



New Era in Public Safety

Powerful new technologies use existing infrastructure to improve safety without huge costs.

Public safety and security are on more people's minds these days, and with good reason. Many high-profile incidents in recent years have changed the way government leaders look at public safety and security. It's not a matter to be taken lightly.

Fortunately for public-sector leaders — and for the public — new technology tools are proving to be valuable, cost-effective allies in providing security. The power of these tools is greatly multiplied when they're tightly integrated in the "closed loop" continuum of Cisco's Safety and Security Solution Portfolio. The portfolio contains numerous options that help governments cover five key steps when it comes to dealing with a variety of hazards and threats: prepare, prevent, detect, assess and respond.

The portfolio is based on a secure, multiservice network infrastructure. It's a network that can handle all kinds of data, whether it's simple e-mail or more complicated audio and video. With the network's open platform, it can easily integrate Cisco's partners, allowing governments and educational institutions to put together the exact pieces they need to protect the public, borders, facilities, infrastructure, students and employees.

Whether the need is for asset protection, video surveillance, video analytics, network security, building access control or a variety of other security measures, public-sector agencies can get what they require from the Safety and Security Solution Portfolio.

The portfolio provides a lot of flexibility. Cisco and its industry-leading partners offer a unique set of possibilities. It's a strong package that can't be duplicated. Cisco's open platform allows partners to engage the network and each other, building on other partner capabilities for a much stronger security presence.

Most public-sector agencies have built their security systems in a more piecemeal fashion. The result is a collection of disparate systems that often can't communicate with each other — and certainly can't communicate as quickly as a system with the latest tools.

Cisco combines an organization's existing infrastructure, its own proven solutions and its partners' technologies to significantly expand an organization's safety and security capabilities. By leveraging an organization's existing equipment, it can add big value in a cost-effective manner.

The result is a nimble, integrated system that can automatically respond to many incidents. And when human decisions are needed, decision-makers have a wealth of information in an easy-to-grasp format. That enables quicker, better decisions, which means improved safety for employees, students, responders and the public.

The Five-Step Continuum

Prepare, prevent, detect, assess and respond: It's a cycle that's based on federal government recommen-

CASE STUDY

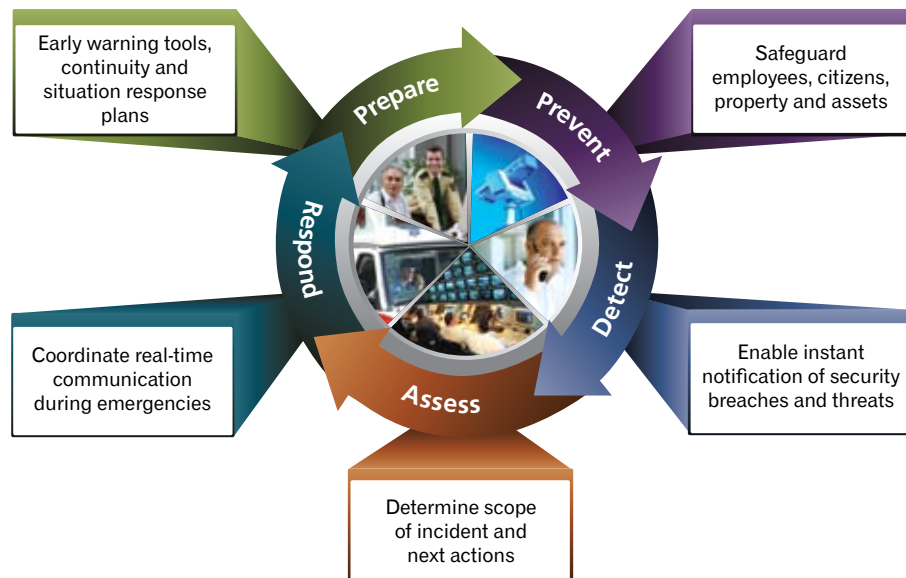
Interoperable Communications

How can five jurisdictions communicate seamlessly with each other when they're on separate, private radio networks? For law enforcement and emergency response agencies near the Virginia/North Carolina border, the answer was an IP-based communications system from Cisco. The solution leveraged the existing IP network and equipment, keeping costs low. Expenditures were 10 percent of what they would have been if each agency changed to the same system.

