HOSPITAL / SCHOOL / UNIVERSITY
Campus Safety

Campus Security Technology Trends to Watch in 2024

SIPPAPAS/STOCK.ADOBE.COM

Campus Security Technology Trends to Watch in 2024

Is your organization leading the pack in security technology upgrades, in lockstep with your peers, or lagging behind? Read on to find out. ***By Robin Hattersley***

The overall demand for security technology is forecast to be strong in 2024, according to the latest research from the Security Industry Association (SIA), and studies conducted by *Campus Safety* in the past year confirm SIA's outlook for college campuses, K-12 schools and districts, and healthcare facilities.

As we begin another year, there is no better time to review the technology trends we've been experiencing recently to see which ones will continue, as well as new advances your organization might want to consider. Here's what school, university, and hospital protection professionals can expect to see technology-wise in the upcoming year.

Is your organization leading the pack, in lockstep with your peers, or lagging behind? The following trends on access control, video surveillance, emergency notification, panic alarms, and more will show you where you stand.


THOMAS/STOCK.ADOBE.COM

ACCESS CONTROL

The demand by K-12 school districts, institutions of higher education, and hospitals for access security, locks and door hardware upgrades will continue to be very strong in 2024. The increased demand applies to a wide range of access control technologies, from traditional locks to newer systems.

According to the **2023 Campus Safety Access Control and Lockdown Survey**, locks and/or door hardware are the most popular planned purchases or upgrades, with 43% of all survey takers saying they made upgrades to their systems in the past two years and are considering doing so by 2025. Another 13% haven't recently made upgrades to their locks and door hardware but are considering doing so in the next two years. Overall interest in future purchases/upgrades of this technology increased from 45% in 2021 to 56% today.

Survey takers indicated many of them are considering visitor management upgrades, with 55% of them thinking about making improvements soon. Additionally, Near Field Communications (NFC) and Bluetooth Low Energy (BLE) mobile phone access control have grown in popularity compared to 2021. Now, 55% of all survey respondents have either recently purchased this type of solution and are considering adding more in the next two years or haven't recently made a purchase but are considering doing so by 2025. That's ten percentage points more than in 2021. More respondents also say they are considering acquiring window safety and/or security solutions in the next two years… 53% now compared to 44% two years ago.

Other types of solutions are also getting a lot of attention, with the following technologies being considered by campuses for upgrades in the next two years: Intercoms (52%); cloud-based access control (51%); card and/or biometric access control (46%); secure front entrance vestibules (46%); and fences (43%).

Tragedies Receiving National Attention Often Serve as Motivations for Improvements

When asked why they upgraded or plan to upgrade their access control and lockdown

technologies, policies, and procedures, more than half (53%) of all respondents said, "Recent incident(s) that happened in other parts of the country." When the answers were segmented out by organization type, 66% of K-12, 73% of healthcare, and 41% of college and university respondents said incidents that happened in other parts of the country were motivating factors.

The differences in responses by sector are understandable. The May **2022 Robb Elementary School mass shooting** in Uvalde, Texas, as well as the March 2023 active shooter attack at **Covenant School** in Nashville, Tenn., were widely covered by the media and garnered national attenton.

Additionally, the dramatic rise in active shooter incidents in the U.S. as a whole has certainly prompted many campuses to bolster security. Two active shooter tragedies that happened on college campuses in 2023 – on February 13 at **Michigan State University** (MSU) and on December 6 at the **University of Nevada, Las Vegas** (UNLV) – were reminders that institutions of higher education are not immune to active shooters.

66% of K-12, 73% of healthcare, and 41% of college and university respondents said incidents that happened in other parts of the country were motivating factors in upgrading campus access control.

In response to the shooting that happened at MSU, the school now requires students and faculty who want to access on-campus buildings after hours to use their MSU ID cards. Key fob access control has also been installed. Other technologies have also been installed or upgraded.

UNLV has just begun to identify and then plan its security upgrades. Officials there are looking to bolster security with more access control and video surveillance. Additionally, nearly 14,000 people signed an online petition calling for a closed campus that would only allow authorized students and faculty access. Which upgrades will actually be implemented, however, has yet to be determined.

Much like how K-12 schools and districts reacted to the Uvalde and Nashville mass shootings, both MSU's and UNLV's tragedies may prompt other U.S. colleges and universities to review their security profiles and upgrade their technologies in 2024. If so, this would reverse the **2022 trend** of institutions of higher education lagging behind K-12 schools in their monthly and quarterly site security assessments.

