CREATING SA
MORE SECURI
CAMPUS ENVI

Seven Keys to Implementing Smart Strategies and Technologies

Dave Stolerow


FER,
E
IRONMENTS

In today's world, cultivating an environment of safety and security has become increasingly complex. Fortunately, the changing nature of security threats comes at a time when technological advancements are, with the right partner, able to keep up and deliver safer, more secure campus environments. Schools, colleges, and universities face a unique set of challenges as they work to maintain an open, welcoming environment while minimizing exposure to risk and danger. It's both a delicate balance and a community effort. That is, students, faculty, and staff feel freer to focus on the core mission of education when they all feel safe, secure, and comfortable.

In this article, we present seven smart strategies and technologies for securing our schools and campuses. This topic is a continued exploration of one we at Siemens have been working on for many years, and warrants a renewed perspective.

What's at stake

School and campus security has become a fundamental expectation for students, faculty, staff, and the broader community, as well as parents of potential students. And yet, recent incidents illustrate just how vulnerable institutions – and the people who attend them – remain.

At the University of Nevada Las Vegas (UNLV), a gunman killed three faculty members and injured three other people, including two law enforcement officers. One student who recounted the incident said it was not her first active shooter experience[i]. Students at the University of Houston protested in February 2025 to demand greater campus security and safety[ii] after "a string of robberies and a sexual assault were reported on campus."

The ability to respond effectively to any safety incident begins long before an incident occurs, and these tragedies highlight the devastating consequences of security gaps. They also reinforce the importance of preparation, prevention, and aligning security strategies and technologies with industry recommendations and evolving trends.

Aligning campus security strategies with industry trends

In its 2025 Security *Megatrends* report[iii], the Security Industry Association (SIA) identifies several key trends that are shaping the future of security. Artificial intelligence (AI) is an already driving force behind many of today's most effective security solutions. The combination of visual intelligence, predictive analytics, and autonomous threat detection will have a significant impact, they say, on the effectiveness of video surveillance and emergency response. It's a shift that's enabling campuses to shift their security strategies from passive monitoring to proactive threat detection.

SIA also highlights how the continued convergence of information technology (IT) and operational technology (OT) systems means that security technologies can now be integrated with campus infrastructure in ways that enable real-time, data-driven decision making. For example, with IT-OT convergence, access control, video surveillance, and emergency communication systems can work together with campus automation, lighting, fire safety, and HVAC systems to create a truly unified response to campus emergencies.

Finally, the *Megatrends* report points to cloud-based management of security technologies as a key trend. Cloud-enabled platforms enable campuses to take advantage of real-time software updates and security patches, proactive monitoring, and seamless integration across a variety of security and building functions – all of which help campus technologies remain current, effective, and scalable

Effective emergency responses start with effective emergency plans + practice

The best, most effective emergency responses start with effective emergency plans and processes. What should happen in the event of a fire alarm, a problem with a campus lab space, an active shooter situation? All these contingencies must be carefully considered and planned for, because the expectation is that administrators will know exactly what to do and how to respond in each of these situations. The time to understand and learn these processes is not during an emergency.

Securing our educational institutions means more than having an emergency plan; it's about practice, too. Consider how athletes prepare for a game. They practice game situations, run drills, and study their opponents. Emergency preparedness must follow the same approach. By running drills and understanding emerging threats, everyone can react appropriately to have the best possible outcome in the event of an emergency.

Educational institutions cannot afford to take a reactive approach to security. To help ensure a reasonable level of security for students, faculty, and staff, schools and campuses must strategically layer security into their daily operations while recognizing that both security threats and the technologies to prevent them continually evolve and improve.

Many schools and campuses have been architecturally designed to create open, welcoming spaces, although access control platforms have been important for securing interior building spaces.

Today's approach for implementing smart strategies and technologies

In 2014, the Partner Alliance for Safer Schools (PASS) published its first "guidelines for implementing a layered and tiered approach to securing and enhancing the safety of school environment." Their original report, now in its sixth edition[iv], still recommends a multi-layered approach that integrates security into daily operations. Today, building a more secure, more resilient educational environment means leveraging both strategic planning and advanced technologies to mitigate risks before they escalate into crises and help speed response of first responders should an event occur.

The following seven keys outline actionable strategies, along with enabling technologies and services, that schools and campuses should adopt to establish a more comprehensive security framework and most importantly, help create safer, more secure learning environments.

1. Assess the current state of security and plan for a unified approach.
2. Evaluate perimeter security and close gaps as needed.
3. Control access into and out of buildings and in secure areas.
4. Implement an intelligent video surveillance platform.
5. Unify security technologies through integration to help improve efficiency and response times.
6. Employ an effective notification and communication platform for all stakeholders and visitors.
7. Service and maintain security systems to enable proper operation and reliability; leverage digital services to create efficiencies and fill staffing gaps.

1. Assess the current state of security and plan for a unified approach

Over the last decade, schools, colleges, and universities have done a tremendous amount of work to shore up their security measures, protocols, and technologies – and this work has paid off. In January 2025, there were 50% fewer school shootings than there were in January of 2024, progress that can be attributed to the combination of emergency response planning and security technologies[v].

The first "wave" of securing both school and campuses involved securing the perimeter, restricting entry points, and deploying cameras to record activity. Now, security professionals must modernize their approach, including leveraging new technologies, as campus environments continue to change and adapt.