Public-sector agencies in the Danville, Va., area have seen significant results. Now, for example, it's no longer common for speeding cars to get away at the state border. Prior to the new system, they could, because different police departments couldn't communicate well. That scenario occurred about 200 times each year.

Cisco's IP Interoperability and Collaboration System (IPICS) made it all possible. IPICS converts disparate communications signals so they can be carried over an ordinary IP network. Thus communications from different devices, frequencies and departments are smoothly integrated, and each agency can talk to other jurisdictions on the system, regardless of their individual equipment and infrastructure.

Safety and Security: A Five-Step Process



ditions for public safety. It's about creating a cohesive system for better protection and responsiveness. By taking this holistic approach, governments and educational organizations can have security systems in which the parts complement each other for better overall performance.

The five-step continuum is best seen as a circle or loop. Closing that loop as tightly as possible means moving information to the right place at the right time — with no latency or delay. It can be the difference between life and death.

Prepare — The federal government highly recommends preparation for threats and disasters of all kinds for state and local governments. The federal government follows the National Incident Management System (NIMS), which includes heavy emphasis on continuity of operations (COOP) planning.

A COOP plan lets an organization continue operating through a variety of security incidents. Business continuity plans have served the private sector well. Governments should lay out their continuity plans too. Preparing for all possible security threats is a key first step. One way to prepare is to have Internet protocol (IP) networks linked to physical security systems. This enables video, sensors, alarms, notifications and more.

Prevent — Solid prevention keeps people safe. Whether it's a video surveillance camera or building access controls, strong technology makes employees, citizens, property and assets safer.

In physical security, video surveillance cameras are showing up in more places than ever before. That's because they're effective. New cameras can see more detail, and sending the signals over an IP network gives a lot of flexibility in how images are viewed. Even the mere presence of video cameras



can prevent incidents, as criminals don't want to be seen on camera.

Network security can be improved too, with stronger internal security policies and applications that enforce them. Proper emphasis on network security can prevent cyber-attacks from damaging systems.

Detect — Security breaches and other threats can do serious damage if they go undetected for even a short time. A strong security system can notify administrators of physical and network security issues immediately. Access control systems, for example, can detect not only actual breaches, but also attempted breaches. If someone tries to gain entry by swiping a bad card, they won't get in, and the system can alert people of the attempt. If someone physically forces a door open, the system will be aware of that too, and can set off alarms and alerts automatically.

Surveillance cameras can be linked to gunshot detectors. Sensors not only pick up gunshots, they can also alert officers and trigger a surveillance camera to move toward the source of the sound.

Decision-makers need to determine the scope of the incident and decide on the actions needed in response. The more situational awareness they have, the better decisions they can make.

CASE STUDY

A Sound Investment

The Georgia Forestry Commission (GFC) provides fire protection services for 129 counties. The GFC needs a dependable communications system, both internally and with local firefighting agencies. Other state agencies, such as the Georgia State Patrol, also rely on the GFC radio network when out of range of their regional networks.

Previously radio traffic between districts traveled over leased analog circuits. That proved to be not only too expensive, but also undependable at times. The answer was Cisco's IPICS and a multiprotocol label-switching (MPLS) virtual private network (VPN). IPICS and the VPN

enabled highly reliable communications for the GFC and agencies it interacts with.

The solution improved interagency collaboration and also improved policy compliance, as different channels were established for different types of communication. Return on investment was also positive since the new system was paid for within three years with the savings realized by turning off the analog circuits.

IPICS is also expected to enable more elaborate projects in the future for the GFC, which now has the flexibility to adopt regional or centralized dispatch as the needs arise.

CASE STUDY

Pandemic Planning and Response

Oakland County, Mich., challenged itself — and won — with an ambitious exercise in flu pandemic planning and response. Using Cisco communications to keep numerous staffers and agencies on the same page, the county vaccinated 12,096 residents in five hours. It took a lot of cross-boundary planning and collaboration, but the exercise was highly successful.

The county brought in Cisco to provide a network-centric communication and situational awareness platform. This allowed a broad array of organizations to communicate and work together efficiently. Cisco deployed IPICS and Video Surveillance Manager (VSM). VSM

allowed both analog and IP cameras to stream video over the Internet to the emergency operations center (EOC) and various devices.

