

Safety and Security: Strengthen the Five Steps for Incident Response

When your security personnel receive an alert that a door has been forced open, what do they do? Calling people who work in the area to try to find out what's going on can postpone response. But sending an armed guard is an unnecessary expense if the alarm was triggered by an employee holding a door open for a package delivery.

Now you have a better option. When all physical safety and security systems are connected to the building's existing IP network, you can set up the building access control system to tell the video surveillance cameras to begin streaming video whenever an alarm is sent. Even better, the system can send an alert to the nearest security employee, on any communications device, based on the time of day and other business rules.

"Government's investments in video surveillance cameras, building access controls, sensors, and communications become even more valuable when they can work together over the existing IP network," says Jennifer Bremer, with Cisco's safety and security solutions group. By integrating physical security solutions on the IP network, agencies are better equipped throughout the five-step incident response: prepare, prevent, detect, assess, and respond.

Prepare: Distribute Information to Any Location, Any Device

Disaster preparedness is an essential component of government continuity of operations (COOP) plans. When your agency's physical safety and security systems are connected to the IP network, authorized employees can monitor and control them from any location with a wired or wireless network connection, including home.

Prevent: Encourage Good Behavior

Deploying visible video surveillance cameras can encourage good behavior. As an example, the Chicago Transit Authority used a Department of Homeland Security grant to install Cisco mobile access routers in police vehicles and 40 buses, which had earlier been equipped with IP-based video cameras and digital video recorders. When police officers are within 600 feet of a bus, they can view streaming video of activities within the bus on their dash-mounted, ruggedized laptops. "The mobile video-surveillance system is an effective deterrent to crime and vandalism and also lets officers spot brewing criminal or terrorist activity," says Morgan Wright, global manager for public safety, Cisco.

Prevention extends to information security—as well. Your agency can use Cisco Self-Defending Network technologies such as intrusion prevention and network admission control to prevent cyberattacks and unauthorized access to sensitive information.

Detect: Use Any Kind of Sensor, Old or New

Security personnel and first responders can detect threats sooner when they can view inputs from a variety of sensors on one management interface, including:

- Chemical, biological, radiological, nuclear, and explosive (CBRNE) sensors
- Video surveillance cameras, with or without video analytics software, that can detect predefined events such as an unattended package, or a person tailgating an employee through an access gate
- Building access controls
- Motion detectors
- RFID readers, which can indicate if equipment is taken out of an area
- Gunshot detection and location systems, which detect gunshots and begin transmitting GPS coordinates and video

When your IP network is used as the platform for communications as well as physical safety and security systems, detected events can automatically trigger alerts to appropriate personnel on their chosen device: phone, mobile phone, radio, or pager. If video analytics software detects an unattended package, for example, it can direct a chemical sensor in the area to begin sampling, and transmit the information to the appropriate personnel based on the agency's policies.

Assess: Determine the Appropriate Response

After detecting a threat, safety personnel need to assess it to determine the appropriate response. Is the intruder a person or an animal? Is an odor a simple natural-gas leak that one person can fix, or a major chemical leak that threatens a neighborhood and requires a multi-agency response? The ability to view information from multiple sensors from the same interface, then project it on maps and three-dimensional models, helps you decide on the appropriate response.

Respond: Communicate with Personnel and Citizens

When responding to an incident, you need to coordinate with people in the same or different agencies, using different communications devices. Cisco IP Interoperability and Collaboration System (IPICS) enables people to communicate directly using any type of radio system as well as phones, cell phones, or laptops. To provide citizens with updates and instructions, your agency can use Cisco Unified Communications applications that automatically make phone calls or send emails or text messages. And with Cisco Digital Media System (DMS) you can send up-to-the-minute alerts to digital signage deployed in high-traffic areas—such as airports, mass transit stations, and downtown areas.

You can integrate your existing physical security systems into your IP network using the Cisco Open Platform for Safety and Security.

To read more, visit: www.cisco.com/go/govsafety.




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.

 CCDE, CCVP, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn is a service mark; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0801R)