physical security and surveillance,” said Robert Lecher, owner

‘What ends up winning is the best channel program regardless of technology.’

—Joseph M. Heinzen, e-Convergence

and president of value-add distributor Re-Logix LLC, Shelby Township, Mich. "There are also people from the automation business starting to look at this market as a potential growth area."

Lecher sees a continued repositioning and re-education among manufacturers, distributors and resellers alike. "This is part of the challenge that will continue with the existing security base," he said. "I see people with the knowledge of IT technology move into the physical security space and see that transition being easier than the traditional security people learning IT."



Dvir Doron

For iomage, a maker of digital signal processor (DSP)-based video surveillance devices, encoders, IP cameras and analytics software tools, distribution is paramount in its effort to reach mid-range markets, said Dvir Doron, marketing vice president with the Herzila, Israel, headquartered company.

With U.S. offices in Denton, Texas, iomage has reps, integrators and distributors in its U.S. lineup, including e-Convergence Solutions of Centreville, Va.; Northern Video Systems of Rocklin, Calif.; and most recently, Supercircuits of Austin, Texas.

Doron says the companies need the ability to reach mass distribution markets, but he adds that large systems integrators are in the field with direct end-user bids at the high end of the market. It remains questionable whether either approach will emerge as dominant within the next two years, but right now the overall value proposition offered by IT/IP and security keeps competitive price, margin and shakeout pressures at bay.

One of iomage's distributors likens the current security environment to the voice business's early digital technology migration, culminating with the voice over IP (VoIP) invasion.

"The data VARs got it but for many of the voice VARs, it was 'never the twain shall meet,' right?" remarks Joseph M. Heinzen, president of e-Convergence. "Now much has changed in the market due to that conversion mix and migration. The transition is similar with adding physical security and video to IT and IP."

"There could be a shakeout of distributors and resellers relative to sales strategies

The 900-lb. IT Gorillas

Do IT companies stand to be friend or foe? Either way, they will change the way security integrators do business. Skeptical segments of the resale channel tend to see the likes of Cisco, EDS, HP and IBM as 900-lb. gorillas that can cause havoc even when it's not intended.

However, optimists believe these beasts can be tamed.

Several channel players pointed out that Cisco Systems' approach is to understand the security business and position distributors to help resellers increase margins. Cisco, which has made several investments and acquisitions in recent times to enhance its system resource and network security offerings, is well known for elaborate third party certification and partnership programs in multiple industry segments.

Robert Hile, vice president of business development at Adesta, maintains many vendors of IP-oriented surveillance systems, service platforms and software will continue to look to the traditional security channel for reseller partners. Nonetheless, he also believes security resellers who seek these partnerships must be prepared to adjust to the more structured channel programs typical in the IT supply chain. This usually involves a willingness to commit management and employees to ongoing training, qualification and certification. The result, however, can be the rewards of new, more in-depth business. Cisco's channel program is typical of this approach, and the company has expressed interest in the traditional security channel in numerous forums. HP, IBM and Seagate are likely to follow Cisco's path, Hile says.

Joseph M. Heinzen, president of e-Convergence, agrees. Major systems integrators interested in physical security are looking at third parties to handle contracts, and such vendor companies as IBM and HP are developing channel plans comparable to Cisco's.

Channel executives for the most part foresee large national companies bidding mainly on the largest of commercial, corporate and government contracts, with security a part of the larger action. "The large integrators will always be there," said Art Morrison, operations manager at ProTech. "Let them play in their own markets. They really don't pose a threat to me and many others."

and IT knowledge, and this could impact manufacturers also," Heinzen continues. "What ends up winning is the best channel program regardless of technology. I think it's going to happen quick, with video now following the pattern of VoIP [Voice over Internet Protocol]."

'LINES IN THE SAND'

Channel executives, however, don't foresee formal joint ventures and M&A maneuvers among their peers—IT distributors, integrators and resellers.

"The lines in the sand are still clear enough for most of our businesses that we don't have to share investments and revenues in a true JV," Adesta's Hile remarks. "The models are still very different. And I think the manufacturers will stay away from integrators to avoid end user bidding conflicts."

Gaillard also warns of end-user bidding conflicts if competitors blur the distinctions between distributor, installer and integrator. "These can be disruptive strategies within the channel," he says. "The classic supply chain views each party as having a role to play. If everyone does their work, the supply chain works."

