# Anticipate, Overcome, Recover:

## A Strategic Framework to Create Safer Higher Education Campuses

## Introduction

There's increasing awareness of the need to protect the physical and digital safety of students and staff on college campuses. However, the range and complexity of potential threats are growing even more quickly.

While anticipating and preventing high-profile scenarios such as active shooter events and intruders is the highest priority for campus leaders, they must also increasingly contend with the threat of cyberattacks that can compromise personal information or disrupt mission-critical systems.

"For a long time, physical safety was the area of focus," says Dr. Greg Mathison, Cisco's solutions manager for education. "Now cybersecurity challenges have grown exponentially and continue to grow."

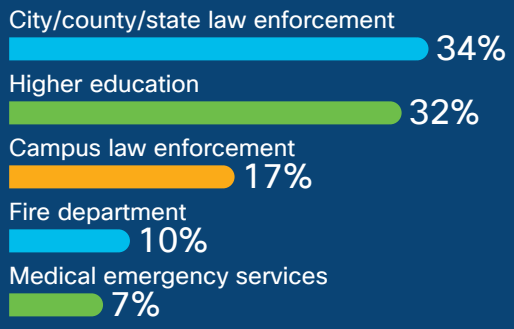
Drawing from a recent national Center for Digital Education (CDE) survey of higher education leaders, campus security personnel and first responders, this white paper explores key security priorities and challenges, and outlines technology-driven approaches that can help ensure campuses — and the people who learn and work on them — remain safe.

"This is all about the personal element," Mathison says. "How are people supposed to learn if they don't feel safe? How can they teach if they don't feel safe?"

## About the Survey

CDE surveyed 175 stakeholders involved in higher education campus safety, including campus leaders and law enforcement officials and their counterparts among city, county and state law enforcement officials; medical emergency services; and fire departments. Respondents were roughly evenly divided among campus and non-campus roles.

## Which best describes your jurisdiction/ primary employer?




*Source: CDE Survey*

## Key Priorities and Challenges

Higher education leaders, as well as their students and staff, are all too aware of the reality of physical threats. At the same time, the rapid growth and evolving nature of digital threats challenges cybersecurity efforts at many institutions.

"The threats are exponential in nature — more devices, more attack surfaces and more attacks to manage," says Mathison. "Based on this, campuses need greater automation and the ability to orchestrate their security response."

### Physical Threats

The three most commonly cited physical threats by CDE survey respondents involve averting potential acts of violence. More than three-quarters of campus leaders (77 percent) rank active shooter events as their top safety concern, followed by assaults and rapes (70 percent), and intruders entering campus (47 percent).

Campus leaders also cited the importance of protecting students and staff from natural disasters (43 percent) and preventing thefts and burglaries (29 percent cited the theft of student property as a top concern).

There's also growing recognition of the impact of alcohol and drug abuse, cited as a top safety concern by nearly half (45 percent) of campus leaders. One-third of respondents also noted suicide prevention is a top concern, reflecting the increasing emphasis on mental health and well-being on many campuses.

### Digital Threats

Campus leaders are clearly aware of the threats cyberattacks pose to their institutions and those who learn and work in them. Two-thirds of survey respondents (66 percent) ranked cyberattacks a top concern in the CDE survey — superseded only by active shooter events and assaults.

The recognition of the threat, in many cases, may come from direct experience. In a 2018 Cisco survey, 60 percent of higher education institutions reported at least one

public security breach – a rate five percent higher than the average across all industries.[1] As one CDE survey participant said, "We're vulnerable."

Cyber threats have been exacerbated in recent years by the proliferation of student-owned laptops, smartphones and tablets on campus networks. Security experts also point to the growth in connected campus IoT devices, including traditional systems like HVAC but also newly connected services like internet-enabled washers, dryers and vending machines.

Not surprisingly, more than 70 percent of higher education leaders responding to the Cisco survey said IoT and student devices pose a high or moderate security risk on their campuses. More surprising is that nearly one in three (29 percent) respondents have already faced attacks in operational technology areas, including the IoT-driven hardware and machinery described above. Another 36 percent anticipate attacks in the next year, according to the survey.

