

The new technology of campus security

IP and networked environments allow for better-coordinated surveillance and faster campuswide notification

By L. Samuel Pfeifle, editor, Security Systems News

In the weeks following the Virginia Tech shooting, Security Systems News polled our readers about what might improve campus security going forward, and what hinders security, if any such obstacle exists, on U.S. campuses today. Of 114 respondents to our survey, who answered seven questions and offered long-form essay answers, 81 percent said universities were not currently taking full advantage of the high-tech security offerings on the market.

This should come as no surprise. Integrators and installers are well aware that security is often seen as a cost center, and is not a budget line item that often gets significantly increased year to year. Roscoe Coffman, operations manager for access control software manufacturer Open Options, perhaps puts it most bluntly: “Most college and university administrators are woefully uninformed about the capabilities of current systems ... most would be astounded at the fact that critical video call-up, access control

environment, 32 percent said surveillance systems, with another 15 percent saying analytics should be layered on top of that video, but 29 percent of respondents chose “Other” and gave a wide variety answers that ranged from “training and arming faculty” (some might not consider that a “technology”) to “mass notification systems” (the most common answer). Of the remainder, 16 percent chose smart card-based access control, 5 percent listed contraband detectors, and 4 percent said biometrics-based access control could be best utilized to strengthen campus security.

Mark Craft Blacksburg, Virginia Tech Class of '91 and vice president at Professional Technologies, had this to say: “More than any previous generation, this generation of college students has grown up under electronic surveillance with an unprecedented expectation of safety. We, their parents, have employed baby monitors, nanny cams, web cams and security systems for their protection since birth. School time brought CCTV surveillance, access cards and cell phones. Less afraid of ‘big brother’ than previous generations, they are accustomed to being supervised with technology. The question is: How far must this society go in order to feel safe?”

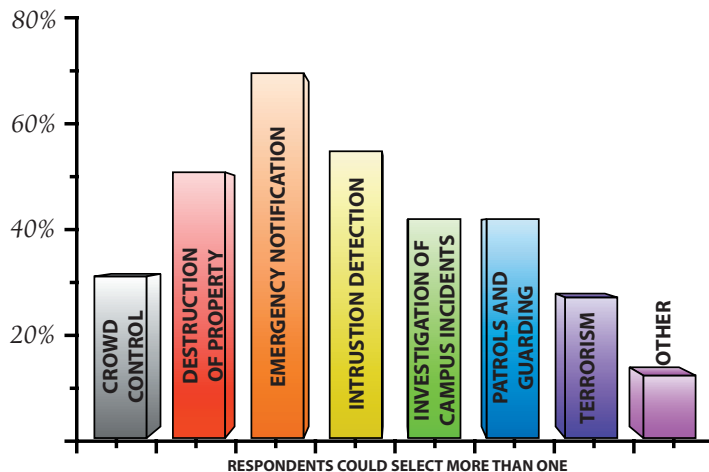
Just in the last few months, Western Nebraska Community College, the University of Iowa, and Virginia Commonwealth University have announced additional video surveillance projects. IP camera maker CoVi Technology has installed cameras at the University of Maine, Endicott College and the Berkshire Farm School in the last year. These are only a small sample of the surveillance jobs completed on campuses in the last few years. Clearly, video surveillance, often with IP-based video management software, is being rapidly adopted by university and college security directors.

However, it is notable that mass notification was the most common “other” response. We at SSN did not offer it as a selection in the poll when it was issued in May, but since that time the industry has been abuzz with mass notification talk. At the June NFPA show in Boston, mass notification was inescapable and a number of companies, including Send Word Now and Vasona, have recently released new products or rapidly increased their marketing.

This should not be surprising in consideration of integrators’ perception of security directors’ needs. When asked to list the prime concerns of their customers, integrators only reached a majority on three answers: destruction of property (51 percent), intrusion detection (55 percent) and emergency notification (69 percent).

Largely because of feedback like this from its customers, Oregon-based security systems integrator Selectron has teamed with

WHEN TALKING TO CAMPUS SECURITY DIRECTORS, WHAT ARE THEIR MAJOR CONCERNS?