Heinzen of e-Convergence said past instances of security distributors selling against their VARs were "horrible" developments, but he foresaw future corrections of such practices. "There's a conflict if distributors sell direct to end users, and such companies eventually can be out of business," he adds. ☹

Frank Barbetta is a free-lance journalist based in Little Falls, N.J. He can be reached at frank_barbetta@yahoo.com.

Applications, Strategies, Solutions



1 Chicago PD Opts for AirVisual

AirVisual Inc., a solution provider for the enterprise security and public-safety market, has deployed its IntelliViewer 2.0 software for use by the Chicago Police Department. The system, purchased and integrated by RMS Technology Solutions, has been added to the existing camera network to give the CPD the ability to deliver pre-recorded and live video and other critical information to computer terminals and mobile devices. The system also gives the CPD the ability to integrate disparate security surveillance systems onto a single emergency response platform, while delivering the information wirelessly to responders over any network and to virtually any mobile device.

The open-architecture, IP-based platform connects to video sources, access control, RFID, sensor networks, and performs adaptive routing, optimization, distribution and delivery of content based on a rules-based system.

www.airvisual.com

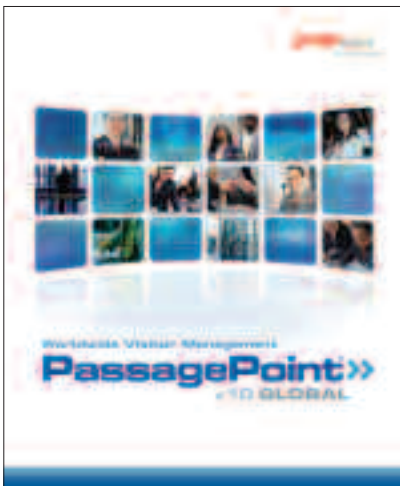


2 STOPware Visitor Management System

STOPware Inc. has released a new version of its visitor management software (VMS) system that can control global facilities access and management from a centralized location. PassagePoint Global v10 offers integration with IT infrastructure to link to any ODBC or LDAP directory systems, as well as the capability to create a directory of hosts, and link to Active Directory to leverage single sign-on capabilities.

The software is compatible with most major access control manufacturers and can accommodate biometric scanners to allow repeat visitors to sign in by scanning their thumbprint. The upgraded version also supports PassagePoint Mobile, software that allows security personnel to process visitors at any location with a wireless handheld device.

www.stopware.com



3 DVTel SOC Software

DVTel's latest release of Latitude NVMS V5, a component of its unified intelligent Security Operations Center (iSOC), is a fully scalable, standards-based, enterprise-level multimedia management system. This advanced network-based system's architecture permits simultaneous monitoring of video and audio, live and recorded, from multiple stations. The software can be configured to store and view from one to thousands of cameras and monitor connections across an unlimited number of servers. All the necessary networking, computer workstations, servers and storage hardware are available off the shelf. Latitude V5 integrates fully with existing legacy CCTV equipment and all third party hardware and software solutions.

www.dvtel.com



4 Bosch Security Software

Bosch Security Systems has introduced a modular software program for small to medium businesses that require a high level of security but do not currently need a large-scale system.

Bosch's Access Personal Edition is designed for retail stores, office buildings and manufacturing facilities. The software supports up to 2,000 users, 64 readers and 16 workstations. It communicates with Bosch's Access Modular Controller hardware platform via TCP/IP and RS-485 connections.

The Access Personal Edition solution includes a data management system for personnel information, access profiles scheduling and visitor management. Anti-passback capabilities and automatic card cancellation after expiration give administrators the ability to protect against unauthorized use of access cards. The software uses a Windows-based interface. Users can define access privileges, time schedules and door parameters to meet their specific needs.

www.bosch.com



5 Imprivata Access and Authentication Software

Imprivata Inc. has released a new version of its OneSign platform, extending OneSign's identity-centric access and authentication services across system and geographic boundaries with complete distributed management, delegated administration and business continuity capabilities. With OneSign Version 4.0, security professionals can implement integrated authentication management, single sign-on and physical/logical convergence functionalities in a fully distributed enterprise environment.