The impact can be significant. Of campus leaders who have experienced cyberattacks, half (49 percent) say their systems were down for nine or more hours as a result of a security breach. And more than half of all attacks (51 percent) result in financial damages greater than $500,000. Nearly three-quarters (74 percent) result in at least $100,000 in losses.[2]

As with physical threats, there's a redoubled emphasis on students' emotional health in the digital sphere. Nearly one in three (30 percent) campus leaders responding to the CDE survey ranked bullying – both in-person and online – as a top safety concern at their institutions.

## Key Challenges

Higher education institutions face unique challenges in addressing these physical and digital threats, many of which stem directly from their core mission. Most campuses are open by design, have a wide range of facilities and buildings, and draw large numbers of people – including the public – to events. Students who learn and live on campuses also require access to campus networks. They can have as many as eight or nine personal devices connected to campus Wi-Fi networks, campus technology officials say, requiring additional capacity and security to protect personal information.[3] Longstanding institutional

culture contributes to a siloed approach to decision-making on many campuses, with an emphasis often placed on consensus-building among all stakeholders. All these challenges make planning and coordinating responses to physical and digital threats more complex.

Addressing physical threats is complicated by a range of factors, including crime in the surrounding community, disagreements on the best ways to improve campus safety, a lack of mental health services, and regulations or rules that prohibit safety measures, according to the CDE survey.

Campus leaders also cite multiple challenges in addressing digital security, including limited budgets for cybersecurity monitoring, a lack of existing technology infrastructure and concerns that cybersecurity measures could result in policies counterproductive to the campus mission. Staffing for cybersecurity efforts is particularly difficult in higher education. The median number of digital security personnel at colleges and universities of all sizes is 20 — half of that across all industries.[4]

> "On many campuses much of the effort is on mitigating the impact of events. … The real burden is the more challenging aspect of recognizing early indicators and enacting proactive prevention methodologies."
>
> *Craig Coale, Senior Advisor for Public Safety and Defense, Cisco*

And survey participants noted a range of cross-cutting challenges impacting their efforts to assure physical and digital safety, including privacy concerns, cumbersome procurement and budgetary processes, lack of buy-in from campus leadership and staff, and challenges communicating key policies to all stakeholders given the siloed nature of many institutions.

"There's often no single point of accountability and authority," says Mathison.

## Anticipate, Overcome, Recover: A Strategic Framework

Over the past few decades, higher education institutions have refined their approaches to address these challenges. Reflecting the mission areas in the Department of Homeland Security National Recovery Framework,[5] campus leaders often approach safety measures across three broad domains:

- **Anticipate** — preventive measures to identify potential threats and protection strategies to limit physical and digital access
- **Overcome** — strategies to respond to incidents and mitigate their impact
- **Recover** — a comprehensive approach to communicating and prioritizing safety after an incident occurs

> The median number of digital security personnel at colleges and universities of all sizes is 20 – half of that across all industries.

"However, on many campuses much of the effort is on mitigating the impact of events. … The real burden is the more challenging aspect of recognizing early indicators and enacting proactive prevention methodologies. The intent is to notice individuals in need based on indicators and get them help before there is an incident," says Craig Coale, Cisco's senior advisor for public safety and defense. "This does two things. It first moves the intent of the campus safety to helping individuals in need and getting them genuine assistance. Second, it alleviates each interaction with police from becoming a punitive incident."

Most campuses have developed and refined comprehensive emergency management plans to help address potential threats. At the behest of federal officials, these plans now are often made in coordination with local public safety organizations, first responders and other community organizations to maximize the use of resources. Majorities of leaders in higher education and public safety agencies agree these efforts are working well. More than half of all survey respondents (57 percent) say their organizations work very or somewhat well together, according to the CDE survey. (To learn more about collaboration between higher education and public safety organizations, see the report, "Building Safer College Campuses with Greater Collaboration," available at govtech.com/education/papers/safercampusreport.)