Re-assessing the current state of security means taking a fresh look at vulnerabilities and acknowledging that yesterday's solutions may no longer be sufficient for today's risks. Re-assessment may mean looking at smarter, more adaptive, and AI-powered platforms; refining emergency response protocols; shoring up cybersecurity training; and aligning security solutions with the latest threat intelligence.

School and campus security has become a fundamental expectation for students, faculty, staff, and the broader community.

Likewise, planning for a unified approach helps ensure that campus security becomes more than a fixed set of tools; it can become an evolving strategy that prioritizes risk aversion, situational awareness, effective emergency response, and community well-being.

2. Evaluate perimeter security and close gaps as needed

You have likely already invested in a range of perimeter security measures, from natural barriers; building fortifications like fencing, window film, and vestibules; and security technologies like lighting, sensors, exterior cameras. Over time, building usage may have shifted, or green spaces have evolved.

For college campuses, it may also be time to evaluate code blue stations for effective functionality. Are these stations working correctly? Is camera resolution acceptable? What about lighting – is that adequate or introducing risk? Consider, too, that today's AI-powered technology can detect screams and calls for help, automatically activating alarms within the command center.

Now is the time to re-evaluate the effectiveness of these measures and close any gaps that may remain.

3. Control access into and out of buildings and in secure areas.

Many schools and campuses have been architecturally designed to create open, welcoming spaces, although access control platforms have been important for securing interior building spaces. Security teams are now looking to close these gaps, adding access controls to building entrances as well as interior spaces that were not previously equipped with security.

Today's access control systems have evolved significantly since their first implementations. Now they can manage access to multiple buildings and environments that all come with their own set of security requirements—such as the differences between research areas versus dormitories or academic buildings.

4. Implement an intelligent video surveillance platform

Effective, modern security demands adaptive visual intelligence platforms that can provide your security team the insights they need to actively interpret and respond to potential threats in real time.

The first step is to evaluate your current video coverage and scope. Are cameras placed in the right locations? Have you done all you can to minimize blind spots? It's also essential that you evaluate your cameras themselves, as newer devices have much greater resolution, giving security teams much more detailed images than ever before—even so far as allowing one new camera to do the work of several older ones. Could it be time to replace aging cameras with new ones that can provide better evidence?

Historically, cost and complexity meant that

many camera features weren't configured at their deployment. But today, self-configuring, self-alarming systems make it much more accessible for campuses to activate AI-powered analytics. Are you fully utilizing and leveraging the analytics capabilities your system offers?

Additionally, real-time forensic search capabilities can now identify people, clothing, animals, and unusual movements; detect distress signals, such as calls for help or screams; and empower response teams to react swiftly, even in areas without direct camera visibility. These AI-powered features can provide security teams with the situational awareness they need to detect, analyze, and respond to threats much faster and more accurately than before.

5. Unify security technologies to help improve efficiency and response times

Traditionally, security setups have involved disparate software solutions for access control and video surveillance. This structure created operational silos that could slow down decision-making. Today, however, security platforms can be truly integrated and unified in an ecosystem that breaks down these silos, seamlessly sharing data across platforms and managed from a single interface.

With a unified approach to security, for example, a person swiping a badge at an entry point can be instantly cross verified with their photo ID through the security platform, rather than requiring an extra, manual step. Unification can also extend beyond security to encompass other building systems, such as fire and automation. In this way, the IT-OT convergence empowers campus facilities teams to receive and act on alarms in real time and with a unified approach. Let's say a fire alarm is activated; access controls in that area can be triggered automatically to assist in evacuation, HVAC systems can respond as needed, and video surveillance can be enabled to support first responders – all without a manual intervention at a time when every second matters.

Ultimately, campuses that plan for and invest in unification today will be better equipped to adapt to future innovations and more deeply embed security into all aspects of campus facilities.

6. Employ an effective notification and communication platform for all stakeholders and visitors

In any emergency – whether we're talking about a weather event, an environmental hazard, or a hostile threat – every second counts. Educational leaders must help ensure that communications are immediate, accurate, and delivered automatically through the channels that first responders, students, faculty, staff, and the community already use and trust.

However, many schools and campuses still rely on outdated, manual notification protocols that delay information to those who need it most. As a personal anecdote, as I was working on this article, my local campus's hard lockdown alarm was activated, as it turns out, inadvertently. At 11:21am, I received an email outlining the false alarm, the administration's response, and the fact that campus operations had returned to normal. Two minutes later, at 11:23am, I received a text message notification about the lockdown. Two minutes after that, the all-clear came through. These messages arrived out of sequence, and underscore the need for unified, automated communications.

The National Fire Protection Association (NFPA) has incorporated emergency communications into its NFPA 3000™ Standard for an Active Shooter / Hostile Event Response (ASHER) Program[vi]. Nearly every campus has a notification system that can communicate via text message, app-based alerts, email, and so on. Technology today is available that empowers campuses to leverage their existing communication infrastructure and create a seamless, unified communication platform that integrates with access control, surveillance, and environmental monitoring so that the right message gets to the right people at the right time—without relying on manual activation.

When notification and communication combine with access control and visual intelligence platforms, the entire security approach can become an autonomous, integrated function; schools and campuses can ensure that critical alerts don't just go out, but include timely, precise, and accurate information people can use to act and respond appropriately.

Dave Stolerow is the National Business Manager - Enterprise & Smart Buildings/Security at Siemens Industry, Inc.

[i] USA Today
[ii] Houston Public Media
[iii] Security Industry Association
[iv] Partner Alliance for Safer Schools
[v] Campus Safety Magazine
[vi] Campus Safety Magazine