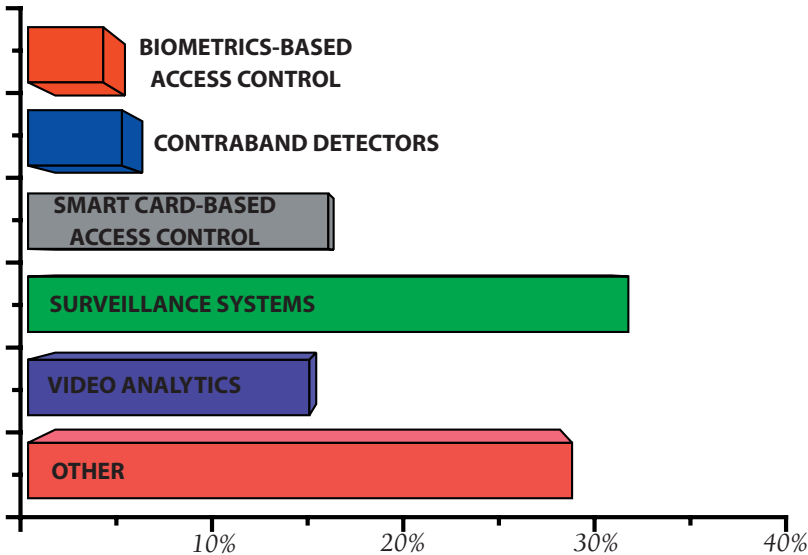


lockdown and campus-wide audio annunciation can be accomplished with a single mouse-click.” This presents a clear opportunity for integrators to educate school officials and get them up to speed on the capabilities of a new security system.

However, there was very little consensus on what technology could best help a campus environment (and many made the point that there’s little difference between securing a school campus and the campus of a Fortune 500 company). When asked to choose a single security technology that would most benefit a campus

SECURITY IN A CAMPUS ENVIRONMENT

IF YOU HAD TO CHOOSE A SINGLE SECURITY TECHNOLOGY THAT WOULD MOST BENEFIT THE CAMPUS ENVIRONMENT, WHICH WOULD IT BE?



mass notification software firm Vasona Technology to launch a Campus Public Safety Case Study Program, which will include free installations on select college campuses and a recently completed campus security seminar, held July 9 and 10. The mass-notification software that companies like Vasona make is increasingly of interest to campus security directors, who want to avoid the confusion that gripped the Virginia Tech campus.

Selectron systems engineer Gary Clark, who's been with the company 14 years, said technology advancement in recent years has greatly advanced the ability to move information around a campus. The move to a networked environment has allowed access control and video management manufacturers to increasingly integrate disparate systems, he said, and "these systems do a wonderful job of collecting alarm data and collecting video, but the question is, 'When it comes into the system, who sees it?' At this point, it's only the security manager or the guard on duty." Now, he said, with software like Vasona's, which is loaded directly onto the local network, "information can be transmitted to the people that need to know what's happening, but also to literally anybody in that facility, be they students, or workers, or engineers, whomever—every single laptop, every single pager, every single cell phone, in a matter of seconds."

Other mass notification products from companies like Send Word Now, MadahCom, Honeywell, GE Security, Siemens, Dedicated Micros and Simplex Grinnell offer similar capabilities, though they differ in respect to having an audio component, whether they will actually take over linked computers instead of just sending emails or texts, and in other ways.

However, paramount is that the message gets out to everyone simultaneously. This all-inclusive thinking is becoming dogma in the end user community. It's no longer okay for them to have their access control, intrusion, video and notification systems working independently. Jeff Sturza, a sales engineer at Security Corp., which will soon complete an installation of 1,000 IP cameras in the

Saginaw, Mich., school system, said, "the most important thing for the security people is to have one system that does everything." As part of a sales and marketing program like Learn Safe, manufacturer/integrator MDI can, for example, not only link a video image to an individual card swipe, the company's technology can also provide the background-check information about the individual pictured, if it's an employee, or a student's personal file. Security directors might be amazed by the advances in security technology, but networks, the Internet and the new browser-based world isn't lost on them. It's how they do their HR administration and their payroll, why shouldn't their security work similarly?

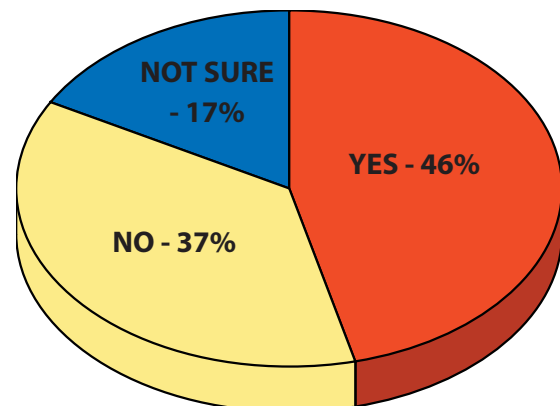
"The IT department is calling the shots today," said Sturza, echoing a number of interviewees over the past year. "Nothing is going to happen unless the IT department gives it their blessing."

