University Builds Physical Security Framework for Growth

California State University Channel Islands centralized video surveillance and physical access control systems.

EXECUTIVE SUMMARY

CALIFORNIA STATE UNIVERSITY CHANNEL ISLANDS

- Higher Education
- Camarillo, California
- 575 Employees; 4055 Students

CHALLENGE

- Create a safe environment for learning
- Prepare for campus growth
- Minimize ongoing operational costs

SOLUTION

- Deployed Cisco Physical Access Control Solution to control existing door locks over the network
- Engaged NIC Partners, a Cisco Gold Certified Partner, to implement Cisco Video Surveillance solution, connecting existing analog cameras as well as new Cisco IP Video Surveillance Cameras
- Integrated Cisco solutions with Microsoft Active Directory

RESULTS

- Saved US$50,000 annually to rekey locks (expected)
- Freed University Police from 10 to 50 calls per week to open doors
- Reduced long-term operational costs for video surveillance

Challenge

Founded in 2002, California State University Channel Islands (CI) is the newest of the 23 universities in the CSU system. The student-centered, four-year, public university is known for its interdisciplinary, multicultural, and international perspectives and its emphasis on experiential and service learning.

CI is currently renovating the sprawling campus, originally built in the 1930s, to create a 21st century learning environment. To preserve the University's excellent safety record, the IT department and University Police sought modern physical security systems that would minimize ongoing operational costs and scale in step with campus growth. "We knew that a network-based physical access control solution would increase administrative efficiency and improve security for students, staff, and faculty," says A. Michael Berman, Chief Information Officer at CI.

Since opening, the University had acquired a mix of physical access controls for exterior doors, including locks with wired and wireless connections to the network and computer-managed (CM) locks that a technician must physically visit to program. The lack of central management increased operational costs. For example, if someone lost a master key, replacing locks could cost up to $40,000 in hardware and labor, and even as much as $100,000. Furthermore, University Police officers had to take time away from their primary responsibilities to open doors for employees who had lost their keys or needed to enter buildings after hours. "We wanted to offload our police officers from having to unlock doors so that they could focus on campus safety," says Herbert Aquino, manager of IT infrastructure at CI. "We envisioned a physical access control system that would enable authorized personnel to lock and unlock doors centrally, over the network."

At the same time, the University decided to consolidate its disparate video surveillance systems to reduce costs and ease the management burden. Previously, individual departments had purchased their own video surveillance cameras and digital video recorders. University Police had to learn to use each system in order to review the events leading up to an incident. Bringing analog cable to video cameras in remote parts of the campus was costly. And the IT department had to learn to troubleshoot and maintain the disparate systems, taking time away from strategic projects. "A centrally managed video surveillance system would simplify incident investigation and also reduce support overhead for the IT department," says Matt Hughes, network analyst at CI.

The opportunity to standardize on physical security systems arose when CI decided to institute a one-card system for meals and copy and print services. University leaders realized that using the card for building access would increase the return on investment.

Solution

CI is building a physical security foundation for the future, using Cisco® Physical Access Control and Cisco Video Surveillance solutions. “We had confidence in Cisco Physical Security solutions because of their quality, open standards-based approach, and Cisco’s corporate stability,” says Berman. “We know we can count on Cisco to be an IT partner for the University for the expected 10- to 15-year life of the solution.”

The IT department especially liked the integration between its Cisco network and the Cisco Physical Security solutions. “The other vendors we evaluated provided only one capability, such as door control,” says Mike Long, senior telecommunications analyst at CI. “Only Cisco provides both the underlying network and the physical security hardware, simplifying integration with Active Directory, our campus identity management system.”

The University IT team engaged NIC Partners, a Cisco Gold Certified Partner, to collaborate on designing and implementing the Cisco Physical Security system, integrating it with the existing Cisco network and Microsoft Active Directory. The University conducted a proof of concept in the main IT building. All exterior doors can be locked or unlocked from a web-based management console, according to a schedule or on demand. The IT team and NIC Partners integrated several existing analog video surveillance cameras into Cisco Video Surveillance Manager, as well as new Cisco IP Video Surveillance Cameras. When a Cisco camera senses motion, it begins capturing video for later review. Cameras also begin capturing video when Cisco Physical Access Control Manager detects that a door has been opened, giving campus security personnel earlier awareness of issues that require investigation.