The Oakland County Health Division (OCHD) led the exercise, which included the county executive's office, county IT, hospitals, police and fire departments, medical responders and others in the community. The OCHD organized the EOC, various responders, and the staging of vaccine-dispensing locations in schools, hospitals and other public buildings. It was a big job, but the Cisco platform enabled seamless communication, and the county is now better prepared for a flu pandemic.

Video analytics — software that watches security video so people don't have to — can alert authorities upon "seeing" several types of incidents. For example, analytics can catch someone trying to "tailgate" their way through an access point. If someone swipes a badge to properly gain entry, and someone else follows them in, the

system will know about it and can alert administrators. If a person leaves a bag outside a door and then walks away, video analytics can spot that too. It can also raise an alert if someone crosses the sidewalk outside the building at 3 a.m., for example.

There are numerous other kinds of sensors that can be linked into the network. Some of these sense light, radioactivity, heat and other changes in conditions.

Assess — Once an incident has been detected, the assessment phase becomes critical. Decision-makers need to determine the scope of the incident and decide on the actions needed in response. The more situational awareness they have, the better decisions they can make.

Command centers today can be much more effective than in the past. Data flows in and is displayed on monitors so decision-makers can grasp the entire situation quickly. Video can be displayed along with contextual information, and it can be complemented with views from any perspective and 3-D modeling. It works much better than trying to piece together data from disparate systems.

Much of the information can be displayed on maps. It's all about putting the information together in a meaningful way. Cisco and its partners allow safety officials to quickly understand a situation. Proper assessment helps dictate an

appropriate response. Officials don't want to send 50 vehicles to a false alarm.

Respond — Taking the proper response to a security event can be critical. Communication is often a key part of that response. Cisco's

CASE STUDY

Fewer Silos, Better Public Safety

The Sheriff's Office in Boulder County, Colo., wanted to foster better communication among agencies, while also improving productivity. It succeeded at both with the help of Cisco. The Sheriff's Office used the existing Cisco network infrastructure as the foundation for a new, IP-based communications system.

Cisco's IPICS was instrumental in providing better service for the Sheriff's Office. IPICS enabled the creation of virtual talk groups, which allow people on a number of different devices to participate in a discussion. Participants can use radio systems, IP phones, cell phones or PCs to connect with others.

The interoperable system also enabled better service and safety for the public, a safer environment for officers, and countywide collaboration. Boulder County is a mountainous region, making reception unpredictable with traditional radios. That's no longer a problem.

The flexibility that accompanies an IP-based solution will pay dividends for years to come. It's much more dynamic than the traditional land-mobile radio system. In fact, the Sheriff's Office sees much potential for even more interoperability and is planning several projects.



IP Interoperability and Collaboration System (IPICS) enables interoperable communications, so multiple jurisdictions can talk to each other no matter what type of equipment they have.

Unified communications, mobile messaging and wireless communication may all be needed in an emergency. Alerts and notifications must be sent. Cisco's Digital Media System (DMS) gives digital signage and mobile messaging capabilities for emergency notification. Cisco and its partners can help officials reach key people no matter where they are. Virtual talking groups can be created instantly, to get all the various responders on the same page.

Evaluate — Once an agency has gone through the five steps with an actual event, it should review the process. How did the process go? What could be done better next time? This after-action analysis allows an organization to fine-tune its five-step process and make it stronger. The process is never actually done. It's a continuum; it keeps going. It's always time to prepare for the next incident.

The Network Foundation

The continuum works when it's based on a secure, multiservice network. A solid network foundation lets responders and decision-makers do their best work. The end result is greater safety for government employees, students and the general public.

The network links in with quality-of-service, application optimization and other key elements. These and other enhancements allow the network to perform at the highest possible level. The network knows how to handle the different types of data coming over it and how to prioritize that data for optimum efficiency.

Cisco understands the importance of using the tools that are available. With its own expertise and that of its partners, Cisco helps governments and educational organizations across the country make the most of their current systems while stepping up to the next level — better safety and security for assets, employees, students and the public.



For more information call: **408-526-4000 or 800-553-6387**
www.cisco.com/go/govsafety