The software allows a single centralized employee IT access policy to determine every aspect of access across all users, all rights, all locations and all conditions. OneSign delivers these capabilities without requiring changes to existing IT and physical access infrastructures.

www.imprivata.com



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

On the Hotline

By Kathleen Kotwica



Report Provides Foundation For Effective Action

Historically, corporations have struggled to accurately assess hotline performance because they had nothing to compare it to. They could collect data on their own hotlines to see how many reports had been received and what action had been taken based on those reports. But with no way of knowing how those numbers stacked up against those of comparable organizations, they couldn't draw any reliable conclusions about the quality of their hotlines and reporting programs.

For the second year in a row, the Security Executive Council has joined forces with The Network Inc., the leading provider of ethics and compliance hotline programs in the U.S., to create the *2007 Corporate Governance and Compliance Hotline Benchmarking Report*, which provides more extensive hotline benchmarking data. The 2007 report breaks out the

data by industry and by year, and it presents several data points in the form of rates instead of percentages, which controls for data variations between industries and business sizes.

The report is based on an analysis of more than 277,000 hotline

The report is based on an analysis of more than 277,000 hotline incident reports from more than 650 organizations.

incident reports from more than 650 organizations across all major industries over a five-year period. Participants—or those who made reports—may be employees, former employees, vendors and the public. The data was masked to protect confidentiality.

Findings that accounted for aggregated frequencies across five years included:

- ▶ For those reports where case outcome was provided, most reports (65 percent) were serious enough to warrant an investigation and 45 percent resulted in corrective action taken.
- ▶ The research showed that half of the reports received concerned personnel management incidents. Beyond the personnel management category, company/professional code violations (16 percent), employment law violations (11 percent) and corruption and fraud (10 percent) were the most commonly reported incidents regardless of industry.

Aggregated rate data for 2006 only included:

- ▶ A rate of 8.3 incidents was reported per 1,000 employees overall (regardless of incident type).
- ▶ Smaller organizations showed a general decrease of incidents reported over time. Mid-sized and larger companies showed a general increase of reported incidents over time.

continued on page 34

DEVELOP A PLAN

But even with all these improvements, like any other report, the value of this study lies not just in the data, but in what can be done with that data.

First, comparing the numbers alone won't provide you with a complete picture of your hotline's performance. Unless you look beyond the numbers to consider all the potential explanations of why your program varies from the average, you'll still be missing critical insights that could change the whole direction of your program assessment.

For example, after reading the report's assessment of reporting rates, you determine that your organization, given its size, should be receiving eight to nine calls per 1,000 employees. You are only receiving three per every 1,000. This result may be an indication that your organization has far fewer compliance issues than its peers and competitors. While that may be so, it is not the only possi-


ble explanation. You'd likely receive fewer calls than average if company employees were being intimidated by their managers into keeping mum about misconduct concerns. Or, perhaps your awareness program isn't what it should be.

Once you have studied the benchmark data presented here and considered why your numbers are higher or lower in various categories, share what you have found with your partners in other business units. Internal Audit is no longer the only player in compliance and misconduct. Many of the issues examined in this study will impact Human Resources, Legal, IT, and Corporate Security and Safety, among other departments.

Organize a team with representatives from every affected business unit to pinpoint the problems or accomplishments behind the numbers and determine how to correct any shortfalls.

After you've determined what actions

should be taken, present your findings to management and explain how you intend to use the report to help better calibrate your hotline program. Show management that you've organized a collaborative effort to improve performance and tell them what you are doing with the information you have acquired.

Protecting brand image, people, organizational growth and stakeholder confidence are at the roots of what should be driving how you measure the success of your program. 

Kathleen Kotwica is vice president-research and product development for the Security Executive Council. This article is excerpted with permission from the SEC's 2007 Corporate Governance and Compliance Hotline Benchmarking Report. Download the entire report from <https://www.securityexecutivecouncil.com/public/surveys/index.html>.

Network-Centric Security e-news

Now available **in your in-box** twice a month

Join over 30,000* integrators, end users, installers, contractors and IT professionals who get the most up-to-date network-centric security news delivered to their desktops twice a month.

Publisher's Own Data

Sign up now at
www.secprodonline.com/mcv/newsletters/

network  centric
Security

Where Physical Security & IT Worlds Converge