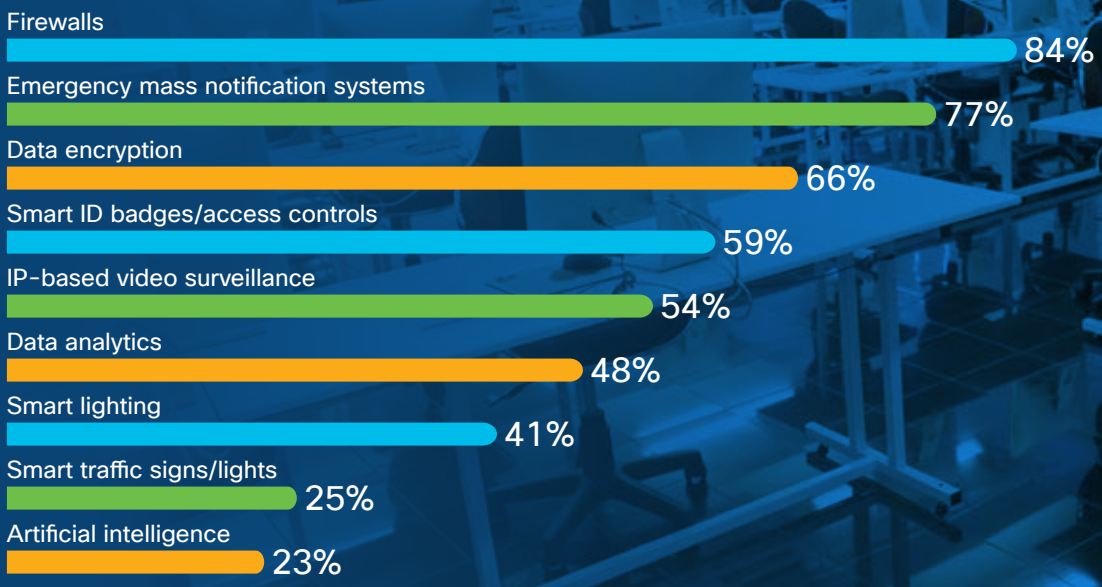
These collaborations are contributing to an ongoing mindset shift toward a greater emphasis on preventing both physical and digital threats on higher education campuses. Federal and state policy are also focusing on early detection and intervention, particularly around mental health issues such as suicide prevention.

"We've moved from after the fact to during the event to the largest extent possible," says Mathison. "[Now] we have to push to prevent."

### The Role of Technology

Technology increasingly plays key roles in comprehensive plans to ensure physical and digital safety on higher education campuses by helping campus officials better

## Physical and Digital Safety Tools in Use




*Source: CDE Survey*

address the full spectrum of prevention, response and recovery within their staffing and budget constraints.

"Technology can be the key asset in enabling this combined approach," says Coale. "It's important to focus equally on detecting indicators to prevent negative events by getting students early help, and enabling better information sharing about events with responding persons to better coordinate across agencies."

### Anticipate

Prevention strategies focus on identifying and deterring potential threats before they take shape, while protection strategies control access and alert public safety staff when issues occur.

Among the technologies that can help campuses anticipate physical and digital threats:

**IP-based video surveillance systems** play vital roles in prevention – from serving as a deterrent to allowing security officials to more effectively monitor campus facilities. When combined with video analytics tools, systems can automatically monitor feeds in real time and alert campus and public safety officials when potentially dangerous events occur, improving response time and potentially saving lives.

**Physical access control systems,** which often are used in conjunction with smart ID cards or badges, limit access to facilities to authorized students or staff. They also can be integrated with video surveillance solutions to allow access to approved individuals or automatically limit access in the case of emergency.

**Alarm systems with sensors,** sirens and lights on emergency exit doors can alert public safety staff when a situation occurs. In similar fashion, help buttons or mobile apps with a reporting function allow students and staff to proactively alert first responders to potential threats.

**Facial and license plate recognition,** combined with analytics based on social media postings or databases of criminal convictions or stolen vehicles, can help identify threats.

**A system of tools working in aggregate** allows campus leaders to detect those who need help by correlating risk indicators. This includes social monitoring, a "see-something-say-something" anonymous platform, bullying detection, self reporting/mental health options and more. An event correlation dashboard with workflow tracking can ensure at-risk individuals receive assistance before negative events or interactions occur.