Meanwhile, the massive number of workplace violence incidents that have occurred at U.S. hospitals for years and intensified during the COVID-19 pandemic may also be motivating healthcare providers to make access control and lockdown improvements. Another development that may be prompting healthcare to pay closer attention to security is the 2022 Department of Health and Human Services Centers for Medicare and Medicaid Services' (CMS) warning that hospitals must protect their employees and patients from violence.

Recent incident(s) that happened "on my campus" or "near my campus" were motivations for access control upgrades for 46% and 46% of hospitals, respectively; 42% and 46% for schools, respectively; but only 23% and 28%, respectively, for institutions of higher education. Four in ten respondents overall said nothing in particular prompted them to make upgrades. They just wanted to improve safety and security.

Only 5% of 2023 survey takers said, "We need to upgrade our access control and lockdown technology, policies, and procedures, but we are not taking steps to do so."

Ability to Lockdown, Track Visitors Varies by Campus Type

K-12 schools continue to lead the way in their ability to lockdown their campuses: 39% can lockdown 100% of their campuses and 44% can lockdown 75-99% of their campuses. The combined total percentage of 83% is 4% more than in 2021 when it was 79%. Only 43% of healthcare respondents and 35% of participants from institutions of higher education said they can lockdown 75% or more of their campuses.

Overall, 71% of all respondents said they can lockdown 50% or more of their campuses, but that's 15% below 2021's findings (86%) and 8% less than 2019's findings (79%).

When asked about visitor management, colleges and universities are the least confident in their abilities to account for everyone in their buildings, with 23% of respondents saying they are "Not confident at all," compared to only 8% of schools and hospitals. Additionally, 10% more survey takers overall said "Lack of a visitor management system, or the system we have needs to be upgraded," is extremely or very challenging for them. That's up from 27% in 2021 to 42% in 2023.

On the other end of the accountability spectrum, more than eight in ten K-12 respondents are really confident (49%) or moderately confident (35%) that they can account for everyone in their buildings.

Concerns with Window Security, Keys, and Campus Layout Increasing

The Covenant School mass shooting appears to have prompted more respondents to be concerned about their windows and other glass openings, as has Texas' new requirement that schools must install window security film. The survey takers who said the design and/or placement of their windows is very challenging or extremely challenging increased 23% from 29% in 2021 to 52% in 2023.

Concerns with the tracking of keys also jumped by double digits, with 50% of respondents in 2023 saying this is an extremely or very challenging issue for them, compared to 33% only two years prior.

More than half of all respondents (52%) said "Our campus layout is open, so it's very difficult to lockdown our campus or control access," is an extremely or very challenging issue for them, up from 39% in 2021.

Lack of Weapons Detection, IT Support, Labor Shortage Posing Problems

Even "Lack of metal detection or our detectors need to be upgraded" and "Our students, faculty and/or staff are required to carry too many credentials (cards) or keys," each saw an increase of 8% of respondents (38% and 31%, respectively) who said these problems are now extremely challenging or very challenging.

71% of all respondents said they can lockdown 50% or more of their campuses.

Additionally, 14% more respondents said the lack of IT department support/buy-in and cooperation is an extremely challenging or very challenging issue — up from 24% in 2021 to 38% now. At 49% and 41% respectively, healthcare and K-12 respondents are struggling with this issue the most. This trend is particularly troubling because most access control, visitor management, intercoms and other related technologies run on the network.

The current labor shortage appears to be affecting the staffing and training required to manage campus access control systems. Ten percent more respondents in 2023 said that "Staff don't know how to effectively manage our access control system(s)" is an issue that's extremely challenging or very challenging for them (39% in 2023, compared to 29% in 2021). Eleven percent more now indicate a lack of staffing is an extremely challenging or very challenging issue for them -- up from 28% two years ago to 39% today.

The 2023 survey also found that 9% more campuses are struggling to develop or maintain appropriate policies to support their access control systems.

Integration, Maintenance, Software Update Issues Continue

Additionally, the need for card access control and biometrics has become quite apparent to campus protection professionals. Now, 41% of all respondents say not having card access control or biometrics is extremely challenging or very challenging for them. That's 18 percentage points more than in 2021.

