

# THE Journal

## November 2007 — Special Feature

### Does the Eye Spy?

by Matt Villano

*Around-the-clock video surveillance is the Holy Grail of K-12 safety efforts. But it raises many questions, including whether or not the cameras are a wholly benign presence.*



**SOME OF THE WORST COLLATERAL** damage from a tragedy doesn't occur till after the smoke clears; namely, the usurping of the name of the location where the event took place, which over time gets repurposed into metaphor and served as a caveat. Vietnam has resonated for decades as a reference to protracted war. Kent State is likewise laden with meaning. And now, Columbine and Virginia Tech have become ingrained as shorthand for campus killing sprees. Both events pointed up in the starkest way the fragility of school security and ratcheted up safety efforts at educational institutions across the country.

At the head of every school's security wish list is video surveillance, which districts are embracing at breakneck speed. In the "School Safety Index," a report released this past summer by technology reseller CDW-G, 63 percent of the 381 responding districts said they have installed security cameras, with many more considering their use over the next two years.

Still, finding those solutions is a process rife with obstacles. "In terms of technology, video surveillance is one of the most challenging decisions a school district can make," says John Navarro, senior systems integrator for Phoenix-based Stanley Security Solutions. "It's one thing to have cameras; it's another to be strategic about them."

How, then, can a district be strategic? Naturally, by doing its homework.

### LENS CAP OFF: CHECK!

READY TO LAUNCH VIDEO SURVEILLANCE IN YOUR SCHOOL? SOME KEY ISSUES MUST BE RESOLVED BEFORE THE CAMERAS START TO ROLL.

- Make sure the local area network has enough bandwidth to support the cameras.
- Install backup power sources, critical in the event of a blackout.
- Purchase enough storage to record at least 30 days of video and keep it on site.
- Invest in an insurance policy that covers damage to cameras.
- Inform teachers that they are going to be recorded.
- Notify parents that their children will be recorded.
- Establish a liaison with the local police department so you know whom to contact in the event of an incident.
- Set up a real-time interface with sex-offender databases to keep track of predators who might enter the school.

### Choosing Wisely

Once you've decided you want video surveillance, the first big issue is picking cameras. This can be a tricky proposition—so many bells and whistles, such a limited budget. Granted, district officials don't have as many options with video surveillance as they do with, say, laptops, but a sizable camera purchase requires some key decisions before an investment can be made.

There are two basic camera systems: closed-circuit television and internet protocol (IP). Historically, the natural progression has been for schools to start with a CCTV system and build out from there. This approach connects a network of off-line analog cameras to a recording unit tucked away in a closet in the principal's office. The upside is affordability (the cost is usually less than \$25,000) and ease of installation. The downside: Most basic systems usually record over stored footage every five to seven days, meaning it's perfectly possible for an incident to be erased.

More-sophisticated systems fall into the category of IP video surveillance. IP runs over a district's local area network, receives power over Ethernet, and sends images over the internet from the camera to a server, digital video recorder, or other storage device.

Officials at **Scarsdale High School** in Scarsdale, NY, opted for IP surveillance when they worked with reseller Select Telecom to upgrade school security after students started a fire in a stairwell last year. Technology consultants configured a separate Ethernet backbone for the cameras, then set up 30 Axis 210 network cameras from Axis Communications in trouble areas the school identified in cafeterias, hallways, and classrooms. With the cameras in place, a four-terabyte network video recorder from Axis was installed to manage video intake and store it on the back end.

Though Scarsdale does not have someone watching the video 24/7, John Trenholm, director of facilities, says the new system already has yielded dividends—after a graffiti incident earlier this year, technologists went back, reviewed the footage, and apprehended the kids responsible.

"In the past we would have had no idea how to go about finding the culprits," says Trenholm, who adds the entire implementation cost roughly \$75,000. "With this technology, we were able to resolve this situation immediately."

### MPEG-7: A NEW STANDARD

**THERE'S A BRAND-NEW STANDARD FOR VIDEO SURVEILLANCE** that incorporates analytics and a technology dubbed "computer vision." Its name: MPEG-7. Unlike better-known video standards MPEG-4 and H.264, MPEG-7 is not about compression, image reproduction, or pixels. Instead, MPEG-7 is a standard for describing multimedia content data that supports some degree of interpretation of the information's meaning, which can be passed on to, or accessed by, a device or a computer code. In the K-12 environment, districts

purchase technology that relies on MPEG-7 to automatically detect when and where a school may be experiencing a security breach.

In the industry, the standard is known as the "multimedia content description interface," and it represents information about content, instead of content itself. Because of this metadata approach, the standard is not aimed at any one application in particular, but includes:

- a set of description schemes and descriptors
- a language to specify these schemes called the "description definition language" (DDL)
- a scheme for coding the description

Goals for this standard are clear. Developers at the Moving Picture Experts Group designed it to provide a fast and efficient videosearching method, describe main issues about content, index a range of applications, and inform how objects are combined in a scene. For more information, visit this site.

### **The New Order**

Just as televisions are going high-def, so too are video surveillance systems. The best camera systems can now make picture resolution up to 12 times greater than traditional analog video.

One of the vendors in this space is CoVi Technologies. In September 2006, the company helped technologists at **Berkshire Junior-Senior High School**

for at-risk children in Canaan, NY, install several HD cameras and a series of distributed media managers to store the video collected by the cameras. In all, the system monitors 17 buildings.

Harith Flagg, the school's chief executive, says the system is a tremendous improvement on the old technology, which produced video footage that was grainy and often unusable.

"The system provides a level of video quality that fundamentally changes the nature of video surveillance," says Flagg. "It allows us to dramatically increase the level of detail of student and faculty incidents, improving our response time and allowing us to reduce investigation time as well."

