CAMPUS SAFETY REPORT:

Campus Security Technology Trends to Watch in 2023

HOSPITAL / SCHOOL / UNIVERSITY
Campus Safety

Campus Security Technology Trends to Watch in 2023

Access control, visitor management, security site assessments, mass notification, video surveillance, vaping/e-cigarette detection and mitigation, and cybersecurity are hot technologies that should be on everyone's radar this year.

By Robin Hattersley

As we start another year, it's time to once again review the campus security technology trends we've seen in 2022, which ones will continue to challenge us, and the emerging technologies that should be considered by security, public safety, and emergency management professionals in schools, institutions of higher education, and healthcare.

Topics covered include access control, visitor management, security site assessments, emergency/mass notification, video surveillance, vaping/e-cigarette detection and mitigation, and cybersecurity. Read on to see what's in store.

Access Control and Campus Security Site Assessments

There was an increased focus on access control, visitor management, and security overall by K-12 schools and school districts in 2022, most likely prompted by Uvalde, Texas' May 24 mass shooting at **Robb Elementary School**.

In Texas, officials began conducting intruder safety audits of K-12 campuses around the state. Each audit takes an in-depth look at school safety, with inspectors checking exterior entry points, as well as how schools manage visitors.

In the U.S. as a whole, 80% of the K-12 respondents to our **2022 Campus Safety Access Control and Lockdown Survey** said they've conducted security site assessments within the year, with 33% saying the last time their campus conducted a security site assessment was within the month.

I suspect the increased focus on access control, visitor management, and K-12 school security overall will continue in 2023 and beyond.

Unfortunately, institutions of higher education appear to not be paying as close attention to campus physical security as their peers in K-12 and healthcare, according to the 2022 Campus Safety Access Control and Lockdown Survey. Only 25% of colleges and universities have conducted monthly or quarterly site security assessments. Twenty-seven percent said they don't know how often their campuses conduct security assessments, and another 11% said their facilities never conduct these types of reviews.

Institutions of higher education appear to not be paying as close attention to campus physical security as their peers in K-12 and healthcare.

Additionally, only 31% of higher ed respondents said 91-100% of their classroom doors can be locked from the inside (57% of K-12 schools can do so).

Another troubling trend uncovered in the survey was that 15% of respondents have purchased door-blocking/barricade devices. When broken down by sector, those percentages are:

- K-12: 18%
- Hospital: 17%
- Higher Ed: 10%

Door-blocking/barricade devices generally don't comply with fire codes or the Americans with Disabilities Act (ADA). Even in the jurisdictions that do allow this type of equipment, campus protection professionals need to remember that there is a whole host of other reasons why the vast majority of these devices are dangerous and a bad investment.

Click **here** and **here** for an in-depth review of the reasons why campuses should not be using this type of equipment, as well as guidance on how to acquire and install access control solutions that are code-compliant and provide the highest return on investment.

Emergency Notification

It's critical for a hospital, college, or K-12 campus to have a robust emergency notification program with multiple technologies in place so that facility administrators, executives, public safety, and/or emergency management personnel can quickly alert students, faculty, clinicians, staff members, parents, and visitors about life-threatening situations.

Unfortunately, the results from the **2022 Campus Safety Emergency Notification Survey** found that fewer campuses are deploying two or more alert systems than they have in previous years.

Only 64% of respondents to the 2022 survey said they use two or more emergency notification systems, with 11% having six or more systems. That's an eight-percentage point drop from **2020** and 16-percentage point drop from 2019. More than a third of last year's respondents (37%) said they use only one system (33%) or zero systems (4%) for emergency notification.

Because of this, we can anticipate more organizations' emergency notification/mass notification systems potentially having single points of failure, meaning that if one technology stops working, there might not be other technologies to bridge the communication gap. Having multiple systems also ensures leaders at a school, college, or hospital can reach more people with alerts during a crisis because the strengths of one technology can compensate for the weaknesses of others.

If a campus is only using one mass notification technology, it most likely won't be able to effectively communicate life-saving information during a crisis to many of the students, faculty, staff, clinicians, and visitors on and off campus.

There is some good news, however. For those respondents who use two or more mass notification systems, the 2022 survey found 9% more have **integrated their systems**, compared to when we asked about integration in 2019. Sixty percent said all (29%) or some (31%) of their systems are integrated, while another 17% are working to integrate their technologies. That said, nearly one in four (23%) respondents said they aren't planning on integrating their emergency/mass notification systems.

The increased rate of integration is a positive trend because integrating systems can reduce the time needed to deploy emergency messages, which helps an organization achieve its goal of quickly disseminating potentially life-saving information during a crisis.

Another positive mass notification trend involves system testing. More than four out of five (82%) survey respondents said they test their emergency notification/mass notification systems several times per year or more.

Frequent and regular testing lets campus public safety and emergency management personnel know if their systems are working properly. It also enables anyone running the technology to practice using it.

Although institutions of higher education have been the primary users of SMS text alert systems among *Campus Safety*'s audience since 2007's Virginia Tech mass shooting, I suspect the Uvalde massacre could have an impact on the mass notification technologies deployed by K-12 schools and school districts in 2023 and beyond. I know of at least two instances (in **Texas** and in **Arizona**) where parents tried to enter schools during lockdowns because they were afraid law enforcement wouldn't respond to reports (which turned out to be false) of a gunman on campus.

