A WHITE PAPER FROM

CENTER FOR
DIGITAL
EDUCATION

Best Practices for Campus Safety and Security

How K-12 and higher education institutions can address funding, planning and deployment of technology for emergency response.

SHUTTERSTOCK.COM

Best Practices for Campus Safety and Security

The Importance of Preparedness

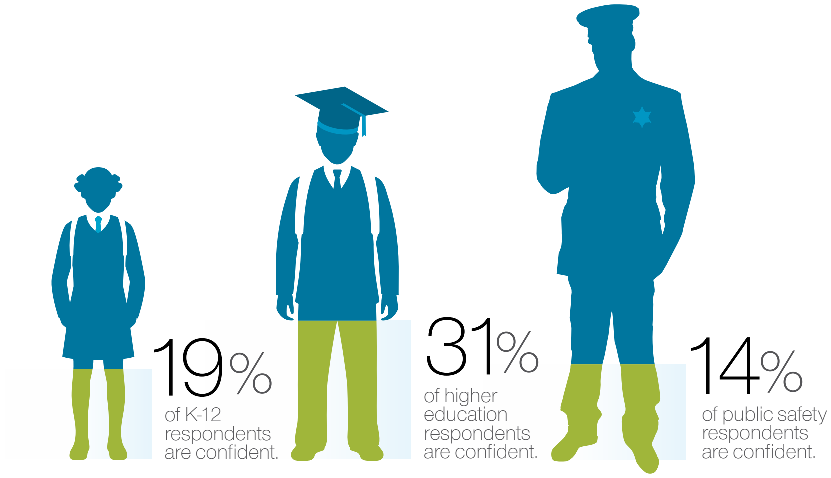
Second only to their mission of teaching and learning, K-20 education institutions must provide a place of safety for students, staff and visitors. To meet this responsibility, schools, districts and higher education institutions routinely work with local public safety officials to:

- Protect a school building or college campus through planning and training for physical security and emergency preparedness
- Keep current on key strategies, technologies and best practices for managing campus safety and security
- Comply with crime reporting mandates such as the federal Clery Act
- Address the challenges of identifying, planning for, funding and migrating to new monitoring and response technologies

K-12 and higher education officials and their public safety counterparts know that up-to-date technologies are vital for maintaining a high level of campus security and emergency response capability. But do educators and first responders have the same confidence in the security and emergency technologies currently deployed? Do they have the same perceptions and priorities for needed upgrades?

Sizing Up Security Planning

The following percentages reflect the confidence levels of survey respondents in the planning and technology used for security and emergency response at education institutions.



Source: CDE Campus Security Survey, K-12 Higher Education and Public Safety Respondents, 2014

These questions were the focus for separate surveys of educators and public safety professionals conducted in early 2014 by the Center for Digital Education and *Emergency Management*. The educators represented K-12 schools and districts, as well as four-year colleges and universities and two-year community colleges. The public safety respondents primarily worked for local police, fire and emergency management agencies.

The survey results indicate largely compatible views about the state of current technology deployments and response processes, as well as what needs improvement. Several questions in each survey were designed to elicit the perceptions of both parties about common concerns, as reflected in the key findings that follow.

Confidence in current security plans and technology. Only 19 percent of K-12 and 31 percent of higher education respondents were very confident in the planning and technology used for security and emergency response in their institutions. This confidence level was even lower for the public safety respondents; only 14 percent were very confident about the preparedness of education institutions within their jurisdiction. Low confidence levels may be a factor in plans to upgrade safety and security systems within the next five years, as indicated by just over 50 percent of education respondents.

Rankings of best security and emergency technologies. Both educators and public safety respondents listed video surveillance, access control and emergency notification (e.g., paging and intercom systems) as the top technologies. Educators gave higher priority to video surveillance and public safety officials gave higher priority to access control; both priorities can be addressed by converged video and access control systems.

Challenges for deploying new technologies. As expected, funding and administrative priorities were listed by both responding groups as top challenges to the deployment of new technology solutions. Additional challenges were ranked identically by educators and first responders: integration with existing systems, infrastructure shortcomings and lack of product knowledge.

