SECURITY Beyond the Copper Wire

Physical threats are becoming a larger focus in IT security.

IT security is usually an inside job. Threats to the network come from within the virtual realm that technology makes possible. Firewalls, (antivirus, antispyware and antispam) filters and other security software, as well as best practices, procedures and user training, all help organizations fend off network-based attacks that threaten from within the copper wire.

But all these sophisticated tools won't keep an unauthorized stranger from copying a hard drive or stealing a notebook containing your organization's sensitive information.

Not all security threats involve someone trying to corrupt your network or steal something from you. Some threats occur without any malevolent intent. Network security software won't alert you to threats such as overheating, fire, smoke, water or unexpected motion. Nor will the software let you view video from these locations to help coordinate countermeasures against such threats.

Given these limitations, it's no wonder that IT security efforts are expanding to include protecting the physical security of IT facilities, equipment and public spaces.

Integrated Security

Until recently security responsibilities have usually been split, with the IT department securing the network and computer activity and the facilities department being responsible for premise surveillance, door access and other physical security functions. Each group would have separate networks and seperate security tools. But this split is rapidly disappearing.

"Up until now, there really hasn't been an integrated approach to overall organizational security," says Jack Gold, founder and president of J. Gold Associates, a strategic technology consulting firm located in Northboro, Mass. "Security had been done in 'islands.' Door-badge security didn't communicate to video surveillance, nor to laptop security."

Not so anymore. Network and physical security activities are rapidly converging. Part of the reason for this, explains Gold, is that more of the products used to provide physical security are based on computer and information technology.

"Five years ago, physical security was very simple. A lock was a lock, and you opened it with a key. Today, you have things like biometrics, keyboards, smart cards and radio-frequency identification. As physical security comes to rely more on computers, it all comes together, which means more involvement from the IT department."

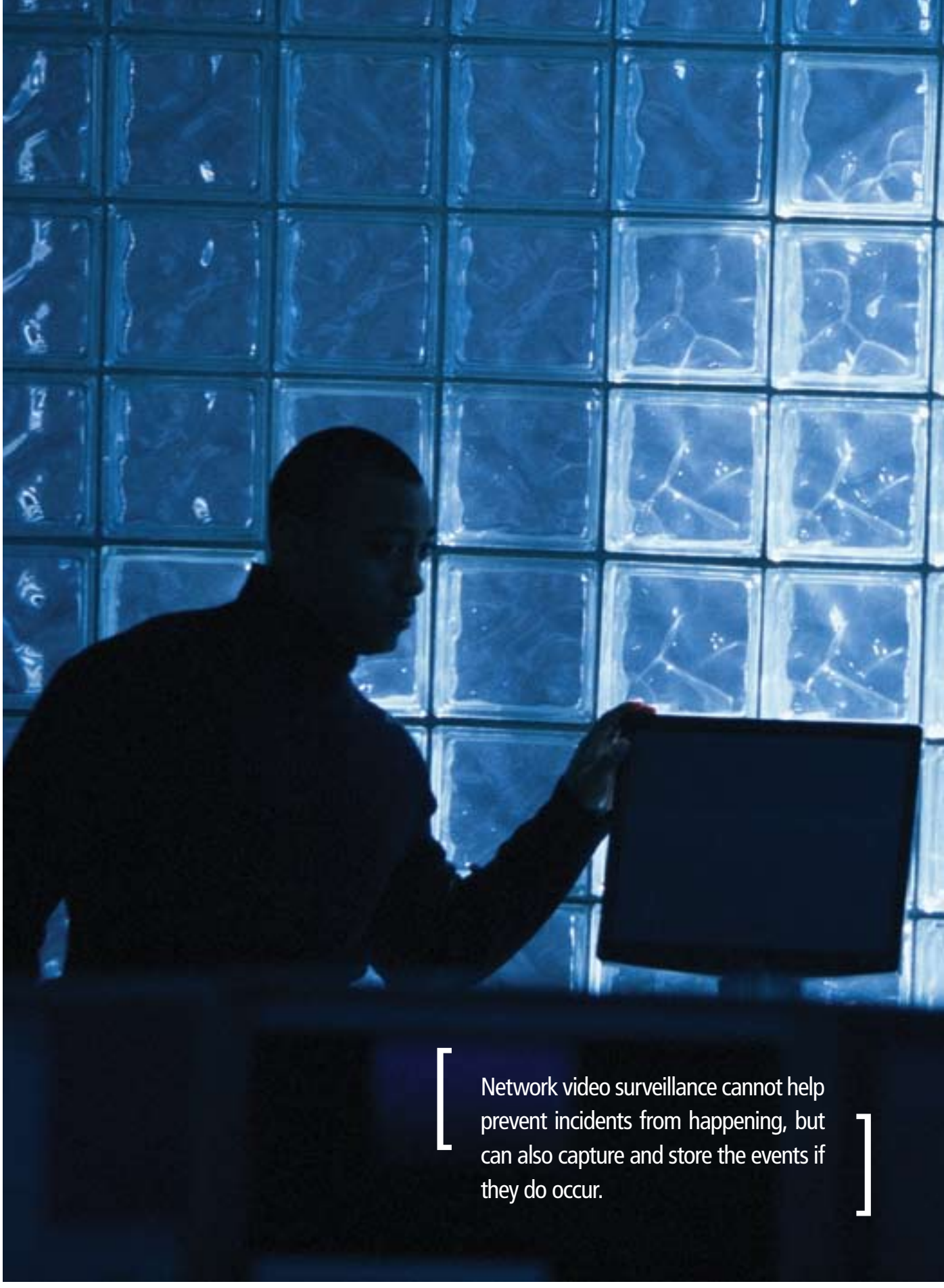
Securing Access to and Monitoring IT Environments