These incidents (and probably others that didn't get media coverage) highlight the need for all schools to have a well-thought-out plan for how emergency information and student/parent reunification instructions will be quickly conveyed via text messaging to parents before, during, and after an incident.

The need for SMS text alerting technology in schools is particularly compelling considering the rash of hoax active shooter threats (commonly called "swatting") that have been plaguing K-12 schools and districts in the last half of 2022.

The need for SMS text alerting technology in schools is particularly compelling considering the rash of hoax active shooter threats that have been plaguing K-12 schools and districts in the last half of 2022.

Last year's spate of bomb threats at Historically Black Colleges and Universities (HBCUs) and healthcare facilities that provide transgender medical care also highlight the need for institutions of higher education and hospitals to continue supporting their emergency notification programs.

Video Surveillance

Schools, universities, and hospitals continue to rely heavily on their security cameras for a wide variety of tasks, according to the **2022 Campus Safety Video Surveillance Survey**, with entrances and exits being the most common areas on campus that are monitored by cameras (90%). Perimeters are the second most common area monitored.

Overall, 93% of survey respondents have some sort of security camera system installed on their campuses. In fact, video surveillance is so critical to campus security and safety that just over half of all of last year's respondents said they are considering purchasing new cameras or solutions or expanding, updating, or replacing the systems they have in the next two years. At 57%, institutions of higher education were the most likely to say they are in the market for new or updated systems, compared to K-12 respondents at 47% and healthcare respondents at 52%.

More than three out of five (61%) said their video surveillance systems frequently provide evidence for **investigations**. At 65% and 63% respectively, healthcare respondents and K-12 school respondents were the most likely to say footage from their cameras frequently assist in their investigations, compared to 54% of respondents from colleges and universities.

Two deeply troubling findings, however, involved maintenance. Nearly one in four respondents said they either don't know how often (20%) or never (4%) replace their cameras. Nearly one in five respondents said they don't know how often (17%) or never (2%) maintain their camera systems.

Vape/E-Cigarette Detection

The rate of vaping and e-cigarette use on K-12 campuses has skyrocketed over the past few years, resulting in many student hospitalizations and overdoses on nicotine, THC oil, crystal methamphetamines, opioids, and other drugs. The use of e-cigarettes has also resulted in the dramatic increase in marijuana use by students. According to Michael Dorn, Guy Grace, and Phuong Nguyen of Safe Havens International, the problem is overwhelming secondary schools, resulting in massive amounts of staff time and other resources dedicated to prevention and mitigation.

Although human efforts that increase supervision of students and develop awareness of the dangers of e-cigarette use can help address the problem, according to Safe Havens, K-12 campuses will also need to embrace integrated technologies. Specifically, Safe Havens recommends schools adopt electronic hall pass systems, cameras with analytic software, proximity card access control systems, and vape sensors the are integrated and supported by policies and practices.

To read more about how schools can address vaping and e-cigarette use, click **here**.

Cybersecurity

Like in past years, the biggest elephant in the campus security space in 2023 will be cybersecurity.

A **report** released by digital security firm Emsisoft this month determined 89 education sector organizations were impacted by **ransomware** in 2022. Broken down, hackers demanded ransoms from 44 universities and colleges, and 45 school districts that operate 1,981 schools. Comparatively, in **2021**, 58 districts running 1,043 schools were impacted, as were 26 colleges and universities.

Vice Society, a ransomware group, has been specifically targeting the education sector, with the Los Angeles Unified School District and Cincinnati State College falling victim last year. The ransomware gang appears to be financially motivated and targets organizations with weak security controls that can be forced to pay the ransom, and education and local government fit that bill.

In December, a hacker group that gained access to Knox College's student data emailed students directly with their ransom demands, which appears to be an escalation of threat tactics.

For hospitals, in previous years, Emsisoft tracked incidents across the entire healthcare sector. However, due to the volume of incidents and unclear disclosures, tracking in 2022 was limited to only hospitals. Last year, there were 25 incidents involving hospitals and multi-hospital health systems, potentially impacting patient care at up to 290 hospitals, the report found.

Data including Protected Health Information (PHI) was stolen in at least 17 cases (68%). The most significant was an **attack on CommonSpirit Health**, which operates almost 150 hospitals in 21 states. The incident resulted in the personal data of 623,774 patients being compromised.

Patient safety was also compromised when a computer system for calculating doses of medication was offline. As a result, a three-year-old patient received an extreme overdose of pain medicine. Other affected hospitals temporarily stopped scheduling surgeries or had to redirect ambulances to other hospitals. The latter **proved fatal in Germany in 2020** when a woman died after she was diverted to another hospital 20 miles away when a ransomware attack shut down the university-affiliated hospital where she was being admitted.

Cybersecurity's outlook for 2023 doesn't appear to be any rosier that previous years, with Palo Alto Networks anticipating talent shortages, database management struggles, insufficient detection and response capabilities, improved skills of bad actors, and more making computer network protection an extreme challenge.

It appears the scourge of ransomware and cyberattacks won't slow down anytime soon, so campuses must continue to bolster their cybersecurity measures for the foreseeable future. ✚

HOSPITAL / SCHOOL / UNIVERSITY
Campus Safety

www.campussafetymagazine.com