Concerns regarding "Our access system(s) isn't integrated with other public safety systems (e.g. video surveillance, intrusion, fire, etc.)" also increased in 2023. Now, 39% of all participants say this issue is extremely or very challenging, which is 13% more than two years ago.

More than one in three (35%) of all survey participants said maintenance of card access systems is extremely challenging or very challenging, which is 13% more than when we asked about this topic in 2021.

Access control software bugs and updates are also becoming more problematic, with 35% of all 2023 survey participants saying this issue is extremely challenging or very challenging for them. That's 12% more than in 2021. At 45% and 43% respectively, healthcare and K-12 respondents are having a much harder time than their peers in higher education, where 23% said this issue is extremely or very challenging for their institutions.

"Older access system(s) can't integrate/interoperate with new access control systems" is an extremely or very challenging issue for 34% of all participants, which is 9% more than in 2021.

VIDEO SURVEILLANCE

With 94% of the organizations that responded to the **2023 Campus Safety Video Surveillance Survey** having one or more video surveillance system on their campus, cameras appear to have earned the respect of practically all security professionals. Even the 6% who said they don't have a security camera system yet are considering making the leap in the next two years.

Artificial intelligence (AI) has been receiving a lot of attention from the general public lately, and that attention is reflected in 2023's survey responses. Seven percent more participants than in **2021** said they've purchased "artificial intelligence related to video

surveillance" over the past two years… 28% vs. 21%, respectively. Additionally, 7% more now are considering acquiring these solutions in the next two years (32% today vs. 25% in 2021).

The cloud is also gaining in popularity. More than one in three of 2023's survey takers (36%) said they've bought "cloud video surveillance solutions" in the past two years, which is 8% more than in 2021. As for the future of the cloud, demand for it remains the same as in 2021: 29% of 2023 survey participants are considering acquiring this solution in the next two years.

Another solution getting more attention is license plate recognition (LPR), with 34% of 2023 respondents saying they've purchased this equipment recently. That's 5% more than two years ago. Additionally, more than one in three of 2023 survey takers (37%) are considering purchasing LPR in the next two years. That's 6% more than in 2021.

New to the 2023 questionnaire was weapons/gun detection. More than one in five participants (23%) have purchased this solution over the past two years, and 36% are considering doing so by 2025. Considering the recent rise in active shooter events in the U.S., this trend is not surprising.

Traditional Video Surveillance Equipment Still Popular

Campus investments in the more traditional type of security camera equipment continue to grow as well.

Historically, fixed security cameras have been the most popular video surveillance equipment purchased by campuses, and that trend continues. Eighty-four percent of 2023's participants have bought cameras in the past two years. That's 5% more than in 2021, when 79% indicated they recently made a purchase of this type of equipment. More than half of 2023's respondents (57%) also said they are considering buying more fixed cameras in the next two years, which is practically the same as in 2021 (55%).

Video management software (VMS) was the second most popular video surveillance solution purchased by respondents over the past two years, with 53% saying they've recently bought VMS. More than one in four respondents (27%) said they are considering buying more VMS solutions in the next two years.

Network video recorders (NVRs) also continue to be popular, with 48% of respondents saying they have recently purchased this type of technology. In 2021, that percentage was 47. More than one in four 2023 respondents (27%) said they are considering buying more NVRs by 2025.

Even digital video recorders (DVRs), which are an older video surveillance technology, are still being purchased. More than one in three 2023 respondents (36%) bought this type of equipment in the past two years. That said, demand for DVRs appears to be decreasing. Only 19% of 2023 survey takers are considering purchasing more in the next two years. That's 7% less than in 2021.

Systems integration is now the biggest thorn in the side when it comes to video surveillance technology. One in four respondents said the issue of "Our video system(s) isn't integrated with other public safety systems, such as access control, intrusion and fire" is either "extremely challenging" or "very challenging" for them. Keep in mind, however, that 25% is much better than the 34% of 2019 survey takers who said integration was extremely or very challenging.

EMERGENCY NOTIFICATION

Emergency notification technologies continue to be popular purchases in education and healthcare, and for good reason. These systems quickly convey information during emergencies that saves lives. It's not surprising then that 71% of respondents

KITINUT/STOCK.ADOBE.COM

to the **2023 Campus Safety Emergency Notification Survey** either plan on deploying new or upgraded mass notification solutions in the next two years (35%) or are not sure but are considering doing so (36%). That 71% is a 20-point increase compared to 2017.