The IT department also benefits from this security convergence. "There's greater concern about things that affect availability beyond the copper wire, such as people, temperature, humidity, water leaks in the room and other environmental changes in the IT facility," notes Christian Cowan, product manager for APC's security and environmental group.

"We provide your eyes and ears with access to remote locations, including under the raised floor, inside the rack, in the plenum and other remote areas," explains Rick Camp, product manager for APC's NetBotz product lines.

"And APC has integrated the Rack Access locks with the NetBotz camera systems, so you can receive a NetBotz alert with the cardholder's name and ID, along with the video, and compare the image of the person who entered with the name to confirm that it's the same."

Network video surveillance isn't just for remote sites. APC's Camp adds, "They're good for places where IT can't be present all the time, like server rooms and wiring closets distributed across a campus, or wiring closets on each floor of a high-rise building. NetBotz can send IT alerts, even images, to their computer or PDAs, and the tech person can decide whether or not they need to be there."



Network video surveillance cannot help prevent incidents from happening, but can also capture and store the events if they do occur.

IP Video Makes Surveillance Simpler and More Powerful

Network-based IP video is integral to creating a broader web of security. "We see an opportunity for the network to play a critical role in enabling formerly isolated physical security systems in silos," says Steve Collen, director of product management for Cisco's converged secure infrastructure business unit.

"Now, you can connect video to when a badge or fingerprint is swiped, which provides an additional audit trail of who entered." This new integrated approach to security is also dependent on video analytics.

Collen explains, "Video analytics can identify images and determine whether a person is authorized to enter a particular zone, and do real-time alerting. For example, many schools are investing in video surveillance not just to see who's on campus after-hours, but also to look at behavior, and whether certain people are where they're supposed to be."

Cisco's Video Surveillance IP Gateway lets organizations connect analog closed-circuit television (CCTV) surveillance equipment to a digital network, giving them many of the benefits of IP video, such as more efficient storage.

Another helpful product is Cisco's Security Monitoring, Analysis and Response System (MARS), which provides security monitoring for network security devices and host applications made by Cisco and other providers.

"We've started to establish relationships with physical access control vendors for devices like badge readers," adds Bob Beliles, senior manager of physical security market management at Cisco. "The network can provide a platform for communications and connectivity for what used to be disparate systems. We see great opportunities for tying network and physical security together."

Network Cameras Are Cost Effective

Beyond the interconnection benefits, technologies like Wi-Fi, Power over Ethernet (PoE) and mesh networking are helping organizations make the cost-benefit case for IP video. "We're rolling out a new generation of network video cameras, and we're seeing a lot of interest in them from K-12 schools and city governments," reports Robert Muehlbauer, national channels manager for Axis Communications.

"The AXIS 212 PTZ Network Camera, for example, has a 140-degree lens and a 3-megapixel sensor, enabling one-click digital pan-tilt-zoom (PTZ). This means the camera has no moving parts, making it less expensive, and that it can be powered using PoE."

PoE allows lower power cameras to be installed without the need for AC circuits; mesh networking allows wireless-enabled cameras to create a wireless network infrastructure extending throughout a building or across a campus.

Identification at Your Fingertips

Along with IP video, biometric authentication is another technology that's changing the way that physical security is done. Biometric identification is a way to establish a person's identity through human physical and behavioral characteristics. The biometric ID method currently most in use is the fingerprint.

"There are two main types of fingerprint sensors, area readers and swipe readers," says David Michielli, marketing manager for computer input devices at Cherry Corporation, a producer of logical access products. "With area readers, you hold a finger down briefly. And with swipe readers, you swipe your finger across the scanner."

ASHE COUNTY CAMERAS AIMED AT PREVENTION

Ashe County is tucked inside the Blue Ridge Mountains of North Carolina. Like Middletown Schools, Ashe County recently switched to network cameras and is very happy with the results. "We've recently begun using IP video cameras for a variety of productivity and preventative security measures," reports Cyrus Hurley, director of information technology for the county.

"We've installed Axis IP video cameras, including one with PTZ capabilities, on the campus of our county buildings. We've also installed a number of cameras around state-owned and privately owned health facilities," says Hurley.

The cameras can be remotely selected, viewed, and with the PTZ camera, even controlled, by any authorized user over a network connection, including virtual private network (VPN) connections from home or notebook computers.