Access to video surveillance. A notable 63 percent of the education institutions surveyed do not give municipal first responders access to campus/building video surveillance systems. Yet more than 84 percent of the public safety respondents indicate that access to live video feeds is important for better preparing an incident response.

Reflecting the trends and priorities identified in both surveys, this white paper discusses the latest technologies available to enhance safety and security on school campuses, and provides recommendations to consider when implementing these technologies and improving the practices used for emergency response in education.

Readiness in Schools Large and Small

A large public university and a small K-12 district illustrate how effective strategies and technologies support real-world protection and preparedness.

Texas A&M University

How do you protect a 5,200-acre campus that has the population of a small city and its own airport? This large scope is the challenge for security administrators at the main campus of Texas A&M University in College Station, Texas.

Video surveillance is a primary security technology, but budget limitations mean it can't be deployed everywhere on campus. Instead, "We prioritize video cameras in the areas that present a clear safety risk, such as parking garages," says Willis Marti, chief information security officer at Texas A&M University. "We also use real-time video monitoring for areas that have special safety and regulatory concerns, like the labs that contain biohazards, toxins or nuclear materials, and the health care offices that store medications."[1]

On-campus police and local law enforcement officers can access the live video stream from security cameras via a secure, authorized connection on the university's wireless network. Stored video files can be retrieved via the campus network or a copy can be sent to the appropriate law enforcement agencies.

5 Best Practices for Enhancing Safety and Security

Campus security officials interviewed by CDE identified five critical best practices for improving safety, security and emergency response.

1 Planning: Regularly test, review and update plans for security measures and emergency response processes. Tailor the plans to cover the incidents most likely to affect each location, including extreme weather, an intruder or violence, fires, industrial accidents and various natural disasters.

2 Transparent communication: Share safety and security plans as appropriate with students, parents, staff and the surrounding community, as well as with the relevant state and local response agencies. Clearly define processes for declaring a disaster, sending notifications and escalating the response effort.

3 Consistent approach: Consistency in policies, processes and technology systems greatly simplifies and increases the effectiveness of security and safety measures. To the extent possible, implement this consistency campus-wide for higher education or at the district level for K-12.

4 Regular reinforcement: Ensure an effective emergency response by conducting regular training and drills for students and staff, as well as simulations and exercises with local responders.

5 Technology, training and policy working together: Implement the right technologies in a way that supports policy implementation and compliance. For example, integration of the public address system with classroom telephones enables any instructor to declare a lockdown and become an incident commander, if such action is supported by district or institution policy and training.

Texas A&M has defined procedures for incident reporting, triage and activating the emergency operations center. Annual "tabletop" exercises and drills allow institution staff and local agencies to validate defined emergency response procedures and correct operation of emergency systems.

Owen J. Roberts School District

"It's only a drill," says a young student, after taking part in a practice procedure for locking down her school. Her calm reaction reflects the commonplace reality of stringent school security requirements, even for small districts in small towns.

The Owen J. Roberts School District in Pottstown, Pa., has many of the same security and emergency technologies as larger K-12 districts and higher education institutions. IP-based security cameras are installed inside and outside of all school buildings to allow video surveillance from the school office and the district's central security office. Electronic card readers on most school doors require an employee to swipe an access badge for entry. Visitor management systems in the school offices run security checks against a database and print badges with the visitor's photo, destination and entry time for monitoring.

Lawrence Mauger, the district's chief of security and safety, offers guidance to other K-12 districts for getting the most value from technology investments. "Buy for quality, not necessarily for quantity, especially for getting the high-quality video images that can be used for investigations and evidence," he says. He recommends high-megapixel video cameras, adequate disk storage for recorded video and adequate bandwidth on school networks to handle the high volume of video traffic.[2]

New Trends in Essential Technologies

The technologies discussed in this section are essential for deploying comprehensive security and emergency response capabilities in an education environment. These systems are mission critical and their design and implementation cannot be taken lightly.

Some of these technologies are deployed at the building level, while others can be implemented on a district-wide or campus-wide basis. All of them should be considered in light of security plans and policies, as well as physical measures implemented in a Crime Prevention through Environmental Design (CPTED) program and social programs, such as "see something, say something" campaigns. The ultimate goal is to find the right combination of technology, planning and policy that will create effective measures for deterrence, prevention, protection and response.