Other departments can be instrumental to the sales cycle as well. For instance, the marketing department. "There are several colleges and universities that are using the current security technology on their campus along with a guard or police force, showing a proactive approach to protecting students, faculty and staff," noted Jim Geyer, general manager of SST, Midwest Region, and those colleges are beginning to tell people of their efforts.

Forty-six percent of integrators feel that schools will begin to make their security capabilities part of their recruiting efforts. "Typically, the moms and dads are paying for their child to be there," said Mark Day of Industrial & Commercial Security Systems. "The universities can sell the security option to the parents as a viable, safe place to go to school."

If an integrator is prepared ahead of time to sell to more than just the security department at a university, college, or municipal school system, it's possible the technology will be seen as more than just a cost center. Further, it's possible that budgets other than that of the security department can be accessed. "Previous thinking," said Walt Bodner, loss-prevention manager at Securitas Security Services, "about security systems' return on investment and the value they add are going to be turned upside down, now."

DO YOU SEE COLLEGES AND UNIVERSITIES USING SECURITY SYSTEMS AS PART OF THEIR RECRUITING?



The holistically secured campus

As technology improves, security directors are wise to remember technology is just a piece of an overarching plan

By Rhianna Daniels, editor, Security Director News

The past 12 months have been tough for schools. The Virginia Tech shootings that left 32 dead and the standoff at an Amish school that killed five still linger in the minds of many security directors in educational environments. It's a changing world with more possible threats to assess than ever before: terror-

ism, workplace violence, student violence, sex offender breaches, et al.

to school security that incorporates everything from employee screening to video surveillance to emergency notification. "To be effective in creating a secure, open environment requires the development of a plan from a holistic approach," said Robert Benedetto, chief of security for Hartford County Public Schools. "All stakeholders have to understand what true objectives are and what you are willing to compromise to reach that goal. Every plan should be viewed as a living document that is constantly reviewed and practiced."

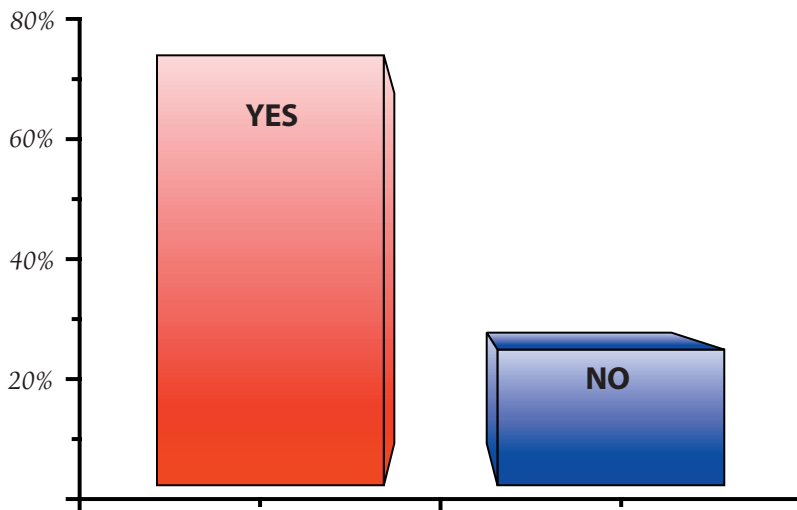
Recent events have served as a wake-up call for school security, propelling many school districts to fast-track plans to install security technology such as CCTV and access control systems, at times without considering how the technology fits into the overall plan. "Unfortunately, [fast-tracking] is exactly what happens, whether it is localized or nationalized, when it is multiple incidents happening across the country," said Steven Kaufer, a consultant with Inter/Action Associates, "School boards react to parents and public pressures, and then they start looking at ways to respond to that."

The response is not always the most appropriate, Kaufer noted, as school officials, looking to appease parents, decide to increase security in what could be considered as a public relations move rather than a security-based decision. For example, installing metal detectors, which are a visible deterrent.

One positive aspect that comes with this increased awareness is that school board officials may be more open to changing security measures, and have more leverage to allocate funds for such changes.