According to Hurley, in addition to monitoring to ensure physical security within the buildings, the cameras have improved worker productivity.

"We can also monitor employee work flow — verify that employees are doing their assigned tasks. At the Valley Nursing Center facility [in Taylorsville, N.C.], for example, work flow has increased by 5 to 30 percent because employees are more aware of the monitoring. We've eliminated a lot of downtime."

The Axis network cameras are also being used to monitor sensitive areas such as medical record file rooms and medicine supply rooms.

"We use the cameras to monitor who enters, logging date and time-stamped images. It's a preventative measure, letting us know who's been in the areas, and making people aware that we're capturing this activity," says Hurley.

"Swipes work great if you're going to use it on your desktop or laptop," says Michielli. "Area readers are better for workers who use it once a week or month — they're more obvious in how they read your fingerprint."

Cherry's fingerprint biometric reader hardware includes basic software that can handle several users on a single desktop, or it can operate through a server at the network level. As Michielli notes, "For larger deployments, organizations can use software like Imprivata's OneSign Single Sign On."

Secure KVM for Secure Access to Computers

A unique challenge to physical security is the end user that needs access to several different computers. In government agencies, for example, users may need access to computers operating at different classification levels (such as classified versus top secret), which means that they can't be interconnected.

Due to the different security levels, they cannot use a standard KVM (keyboard, video display and mouse) switch, so users must have a separate keyboard, display and mouse for access to each layer of security. The problem is that standard KVM

switches are not adequately secure. Standard KVM switches use a single processor to access all the channels that the computers connect to. Data can leak through to the point where it can be "sniffed" (eavesdropped on).

For organizations that want to avoid this kind of desktop clutter, Avocent offers its SwitchView SC KVM switching systems, in four- and eight-channel versions. "We use a separate I/O processor for each channel, so there's a secure channel for each port," says Pete Engler, product manager for Avocent Corporation. "There is 60db of separation between channels, making it impossible to transfer data between the connected computers."

Avocent's Engler continues, "These are the only KVMs with NIAP [National Information Assurance Partnership] approval, which is what all military and intelligence agencies require. Our switches are built to the specifications of the Protection Profile, which the switch has to adhere to in order to pass this approval."

Protecting Notebooks and Other Mobile/Portable Gear

IT security experts will tell you that notebooks present the most pernicious challenge to resolve in the physical security equation. A successful approach to securing an organization's notebooks will go a long way toward securing the network.

"We look at an organization's notebook computers as the gateway to the network. A stolen notebook potentially compromises not only the information on the notebook, but also the information and users on the network," says Roma Majumder, senior global security product manager, security, Kensington Computer Products Group.

Kensington provides customized solutions for education and government organizations, such as the MicroSaver Keyed notebook lock, says Majumder. "We can provide key options like a master key for IT, in case a user loses their key. And we can provide groups of locks controlled by a single key held by an administrator, or let users have access to any of a pool of secured devices."

IT Must Take on More Responsibility for Physical Security

As the collaboration between security and IT continues in the education and government sectors, IT professionals will be shouldering more of the security responsibilities. Consultant Jack Gold stresses, "Computer and network-based security means that your computers and networks have to be more secure than ever."

Gold continues, "When your computers can control your security cameras, or have information on how to get into your buildings, you can't lose them or their data. If somebody can hack into one of your computers, they can probably break into your building."

Axis's Muehlbauer also notes this growing IT presence in physical security. "In government agencies, the responsibility for security is often passed onto the IT staff. And in schools, we meet with the IT folks because they understand the benefits of IP-based cameras, and they understand the implications to their wireless and wired networks and storage."

It is clear that IT professionals are going to be spending more of their time in the future looking outside the copper wire for incoming security threats.

MIDDLETOWN SCHOOLS ZOOM IN ON NETWORK CAMERAS

The Enlarged City School District of Middletown in Orange County, N.Y., with 6900 students, is a newcomer to the realm of network-based security. The district recently installed 265 fixed and PTZ Axis Communications network cameras throughout its nine buildings. The cameras have been installed in public areas such as hallways, cafeterias and parking lots.

"We're hoping to prevent problematic events through awareness of being monitored and recorded, as well as capture incidents, and get that footage in a timely fashion," states Mike Tuttle, CTO for the district.

One feature of the network cameras that Middletown Schools really appreciate is the economy of digital storage. "We capture based on motion — when something enters a camera's field of view," explains Tuttle. "This saves a lot of storage space."

But that wasn't the only feature that won Middletown Schools over. Tuttle continues, "The combination of IP networking for the data connection and 802.3af PoE gave us more flexibility with the installs. By letting us deliver power to the cameras over the network cables, we avoided a lot of expense running electrical power cables, and had more options for where we could put cameras."

This network camera purchase conveniently dovetailed with another tech upgrade the district was making. Tuttle notes, "We were about to deploy Voice over IP. So we were able to leverage the network cabling we'd already installed, and the PoE capability in our LAN switches."