

Technologies Will Augment Personnel in Fighting Crime

Campus police at the University of Missouri-Kansas City employ an IT surveillance system as a force multiplier, enabling them to reduce crime.

Core Topic

Government: Public Policy

Key Issue

How will government policies affect personal use of technology?

Strategic Planning Assumption

University police agencies that invest in cost-effective dual-use technologies by combining environmental and surveillance remote monitoring of their critical infrastructure and physical threats will double by 2005 (0.8 probability).

Law enforcement agencies are required to control crime, maintain order and provide a multitude of services, from responding to 911 calls to preventing terrorism — all with limited resources. Agencies look to technology to enhance their effectiveness. Yet, technological advances are only useful if police agencies can afford them. This is the first in a series of *Research Notes* that will detail technologies designed to address specific problems in a more-effective manner, and provide guidance to law enforcement agencies as they decide which security technologies to consider.

The University of Missouri-Kansas City (UMKC), one of four campuses associated with the Missouri state university system, operates 41 buildings on 30 acres in an urban setting. The continuing theft of UMKC computer and audio-visual equipment by evening students and nonstudents resulted in an average monthly loss of \$1,000. Moreover, man-hours were increasingly devoted to insurance investigations. The executive director of information services (EDIS) and the campus security chief (CSC) were charged with investigating methods and technologies to protect campus property. Their task was compounded by a manpower problem: 25 campus officers for a student body of 15,000 — a student-to-officer ratio of 600-to-1. The U.S. average for four-year institutions is 250-to-1.

University deterrence efforts began with floor-bolted cables and increased patrols. These methods proved ineffective in a college environment. The EDIS and CSC investigated the applicability of closed-circuit television (CCTV) to monitor sites in real time using video cameras. A response could be dispatched immediately and an incident prevented or stopped. However, installation, storage, maintenance and physical difficulties in cabling cameras to a central recording mechanism made CCTV cost-prohibitive.

Gartner

© 2004 Gartner, Inc. and/or its Affiliates. All Rights Reserved. Reproduction of this publication in any form without prior written permission is forbidden. The information contained herein has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Gartner shall have no liability for errors, omissions or inadequacies in the information contained herein or for interpretations thereof. The reader assumes sole responsibility for the selection of these materials to achieve its intended results. The opinions expressed herein are subject to change without notice.

At the same time, UMKC began experiencing indoor climate fluctuations serious enough to damage equipment or short-circuit UMKC's network. This dual threat resulted in bridging the formerly disparate departments of campus security and IT. A mission-specific mentality among departments had traditionally resulted in using "stovepiped" resources to meet individual needs. The EDIS and CSC conducted monthly technology search meetings leveraging universitywide expertise. Attendees, accepting the EDIS' recommendation, agreed to deploy a technology capable of operating on a single, open platform connected to the existing LAN. According to the EDIS, these discussions "crumbled the wall erected between physical and IT security." UMKC became more interested in integrating video surveillance, active monitoring and alert notification capabilities for IT spaces and environments. The EDIS and CSC agreed that they wanted a centralized monitoring capability and a user-defined alert system with the ability to digitally write information to a server. After reviewing several IP surveillance companies, UMKC determined that the environmental-monitoring company NetBotz was the only vendor capable of fulfilling scope and cost requirements. UMKC scheduled NetBotz to perform several on-site demonstrations. These demonstrations deployed a NetBotz 500 monitor appliance — slightly larger than a normal laptop computer — a central processor, digital motion camera and sensor module. This appliance addresses and monitors each individual unit and can store data when not digitally writing it to a server. These modules contain built-in Universal Serial Bus (USB) ports for third-party sensors and are attachable to ceiling, wall or server racks. Sensor units are connected to a server via an Ethernet connection.

Problem: UMKC needed to surmount security obstacles to protect its technology investments from criminal theft and environmental damage by deploying a cost-effective solution that provided flexible monitoring capabilities without running different systems in conjunction with other university networks.

Objective: UMKC sought to deploy dual-use technology to monitor targeted classrooms, critical IT spaces and other environments to protect technology investments on a 24x7 basis.

Approach: Deployment began with the installation of 12 camera/sensor units connected to a centralized monitoring server, consolidating all information into an alert notification system via a user-defined channel — for example, PDA, e-mail or cellular phone. Each targeted room was fitted with two or three ceiling-mounted units requiring an installation time of less than one hour. The cameras were powered by a USB connection and calibrated for recording at two frames per second with a resolution of 640 x 480. UMKC began using 100MB Ethernet

LAN connections for all camera units. This configuration contained an appliance with a built-in, IP-addressable Web server that enabled authorized users to monitor the system via a Web browser. Cameras could be set for motion-activation-only mode to minimize bandwidth usage and data storage demands.

Within four months of installation, the cameras helped to stop three separate theft attempts totaling \$25,000 worth of audio-visual equipment. This success led UMKC to expand the system to 120 units. Police dispatchers use either the motion activation or look-see function for "monitored spaces." The EDIS and CSC use a remote login feature to "look at the campus" during regular and off hours. This set of "electronic eyes and ears" is a law enforcement force multiplier. The system notifies the EDIS, the CSC and the UMKC police dispatcher of the exact scene of a climate change, power interruption or disturbance. In cases of theft, UMKC police can copy images from the server to a CD-ROM drive that is used in identity confirmation by the university or other sources. The CSC claims that investigation-processing time for theft-of-property crimes has been reduced from seven days to 20 minutes.

Results: UMKC was able to gather information from various locations and communicate it over the existing IP infrastructure, providing the capability for asset protection and crime reduction. From a cost standpoint, this Web-based monitoring system cost the university less than \$100,000, which provided critical asset protection and freed campus police officers to cover larger areas and target specific locations. The EDIS calculated that a CCTV system would have cost \$500,000. The EDIS states the university recouped its investment in less than one year, based on the value of recovered stolen property, theft reductions or outright prevention.

Critical Success Factors/Lessons Learned:

Hard-Drive Disk Management: UMKC experienced several server failures due to data overloading. Think in terms of a wagon wheel with the server at the hub and the multitude of units comprising the spokes that constantly feed data until the hub is overloaded. UMKC began using 100MB of bandwidth. Generally, the maximum server capacity is 60 units. Additional units will require a second server. Otherwise, hard drive crashes occur with regularity and increasing server connections to 1Gb is advisable. Management policies should contain image compression requirements, target utilization of motion detection and storage limitations that do not exceed 14 days.

Cyberattacks: Employ IP-filtering software to harden the system against attacks by predetermining IP addresses to be received.

Environmental Factor: UMKC discovered that indoor florescent lighting fools the camera into recording continuously. As a result, electronic masking must be included in the units. These fixes should not cause a discernible drop in performance.

UMKC's system is an incremental step toward converging IT and physical security. However, the system is still susceptible to failure. NetBotz is working on a product line for disaster recovery using mirrored central servers that transmit data between one another. Redundancy must be incorporated into all service agreements. Such contingencies should be accounted for in system requirements.

Bottom Line: Governments at all levels worldwide continue to invest in large-scale video surveillance, with mixed results. However, smaller, clearly defined objectives and criteria have proved to be more successful. IT managers feeling more threatened by cyberattacks may overlook environmental-monitoring systems, but as a dual-purpose criminal deterrent and environmental/power disruption technology, it is worth closer scrutiny.

Acronym Key

CCTV	closed-circuit television
CSC	campus security chief
EDIS	executive director of information services
UMKC	University of Missouri- Kansas City
USB	Universal Serial Bus