Text messaging alerts usage overall has increased significantly over the past several years. In the **2019 Campus Safety Emergency Notification Survey**, 71% of respondents said they use text message alerts, compared to today where 87% use this technology to disseminate emergency notifications.

Intercoms are also much more popular now, with 63% of all respondents saying they currently use this type of system for mass notification. In 2019, that percentage was 53.

Interestingly, most of the other technologies used for mass notification by schools, school districts, hospitals, colleges, universities, and trade schools have remained remarkably constant over the past several years. For example, 38% of 2023 respondents use external loudspeakers, which is only a three-point increase compared to four years ago. Call boxes are used by 23% of respondents today compared to 24% in 2019.

In 2019, emails were the most commonly used mass notification system (76%), and at 71%, SMS texting was the second most popular. Now texting leads the way at 87% with emails being a close second at 86%.

More than half (54%) of colleges, universities, and trade schools use social networking sites to send out emergency alerts compared to only about 30% of K-12 and hospital respondents. By contrast, K-12 and healthcare survey participants (32% and 39% respectively) are much more likely to use phone trees/telephony, compared to higher ed respondents (20%).

About one in three colleges, universities, and trade schools say they use digital displays/signage or scrolling message boards and pop-up alerts via computer/projectors.

4 Out of 5 K-12s Plan on or are Considering Emergency Notification Upgrades

K-12 schools and school districts appear to be leading the pack with 42% saying they plan on upgrading their emergency notification systems and another 42% saying they are thinking about it.

Overall, at 30%, mobile apps are the most popular mass notification solution that campuses plan on upgrading or purchasing in the next two years. Text message alert systems are close behind, with 25% of all survey takers saying they plan on upgrading or purchasing these solutions in the next 24 months.

At 27%, K-12 campuses are also taking the lead in planning to upgrade or purchase intercoms/overhead paging systems, compared to only 13% of institutions of higher education and 4% of healthcare facilities. However, healthcare respondents lead the pack in their plans to acquire or upgrade digital signage: 22%, compared to 17% for higher ed and 14% of K-12.

A significant portion of survey takers still appear to be trying to decide what they will get. More than one in five respondents (21%) don't know which emergency notification systems they will be upgrading in the next two years.

When asked about the challenges experienced with their emergency notification systems, respondents said "database management and updates" is the biggest issue overall, but especially for hospitals (65%) and K-12 campuses (46%). Although "staff enrollment in text message systems" was the second most mentioned issue by all respondents, a whopping 61% of healthcare respondents say staff enrollment in text alert systems is a problem for them.

At 23%, schools and school districts have a lot more problems with the volume and intelligibility of their siren/loudspeaker systems than colleges, universities, and trade schools (10%).

GIORDANO TRABUCCHI/WIRESTOCK/STOCK.ADOBE.COM

PANIC ALARMS AND MOBILE DURESS SYSTEMS/APPS

The high rate of workplace violence at hospitals, as well as the 2018 Parkland high school mass shooting that prompted the passage of Alyssa's Law in several states, are just some of the reasons K-12 schools, districts, colleges, universities, and healthcare facilities have adopted some type of panic alarm or mobile duress system or app. These technologies are effective ways for campus personnel to summon for help when there is an emergency.

Fixed panic buttons/alarm systems are the panic alarm technologies most often deployed in schools, colleges, universities, and healthcare facilities, according to the **2023 Campus Safety Panic Alarm and Mobile Duress System or App Survey**. Two out of three of participants in the study (66%) have this type of system, and 22% said they are considering adding more or buying this technology as new by 2025.

Mobile phone apps used for panic alarms and emergency communications are the second most popular technology used by survey participants: 58% already have this technology, and 22% said they are considering adding more or getting this technology in the next two years.

Motivations for Panic Alarm Purchases Vary

When survey participants were asked what motivated them to purchase a panic alarm/mobile duress system or app, at 35%, the most popular answer was, "Nothing in

particular. We just want to improve safety and security on campus." However, the most cited reasons varied significantly by campus type.

Only institutions of higher education actually cited this reason as their primary purchasing motivation (44%). For healthcare facilities, the most cited reason was, "Recent incident(s) that occurred on my campus or institution." At 36%, "Recent incident(s) that happened in other parts of the country" was the most popular reason cited by K-12 respondents, probably because of Uvalde. That percentage was 33 in healthcare but only 16 for higher education.