The proof of concept has succeeded, and the University IT team will now begin expanding the use of the Cisco solution throughout the campus, beginning with computing and research labs. “Our campus is relatively safe, so we are installing cameras in remote buildings and areas prone to vandalism, such as elevators in student housing,” says Long.

> "We had confidence in Cisco Physical Security solutions because of their quality, open standards-based approach, and Cisco's corporate stability. We know we can count on Cisco to be an IT partner for the University for the expected 10- to 15-year life of the solution."
>
> **—A. Michael Berman, Chief Information Officer, California State University Channel Islands**

Results

Foundation for Growth

California's student population is increasing, and CI is well positioned to expand enrollment because its buildings currently occupy a small portion of the campus. Using Cisco Physical Security solutions, IT staff can easily add cameras and door hardware from any vendor using open standards, and manage them centrally. A projected 500 door locks will take no more time to manage than the 5 in the proof of concept. "Using Cisco Physical Security Solutions, we have built a standard for the future of the University," says Aquino.

Flexible Options for Video Surveillance

The University Police Department uses video surveillance primarily for forensics, to review the events leading up to and during an incident. Using Cisco Video Surveillance Manager, University Police can use a web browser in any location to review video from any video surveillance camera on campus, from any vendor. "Cisco's open-standards approach to video surveillance protects our existing investments in cameras, and gives us the flexibility to add any vendors' cameras in the future," says Long.

What's more, the new system makes it easy for University Police to view real-time video when needed. "With our previous video surveillance system, we had to either monitor all cameras all of the time or use video strictly for forensics," says Hughes. "Cisco Video Surveillance Manager enables our University Police to combine both approaches, archiving all video according to our retention policies, and selectively viewing real-time video for reconnaissance when needed." One example is when someone attempts to force open a door. If this occurs, the Cisco Physical Access Control system signals a nearby video camera to begin streaming video to the Police Department, and can also alert University Police on any communications device, including a Cisco Unified IP phone or cell phone, or by email.

Lower Costs for Physical Access Control

The Cisco Physical Access Control system preserved the University's existing investments, because it connects all types of door locks used on campus: wired connections, wireless connections, and even CM locks, which are not specifically designed for connection to a network.

Ongoing operational costs for physical security have decreased as well. When personnel lose their access cards, the campus locksmith no longer needs to walk to each CM lock to reprogram it. Instead, the IT staff can immediately cancel the old card and issue a new one. What's more, faculty and staff are spared the wait for a new metal key.

Ease of Administration

Integration between the Cisco Physical Security solutions and Microsoft Active Directory saves time for the IT team. "We don't have to spend time adding and deleting users, because Active Directory already has up-to-date information," Aquino says. When a new faculty member joins the University, the IT staff can easily assign appropriate building access control privileges from a web interface.

Next Steps

PRODUCT LIST
Physical Security • Cisco Video Surveillance Manager • Cisco Video Surveillance IP Cameras • Cisco Physical Access Control

To accelerate event detection and response, CI is beginning to integrate physical security solutions from Cisco and other vendors. To minimize the effort, the IT team is using Cisco Validated Design for Education, which provides tested designs of integrated technologies within the Cisco Open Platform for Safety for Security framework. For example, EdgeFrontier Software from Augusta Systems, a Cisco physical security ecosystem partner, will sense when a panic button is pushed and automatically begin streaming video to the University Police Department. Similarly, an event such as a fire or environmental alarm will trigger the Cisco Physical Access Control system to automatically lock or unlock doors.

For More Information

To learn more about Cisco Physical Security Systems, visit: http://www.cisco.com/go/physec

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C36-611693-00 07/10