**Many cybersecurity tools** involved in securing higher education networks and the data stored on them involve limiting access to authorized users. Firewalls and data encryption play crucial roles in a comprehensive cybersecurity solution and are used on most campuses

## At UNC-Pembroke, a Clean Slate for Cybersecurity

The nation's only four-year public institution founded by American Indians for American Indians, the University of North Carolina at Pembroke (UNCP) has developed a robust IT infrastructure capable of serving its more than 7,000 students, faculty and staff. While efforts were focused around technology access and digital classroom collaboration tools, leaders understood the risks to digital safety from the start.

"We are a small school with a very small IT team, yet we confront the same threats as much larger schools with much larger staffs," says Nancy Crouch, who served as UNCP's associate vice chancellor for technology resources and CIO. "We all understand that education institutions are a tempting target, and bad actors are indiscriminate when it comes to identifying those with vulnerabilities."

Leaders made security one of three goals in UNCP's technology plan, hiring a retired military veteran with cybersecurity experience as the institution's chief information security officer (CISO) through the Wounded Warriors program as the institution implemented comprehensive IT and security infrastructure.

"The first benefit we noticed after implementation was the increase in visibility – this was a blessing and a curse. We instantly noticed we had more issues than we thought we had, so it took more time to remediate than planned," says CISO Don Bryant. "Once we had a clean slate and began to take advantage of automation, we were able to see the most significant threats and prioritize on issues ... that have the potential to do the most damage, rather than spending time on the smaller annoyances."

*https://www.cisco.com/c/en/us/solutions/collaboration/unc-pembroke.html*

nationwide (see box, above). Data analytics, which mine data to identify threats or unusual access patterns, are now in place in nearly half of campuses, according to the CDE survey.

### Overcome

Once an incident does occur, the goal is to reduce the impact on people, systems and physical property. Collaboration with first responders, law enforcement and medical personnel, community leaders and the public can mitigate damage and save lives. A critical part of mitigation involves communicating with students and staff in real time, such as issuing orders to evacuate or shelter in place.

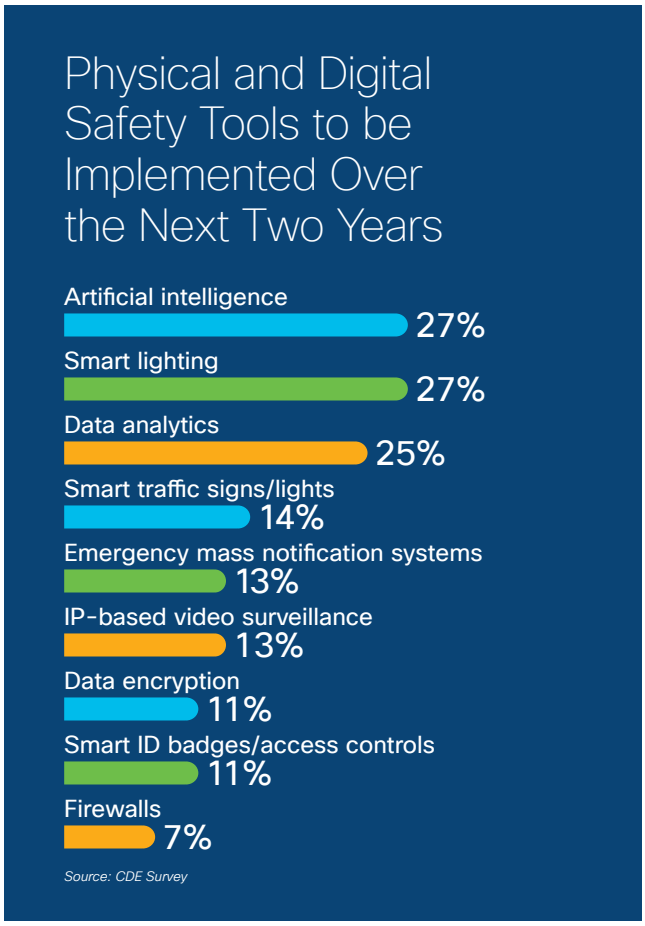
> "Solutions must be deployed in practical and almost passive methods in order to provide additional information-enhancing response without becoming a distractor to responders."
>
> *Craig Coale, Senior Advisor for Public Safety and Defense, Cisco*

Among the technologies that can help campuses during incidents:

**Emergency mass notification systems** are now in place in more than three-quarters (77 percent) of campuses, according to the CDE survey. These systems focus on sharing specific information via computers, mobile devices, digital signage, smart boards or monitors in classrooms and public spaces, and social media. Today, nearly half (41 percent) of campuses also are integrating these systems with those operated by local communities.