Funding is a constant challenge for school districts in regards to all ends of their businesses. Teachers need more compensation, facilities need to be upgraded, new books need to be purchased. It is no surprise that security funding is not a top priority unless the school board comes to the conclusion that the risk of an incident is high enough to warrant stripping funds from its core

HAS THE VIRGINIA TECH TRAGEDY PROPELLED YOU TO TAKE AN ADDITIONAL LOOK AT SECURITY AND CRISIS-MANAGEMENT PLANS?



ism, workplace violence, student violence, sex offender breaches, et al.

According to a *Security Director News* poll, 73 percent of respondents reported that the Virginia Tech tragedy propelled their security departments to take a closer look at its organization's security and crisis management plans.

Jim Black, security consultant with TRC Security, said a crisis like this naturally urges stakeholders to have discussions regarding the state of emergency preparedness at their organizations and evaluate if changes are necessary in the short term and the long term.

Technology is only one part of the solution. Most school security experts recommend a "holistic approach"

business: educating students.

In 2006, Anne Arundel County Public Schools faced a cut in the security funding it expected to receive for the upcoming school year. Ed Piper, then the county's supervisor of security and currently president of Homeland Security Consultants, said at the time that the county had requested \$2 million to install cameras in all of the district's 33 middle and high schools. Instead it received just over \$1 million. He and other school officials were forced to take a look at reallocating resources.

"The strategy has to be multifaceted," he said, "with policies, procedures and training complemented by technology. Technology itself does not solve all the problems."

Instead of spending funds on cameras, Piper focused on implementing crime prevention through environmental design at the schools.

"How you design and maintain the schools and relationships with the community are paramount to keeping schools safe and secure," he said.

The fact that schools are centers of their respective communities, Piper said, should make security and emergency planning a top priority in the minds of administrators.

One of the major challenges security directors in educational facilities face is finding the balance between security and an open campus that regularly hosts various vendors, parents, its students and teachers, as well as other schools traveling to campus for sports and educational events. In our survey, 66 percent of readers said they do not think open environments can be effectively protected from such incidents.

"Open environments cannot be adequately protected, only managed through emergency response systems," said Ron Woodson, director of security and safety for the Center of Forensic Psychiatry. "It would do more harm to even think that an open environment can be protected. It would be a very bad illusion to create such a false sense of security."

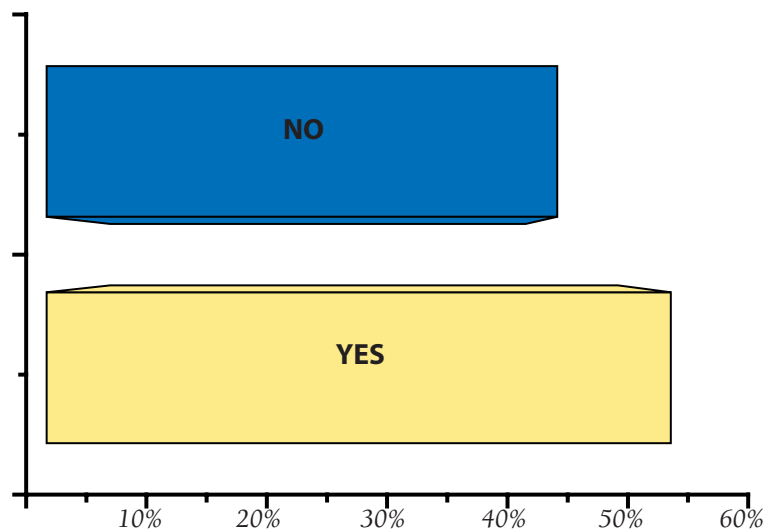
Charles Sheridan, a lieutenant with the Dallas Police Department at the University of Texas Southwestern Medical Center, noted that any organization can come up with a plan, training, equipment and funding, "but I don't think realistically anyone can ever fully plan for a scenario that resembles anything like what Virginia Tech endured."

Black said the open aspect of campuses is inherently part of the learning environment and is a hallmark of campus life and changing that is "counterintuitive to the culture."

Benedetto with Harford County Public Schools said school administrators want to project an open, inviting atmosphere, while the police would like to see limited access. "This is where the negotiating and compromising ensues," he said.

"Increased security measures may infringe upon the open environment that universities have enjoyed," commented Mark Grabowski, director of safety and security at Southwest Baptist University. "The cost of losing some of the 'open environment' may be the only choice to miti-

IS YOUR MANAGEMENT PLAN TESTED ON A REGULAR BASIS?



gate the risk of further tragedy."