Visitor Access Control and Management

Tracking the location and access of all visitors is a security fundamental. An electronic access control system includes access cards, readers and control panels mounted at building entrances, as well as management software. For K-12 schools, access control systems can be used for routine building perimeter security and for protecting individual classrooms during a lockdown.

Computer-based visitor access systems can interface as appropriate with student information systems, employee directories, and law enforcement databases for driver's license and criminal background checks. This expanded information helps front-desk personnel comply with district or institution policy about granting each visitor access to a building or secure area. Texas A&M University uses the visitor control system to give emergency responders special access cards to allow for immediate building access during a disaster or incident.

Also important for higher education is easy management of the access badges given to employees and students. New access systems can provide the necessary single point of control while maintaining an appropriate level of open access to the campus. The security office can use the system to quickly authorize specific locations for each card, such as dorms and dining halls. Just as quickly, the card can be deactivated when a person's access should be blocked.

Video Surveillance

Live feeds and stored footage from video cameras located around a building or campus are vital for security response and investigations. Today's video surveillance technology is based on Internet Protocol (IP), which allows for connection to the campus network and access to video feeds via a Web portal on the Internet. Additionally, campus and community first responders can access individual video cameras and stored video recordings over the Wi-Fi computers in their vehicles for a more effective response to an incident as it happens.

The CDE survey indicates that less than half of education institutions currently have IP video systems, but 56 percent of respondents plan to upgrade their surveillance systems within five years. A video surveillance system includes cameras, software and displays for real-time monitoring and video management, and video-optimized servers and storage devices for video recording and transmission.

The high resolution and high quality of IP-based video surveillance typically reduces the number of cameras compared to older, analog CCTV systems, which reduces system costs. If limited budgets do not allow for installation of a video surveillance system with full campus coverage, schools or universities should identify the buildings and locations that will be likely targets for intruders or that have high safety risks, such as parking lots. Selective installation of security cameras can also address concerns on college campuses about unwarranted intrusiveness into personal privacy.

Building Protection Systems

Systems that broadcast alarms and support remote monitoring for fires, break-ins, flooding, loss of electricity and other conditions remain fundamental for building-level safety and security. This category includes shelter-in-place resources such as backup lines for power and communication, as well as generators.

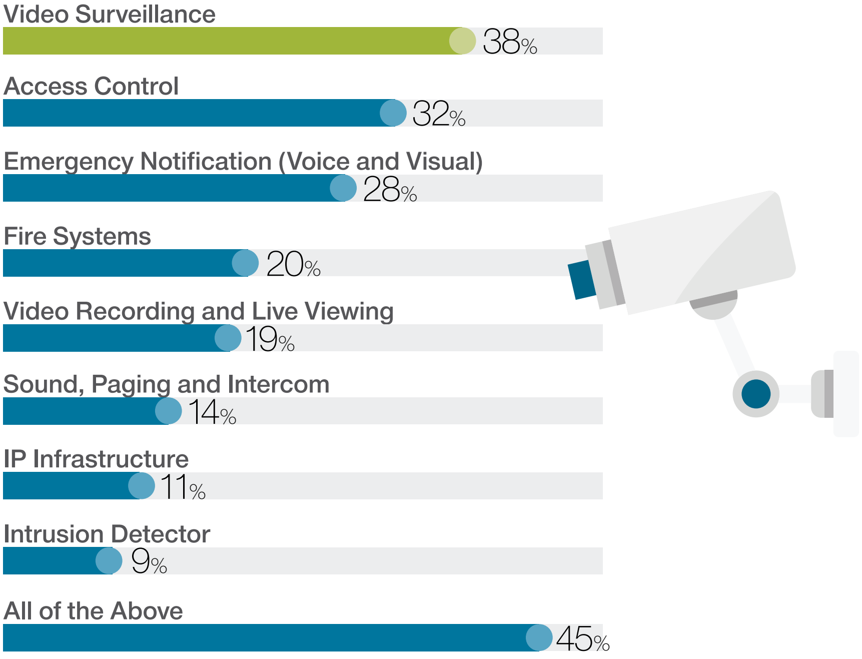
Intercom, Paging and Digital Signage Systems

School and campus personnel need technology systems that will enable immediate mass notification and outreach during a crisis. Intercom and paging systems help to communicate with students, staff and responders in classrooms, hallways, cafeterias and other gathering spaces. An intercom system allows audio-only or combined audio and video communication within a building and entrance control for doors.