Many of the newest camera systems also incorporate a form of artificial intelligence known as video analytics, or "computer vision." This software-based technology, which adheres to the MPEG-7 standard (see "MPEG-7: A New Standard"), can be added to a regular camera or video server and analyzes content as it streams through the interface.

In a nutshell, software from the leading vendors in this space—which include ObjectVideo in Reston, VA; Eptascope in Sunnyvale, CA; and Nice Systems in Rutherford, NJ—decouples the two critical components of intelligent video surveillance: analysis and interpretation. In some cases, the software is embedded in cameras or servers themselves. In other cases, the artificial intelligence capabilities can be added to existing equipment, turning something as archaic as CCTV into a more advanced approach.

Once programmed with what appears to be a normal frame of reference, the software recognizes variables and sounds an alarm when something appears out of the ordinary. If, for instance, a particular camera is trained on a gate, the software will alert users when the gate is breached.

Luis Lajous, vice president of sales and marketing at Eptascope, says the technology doesn't eliminate the need for humans, but it makes their jobs infinitely easier. "With this technology, you can have one operator monitoring 50 cameras at once," he says. "Without it, how many cameras do you think one person would be able to view adequately at one time?"

### **CASE HISTORY**

Throughout the early part of this decade, **Farragut High School**, on Chicago's West Side, experienced about 100 fights per year before installing closed-circuit television surveillance equipment. Since the cameras were put in place in 2003, only three fights have occurred, and other violence, such as stabbings, has disappeared.

#### **Assessing Trouble Spots**

Whatever technology a district selects, Kenneth Trump, president of National School Safety and Security Services, a consulting firm in Cleveland, says that even the most sophisticated systems are worthless unless they are configured to make a difference.

"Security equipment is only as effective as the weakest link in the human chain and the strategies behind it," he says.

Thus, a key consideration in setting up a video surveillance system is making sure the cameras are trained on all the right spots to provide maximum coverage for a district or school. Often, this is accomplished with a security assessment. During this process, security consultants come to a school district and watch entry and egress points for a period of time. Consultants also read through incident reports to see if particular areas of a school are notorious for graffiti or fights or other forms of violence.

Peter Martin, president of Martin Security Systems, a security consulting firm in Peekskill, NY, has done dozens of these assessments over the years, including a recent evaluation for the Union City Board of Education (NJ), and says this kind of foresight usually yields the highest returns.

"If you're putting in a video surveillance system just to have security cameras, sure your campus will be safer, but you're not getting everything you could," he says. "If you do some research and put the cameras into areas that you've identified as trouble spots, the investment will pay dividends you can appreciate much more directly."

Another consideration is archiving video. Most vendors and school board policies suggest that districts keep archived video for anywhere from 30 to 45 days. Still, Patrick Fiel, the former security chief for the **District of Columbia Public Schools** who now works with security service provider ADT on school security projects, says schools easily could archive video of incidents for a year without incurring much added expense.

Fiel hails affordable hard drives and inexpensive CDburning technology for making this possible. He notes that the one-year mark is a safe bet because civil suits can arise up to 12 months after a given incident.

Mark Wojtasiak, channel market development manager for video surveillance at storage vendor Seagate Technology, agrees. "The best systems are those that store video for a while," he says. "Security in general and surveillance in particular are two areas in which the philosophy 'Better safe than sorry' applies."

## links

- **ADT**
- **Axis Communications**
- **CDW-G "School Safety Index"**
- **CoVi Technologies**
- **Eptascope**
- **Martin Security Systems**
- **National School Safety and Security Services**
- **Nice Systems**
- **ObjectVideo**
- **Seagate Technology**
- **Select Telecom**
- **Sony**
- **Stanley Security Solutions**

## Private Matters?

A familiar flashpoint connected with video surveillance is privacy. On one side, parents don't like the idea that their children are being watched. Teachers worry that nothing is sacred. Even school visitors have complained about being videotaped. The opposing side contends that the cameras aren't there to watch, but to protect.

The bottom line, of course, is that if the cameras are in public places such as hallways, cafeterias, and entrances, there should be no assumption of privacy.

"If you see the cameras, you have to assume they're capturing your image," says Al Solis, director of facilities at the **Morgan Hill Unified School District** near San Jose, CA. Solis and his technology teams recently installed more than 60 SNC-RZ25 cameras from Sony at a number of schools in the district— and then had to respond to a sizable number of parents concerned about their kids' privacy.

There are ways to pacify those who are uncomfortable with being subjected to constant video surveillance inside school grounds. A best practices document released by the Arkansas School Boards Association recommends that in the event of an incident, districts blur out the faces of non-involved bystanders before releasing the video to police. The document also tackles the sensitive subject of determining who (beyond authorities) gets to see surveillance footage of an incident.

"Parents of students 'inadvertently' caught in the video do not have the right to inspect," the document reads. "Please note, however, that if a student was not 'involved' in the altercation prompting the disciplinary action, but happened to get pushed by one of the students in the fight, the pushed student's parents have the right to review the video."

Privacy considerations have a flipside, too. Bob Kirby, senior director for K-12 education at CDW-G, notes that while 63 percent of 381 respondents to the company's school security survey say they have cameras, only 24 percent reported having real-time access that enabled them to compare images of visitors to sex-offender databases.

As Kirby explains, these statistics indicate that school officials who insist on blurring the images of non-involved bystanders also could be inadvertently blurring images of potential predators in their midst. "It's as important for districts to know who is trying to gain access to their campuses as it is to watch them once they are there," he says.

Restraint is a virtue whenever considering what security measures to take. But it's ultimately trumped by common sense. In the words of Solis, "Privacy is important, but at the end of the day, it's up to us to make sure the schools are safe."

*Matt Villano is a freelance writer based in Healdsburg, CA.*