Recent high-profile security incidents on higher education campuses have fast-tracked safety plans, including video surveillance, physical access control, and communications.

But vulnerabilities remain. "Forty-three percent of campuses lack a visitor management system, 39 percent have a video management system that is not well integrated with other systems, and 50 percent cannot lock down more than three-quarters of their campus," says Lindsay Hiebert, a senior manager for Cisco Connected Physical Security solutions, citing a survey in Campus Safety Yearbook. "And one in three have radio systems that cannot interoperate with first responders’ radio systems."

Five advances in physical safety help to make college and university safety programs more effective and affordable.

1 – Operate All Physical Security Systems Over the Campus IP Network
Connecting physical security solutions to the existing IP network eliminates the need for multiple specialized networks. It also helps to improve campus safety and security because different systems can work together to accelerate incident detection and response. For example, Cisco® Unified IP Phones in classrooms, lecture halls, and offices can serve as easy-to-use security consoles for:

- Lockdowns: Lock down a room, building, or the entire campus by pressing a button on a Cisco Unified IP Phone.
- Visitor management: When a visitor presses a button to request access to a controlled area, a staff member hears an alert and sees real-time video on the Cisco Unified IP Phone’s built-in display. After the visitor looks into the video surveillance camera to explain the purpose of the visit, the staff member can press a button on the phone to unlock the door.
- Panic message: Press a button to send a panic message by email or instant message to predefined personnel.

And with Cisco IP Interoperability and Collaboration System (IPICS), administrators, campus safety officers, and first responders can join talk groups to collaborate on incident response. They can use any type of radio system, traditional phone, IP phone, smartphone, tablet, or laptop.

2 – Invest Once for All Campuses
It's no longer necessary to purchase management solutions for each campus. With Cisco video surveillance and physical access control solutions, you can centrally manage tens of thousands of endpoints on any campus. Individual campuses need no equipment other than cameras and door controllers.

3 – Lower Data Center Costs with Virtualized Servers
Cisco Physical Security solutions and Cisco Unified Communications applications can operate on a Cisco Unified Computing System™—the same one you might already use for learning, research, or administrative applications. Multiple virtual applications can operate on the same physical server, lowering space, power, and cooling costs as well as management overhead. Virtualization can also improve availability because Cisco UCS® has redundancy built in.

4 – Simplify Large-Scale Camera Deployments with Automated Configuration and Medianet Capabilities
Manual configuration requires 30-45 minutes for each video surveillance camera, an expensive proposition for colleges and universities with hundreds or thousands of cameras. “Preparing a Cisco Video Surveillance 6000 Series IP Camera for use is as simple as connecting a cable,” Hiebert says. Cisco medianet technologies do all the work in the background, and the camera begins transmitting video in approximately 15 seconds.

5 – Capture the High-Quality Images Needed to Identify People
Grainy images don’t allow you positively identify people or read car license plates. New Cisco Video Surveillance 6000 Series IP Cameras provide clear, 2.1-megapixel images and 1080p video streams. Some models have an integrated infrared (IR) illuminator for nighttime surveillance.

To read more about Cisco Physical Security Solutions for education, visit:
http://www.cisco.com/go/physicalsecurity