A paging system uses microphones, alarm horns and speakers or integration with classroom phones for delivering audio announcements. Wall-mounted digital signage monitors can display emergency exit locations, instructions and status messages that are created by security or emergency staff and sent over the building network.

For external communications, email and text messages to mobile phones are particularly effective tools for delivering essential alerts and updates quickly and broadly to students, employees, parents, the media and other community resources.

Most Effective Campus Security Solutions



Source: CDE Campus Security Survey, K-12 Higher Education and Public Safety Respondents, 2014

Wireless Networks

In-building and campus wireless networks provide access to video streams, security system interfaces, floor plans and other information that support routine security monitoring, as well as disaster and emergency response. At Texas A&M, both campus police and officers from local law enforcement agencies can access the university's wireless network from laptops in patrol cars as well as tablets and smartphones, which allows for faster, safer and more targeted mobile response to a campus incident.

Improving Plans, Processes and Policies

Well-defined plans, processes and policies, covering both internal and coordinated actions, are essential to safety and security. In the CDE survey, education institutions reported using drills and simulations, structured walk-throughs of response plans, reviews with municipal first responders and testing of response checklists as regular activities to validate systems and processes.

Joint planning is another vital task. For example, law enforcement and first responder professionals who participated in the survey see major benefits in establishing joint communication plans between education institutions and local agencies. Texas A&M achieves this goal in part by participating in a community network that connects the university with local government agencies, hospitals and school districts in the neighboring towns of College Station and Bryan.

Recommendations for Strategic Technology Improvements

Given that only 19 percent of educators have a very high level of confidence in the technology used for their campus security, it's important to develop a strategic plan for improving those systems and their deployment. The results from the CDE surveys indicate two key recommendations for school districts and higher education institutions.

Develop and Strengthen Internal and External Partnerships

This recommendation reflects the importance of a cooperative effort among all parties involved in assuring the safety and security of any school environment.

- Train IT staff to effectively integrate and maximize the network, server and data storage infrastructure that's needed for the entire safety and security program.
- Work with first responders to validate how new technology solutions can address current gaps in security and emergency systems.
- Combine technology resources and expertise in the institution or district with those of state and local responder agencies.
- Partner with trusted advisors that understand the technology needed to build state-of-the-art security systems in campus environments.

Address the Largest Technology Challenges

This recommendation acknowledges the budget constraints and lack of perceived importance for new physical security technology.

- Locate grants, funding streams and other budget sources, such as ConnectEd, that are earmarked for new technology purchases, and utilize them for physical safety purchases.
- Connect administrative priorities with needed investments in safety and security.
- Ensure the campus network can maximize the integration and effectiveness of new technology solutions

Choose the technology that best fits the evolution of a security plan over time, not just a system that solves the most urgent need of the present moment. Consider the solution's scalability and integration with other systems, such as the student information system or human resources database for access control.

The Network and IT Infrastructure That Brings it All Together

Implemented individually, these systems are good, but when working together over an integrated infrastructure, they're even better. Integrated safety and security technologies offer several benefits:

- ✓ **Allows monitoring of all safety and security systems from a single interface, which permits fast response to, as well as reporting and investigation of, incidents within a building or campus.**
- ✓ **Simplifies budgeting, training and management for the complete solution.**
- ✓ **Leverages standards that support easier communication with local public safety systems.**

Underlying this integration is a robust IT network infrastructure, especially for handling the growing amount of streamed and stored video. For example, all cameras recording simultaneously can tax network bandwidth and Wi-Fi elements in a building. More recorded video that is stored for longer periods requires adequate server resources and storage capacity.

As part of planning for safety and security technologies, review the needed changes and expansion in the underlying network and IT infrastructure.