Florida is one state that passed legislation in an attempt to limit access to its campuses, in effect making them less "open." In 2005, state lawmakers passed The Jessica Lunsford Act, which requires anyone working under contract with state school districts to submit to fingerprinting and background checks by the Florida Department of Law Enforcement and the Federal Bureau of Investigation before entering school areas. The development of the law, which was enacted in September 2005, followed the murder of Lunsford by a convicted sex offender.

Broward County Public Schools, which is the nation's fifth largest school district and accounts for 270,935 enrolled students this year, installed technology it dubs the STAR — Security Tracking and Response — system, which provides an electronic method to identify volunteers and contractors on school property. The solution checks applicants against the nationwide sex offender database, as well

SECURITY IN A CAMPUS ENVIRONMENT

as state and local law enforcement databases.

“This gives us an opportunity to focus on what we feel are our priorities, which are knowing who is coming on campus and making sure that the people that are working with our students are the right ones,” said Dr. Joseph Melita, executive director of the special investigative unit and professional standards for Broward County School District.

While many schools have implemented visitor management systems to better control campus access in recent years, Broward’s stands out because it is networked through the district’s 264 schools, enabling the locations to share the same information.

Paige Tarver, account executive with system provider Johnson Controls, said the system enables the district to screen its entire roster of volunteers — previously it could only check a small number.

This was a capability the school needed and John Ritter, branch manager for the Southeast and Southwest for Johnson Controls, said the system was fully customized and tailored specifically for Broward County. This customization allowed Broward to choose what databases individuals were screened against, instead of working with a pre-programmed solution.

Melita noted that the days of having an open campus are long gone as the current world climate has changed the face of public schools.

“One of the things I have learned since Columbine, Sept. 11, and everything else, is that this is the new norm,” he said. “What used to be is no longer the correct guidelines. We use technology in the hopes of giving parents reassurance that the district and their child is safe.”

“There is a balance,” he said. “You want to focus on education, but you want to keep an eye in the back of your head. Schools that are in suburbs or in small towns or suburban areas—anybody’s a target.”

Many security directors realize this and are forcing administrators to take a look at what technologies will best mitigate threats on their campuses. For example, Endicott College recently added IP surveillance cameras from CoVi Technologies, while the University of Alaska at Anchorage just added an emergency notification system from 3n. Sarasota County School District just integrated 800 Samsung cameras into a video management system. Ike Sloas, Oklahoma City Community College’s security director, added a surveillance solution to increase monitoring of the school’s parking lot.

Since Virginia Tech, the technology in the industry that has received the most buzz is emergency notification systems — schools are hoping that these solutions will help solve the communication problem Virginia Tech experienced the day of the shootings.

Michael Sherer, chief strategy officer for emergency notification service Send Word Now, said the company was barraged with calls from various educational institutions just a few days after the Virginia Tech shootings because they had decided to “fast track” upgrades to crisis management and security plans.

Another area — not technology related — that is a focus currently is emergency planning. In our survey, 55 percent of organizations practice and test their emergency plans on a regular basis.

“A lot of districts have plans in place, but they are hiding in a black binder out back,” he said. “Some of these plans are personalized with names and some of those people are no longer with the school.”

Because of this reason — and a host of others — it is crucial for security officials to be involved in maintaining security plans.

Technology installations and internal planning go a long way toward creating a safer campus, but

after an installation is complete, and a plan is created to utilize the technology, educating the community is a part of the process that should not be overlooked.

Kaufer said one of the most important aspects to minimizing community concern is for security leaders to be educating residents about security programs on a regular basis, not just as a reactive measure.

“Keeping school board, administrators and parents informed on what the program is and why it is designed the way it is will help assure them that the school is a safe place,” he said.

In the end, that is a security director’s dual role, both making the campus safe and letting those who use the campus know about the measures being taken.

Recent incidents, including those not school specific such as the terrorist attacks of Sept. 11 and the recent attempted terrorist attacks in London and Glasgow, push a school security director to focus on a hands-on approach to security on multiple levels.

“We encourage (security directors) to be proactive,” Kaufer said. “No matter how well a security program is designed or implemented, there is still a concern that something might happen.”

**DO YOU THINK OPEN ENVIRONMENTS
LIKE COLLEGES AND UNIVERSITIES
CAN BE EFFECTIVELY PROTECTED?**