"Local, state, or federal laws or mandates" were cited as reasons by 23% of K-12 participants, probably due to the passage of Alyssa's Law in their states.

Although schools and colleges activate their panic alarms most often for medical emergencies, these types of incidents are only the sixth most common reason for activations at hospitals. In healthcare, patients acting out and visitors acting out are the situations when panic alarms/mobile duress systems/apps are activated most often.

VAPE AND E-CIGARETTE DETECTION

E-cigarette use and vaping continues to plague K-12 campuses, resulting in many student hospitalizations and overdoses on nicotine, THC oil, crystal methamphetamines, opioids, and other drugs. Additionally, vaping in teens has been linked to lowered academic performance, decreased student engagement, and increased depression, according to a **study** by Verkada. The study also found that 20% more teens vaped in the 2022-2023 academic year compared to the prior year. In total, 14% of all high schoolers vape, according to the **CDC**.


PIXARNO/STOCK.ADOBE.COM

The widespread use of e-cigarettes at K-12 campuses is overwhelming schools and the SROs deployed to protect them.

Although human efforts that increase the supervision of students and develop awareness of the dangers of e-cigarette use can help address the problem, according to **Safe Havens International**, K-12 campuses also need to embrace integrated technologies. Specifically, Safe Havens recommends schools adopt electronic hall pass systems,

NINA L/PEOPLEIMAGES.COM/STOCK.ADOBE.COM

cameras with analytic software, proximity card access control systems, and vape sensors that are integrated and supported by policies and practices.

One example of the successful implementation of video, audio, and sensor technology to address e-cigarette use on campus was Green Dot California Schools. You can read about their successful deployment of these technologies **here**.

Although studies of e-cigarette use have primarily involved students in K-12 schools, those individuals will eventually graduate, with many of them going on to college. Institutions of higher education should have prepared for when these students arrive on their campuses, along with the health issues that accompany vaping.

CYBERSECURITY

Once again, the biggest elephant in the campus security space in 2024 will be cybersecurity.

Despite considerable investments in security technology, data breaches continue affecting organizations across the globe and causing them more financial damage than ever, according to **data** presented by AltIndex.com. The average data breach cost has jumped by nearly $600,000 in the past three years and hit an all-time high of $4.45 million in 2023.

According to the Ponemon Institute's *2023 Cost of Data Breach Report*, the average data breach cost has risen by 15% in the past three years. In 2020, it amounted to $3.86 million per incident. But a year later, it jumped to $4.24 million. The negative trend has continued ever since, with the average cost of data breaches reaching an all-time high of $4.45 million in 2023. However, not all countries, regions, and markets saw the same cost growth.

The average cost of a data breach in healthcare has grown by more than 50%, from $7.13 million in 2020 to $10.53 million in 2023.

The Middle East has witnessed the biggest data breach cost increase of all surveyed regions, hitting more than $8 million this year. The U.S., which has had the highest average data breach cost of all countries for the past 13 years, has seen the second-largest increase. U.S. data breaches cost an average of $8.64 million in 2023 or $840,000 more than three years ago.

Healthcare continues to experience the highest data breach costs of all industries and has seen the biggest cost growth. Over the past three years, the average cost of a data breach in healthcare has grown by $3 million or more than 50%, rising from $7.13 million in 2020 to $10.53 million in 2023. For the K-12 and higher education market, the average cost of data breaches fell slightly from $3.9 billion in 2020 to $3.65 billion this year.

The behavior of the hackers who carry out these data breaches is truly diabolical.

In November, hospital emergency rooms in several states were forced to divert emergency vehicles to other facilities due to a slew of cybersecurity incidents on Thanksgiving Day. In March, a Russian-based ransomware group published naked photos of patients undergoing cancer treatment after Lehigh Valley Health Network refused to pay a ransom. Earlier that month, another ransomware gang escalated its tactics by releasing data stolen from Minneapolis Public Schools in February after it refused to pay a $1 million ransom. The group leaked photos that included screenshots of handwritten notes describing a sexual assault allegation and the names of three students allegedly involved in the incident.

In light of the continued and growing cyber threat to hospitals, schools, and institutions of higher education, campuses must continue to bolster their cybersecurity measures in 2024 and beyond.

HOSPITAL / SCHOOL / UNIVERSITY
Campus Safety

www.campussafetymagazine.com