Strengthening Cellular Coverage on Campus

The cell phones carried by students, staff, campus visitors and first responders can be valuable communication devices during an emergency, but only if cellular coverage is adequate. In fact, some states are requiring the level of cellular coverage for first responders to meet standards such as the International Fire Code (ICC IFC) and the NFPA 72 standard from the National Fire Protection Association. Recognizing that most students and staff have a personal cell phone, many colleges and universities are reducing the number of landline phones, especially in dorms. Instead, these institutions are looking for ways to improve the capacity and signal strength for cellular service within buildings and across campus. One solution is provided by distributed antenna systems (DAS), which extend the signal from a local cell tower by using repeaters and antennas within a building. Implemented to improve cellular signals in weak spots or increase cellular capacity in high-usage areas, an indoor or outdoor DAS provides several advantages for emergency response:

- ✓ Anyone on the scene can use a cell phone to call 911 and responders can use cell phones to communicate with local dispatch, incident command, hospitals and other resources.
- ✓ It delivers the level of coverage on campus to support the location-based e911 service that allows quick identification and response to incidents.
- ✓ When texting for mass notification, coverage is adequate to deliver the message to students, faculty and staff in all areas of campus.
- ✓ During large events, security personnel and responders have the coverage needed for using their personal cell phones to communicate.

Also consider requirements for backup resources. “You can’t predict how bad a disaster will be, so it’s important to invest in redundant systems and equipment in advance. It’s not cheap, but when you need that redundancy, you really need it,” says Texas A&M’s Marti. “Redundancy is also important for the campus network and Internet access, since so many security and safety systems rely on this network connectivity.”

Finally, consider bringing in consultants for new technology planning and implementation. In the CDE survey, 51 percent of education administrators indicated their district or institution did the work of integrating technologies without external assistance. However, education-focused security system integrators bring experience and insights from other campus implementations. Involving the integrator in planning discussions can yield a broader understanding of potential solutions, help to maintain consistency and coherence across a campus or district, and uncover cost-effective strategies for evolving and scaling systems.

A Safer, Response-Ready Campus

Students, parents, staff and communities have a growing awareness of vulnerability to security risks in education environments. They will increasingly expect K-12 districts and higher education institutions to invest in the technologies, processes and cooperation with local first responders that will strengthen security and emergency response. Forward-looking campuses must accordingly educate themselves about which leading-edge security technologies are the right fit for their campus environments, while establishing stronger relationships with emergency response agencies, system integration providers and community stakeholders.

Endnotes

1. Center for Digital Education interview with Willis Marti, February 13, 2014
2. Center for Digital Education interview with Lawrence Mauger, March 31, 2014

CDE would like to thank Remo Patitucci, director of sales at Integrated Security & Communications, for providing his deep expertise in the field of campus security during the creation of this white paper.

Underwritten by Anixter and its business partners:

ANIXTER

ALLEGION · Arecont Vision – Leading the Way in Megapixel Video · AXIS COMMUNICATIONS · Berk-Tek – A NEXANS COMPANY · BOSCH – Invented for life · COMMSCOPE · exacq Technologies · GALLAGHER · NVT · PELCO by Schneider Electric · TALKAPHONE

Anixter is a leading distributor of the security, building technology and network cabling solutions you need to help create and maintain a safe and efficient educational environment. As active ONVIF, TIA and HetNet members, we understand how physical security and communications technologies and standards can help you meet the growing demand for a safer and more secure campus. We offer the latest in video surveillance, mass notification, access control, intrusion detection and in-building wireless technologies from our Technology Alliance Partners to assist you in effectively monitoring and communicating within the campus environment. Our security and communications technology experts (PSPs, BICSI RCDDs and ASIS CPPs) tailor educational solutions to your campus' specific needs and work with qualified installers, who, with the help of our innovative supply chain services can enhance the efficiency of your security deployment for minimum downtime. **For more information, please visit www.anixter.com/events/campus-security.**

CENTER FOR DIGITAL EDUCATION

The Center for Digital Education is a national research and advisory institute specializing in K-12 and higher education technology trends, policy and funding. The Center provides education and industry leaders with decision support and actionable insight to help effectively incorporate new technologies in the 21st century.

www.centerdigitaled.com