**Collaboration and situational awareness tools** include voice, video and data sharing to ensure first responders receive information about evolving situations and can communicate to coordinate their response. Nearly 40 percent of campus leaders have adopted shared digital communication platforms with local law enforcement and other first responders, supplementing longstanding and nearly ubiquitous communication technologies like 911 systems and two-way radios, according to the CDE survey. But new technologies must be as simple to use as the ones they are replacing, according to Coale.

"Technology adding complexity is a barrier to adoption and use in crisis situations," he says. "Solutions must be deployed in practical and almost passive methods




in order to provide additional information-enhancing response without becoming a distractor to responders."

## Recover

Recovery strategies disseminate information to those involved and help them return to normal activities. They also focus on collecting and sharing lessons learned to prepare for future events.

Among the technologies that can help campuses with this important work:

**Notification systems** play a critical role in outreach to students, staff and the broader community. Campuses can coordinate these systems with social media to help track the location and safety of students following natural disasters or other events.

**Sensors, video, networking analytics and collaboration/communication systems** can be mined for data to help analyze incidents after they occur, identify lessons learned, and reshape prevention and response strategies as needed. According to Coale, after-action reports for incidents consistently reveal a lack of information sharing, an inability to detect indicators of potential threats and a low level of agency interoperability – underscoring the importance of focusing on both prevention and response as higher education leaders rethink their own strategies and systems.

## Conclusion

As higher education leaders' approach to anticipating, responding to and recovering from physical and digital safety events evolves, technology will play an even greater role. The tools campus leaders plan to implement over the next two years will enable them to continue to shift from response to prevention – with AI, smart lighting and data analytics the most commonly cited planned technology upgrades (see box, at left). Notably, every respondent that did not have an emergency notification system in place plans to implement one within the next two years.

Beyond individual solutions, campus leaders must ensure their technology infrastructure can support tools that promote both physical and digital safety. Along with providing connectivity for IP-based video cameras and other surveillance, resilient networks are essential to ensure effective communication with first responders and community partners before and during emergencies.

It's critical that the institution's underlying technology platforms – networks, wireless access points and more – can integrate with existing and emerging safety technologies. Given the range of privacy concerns at higher education institutions, cited as a barrier by 18 percent of campus leaders and 14 percent of local agencies in the CDE survey, it's also important to ensure campus networks and other IT infrastructure have adequate levels of security to prevent them from data breaches and disruptions, particularly during times of crisis.

Public safety officials and other local agency leaders must be able to securely access these tools to have the information they need to make decisions during emergencies. That's particularly true as more campuses build on existing partnerships with public safety agencies to collaborate on digital security, an area where between 23 and 41 percent of campus and law enforcement leaders responding to the CDE survey say significant steps are being taken.

"Campuses must rapidly adapt to leverage the abundance of technologies being deployed as a force multiplier for better awareness, better prediction, more effective response and rapid recovery," says Coale. "The best way to do this is by solving the two big challenges – sharing relevant information more effectively and better coordinating responses across agencies."

Endnotes


1. https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/OCA/Assets/Education/By_the_numbers_cybersecurity_challenges_in_higher_education.pdf?ccid=cc000124&oid=ifgsc008817
2. Ibid.
3. https://www.insidehighered.com/news/2018/04/17/universities-work-offer-complete-wi-fi-coverage-campus
4. https://www.cisco.com/c/dam/m/digital/elq-cmcglobal/OCA/Assets/Education/By_the_numbers_cybersecurity_challenges_in_higher_education.pdf?ccid=cc000124&oid=ifgsc008817
5. https://www.fema.gov/national-disaster-recovery-framework


*PHOTOS PROVIDED BY SHUTTERSTOCK.COM*

Produced by:

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**

For:

CISCO

Digital education is making it possible for students to learn more, in new ways, in new places, with new connections to resources around the globe. Cisco is leading this new digital world in education, including with solutions for Safer Schools, which support students as they learn without limits.
**www.cisco.com/go/education**