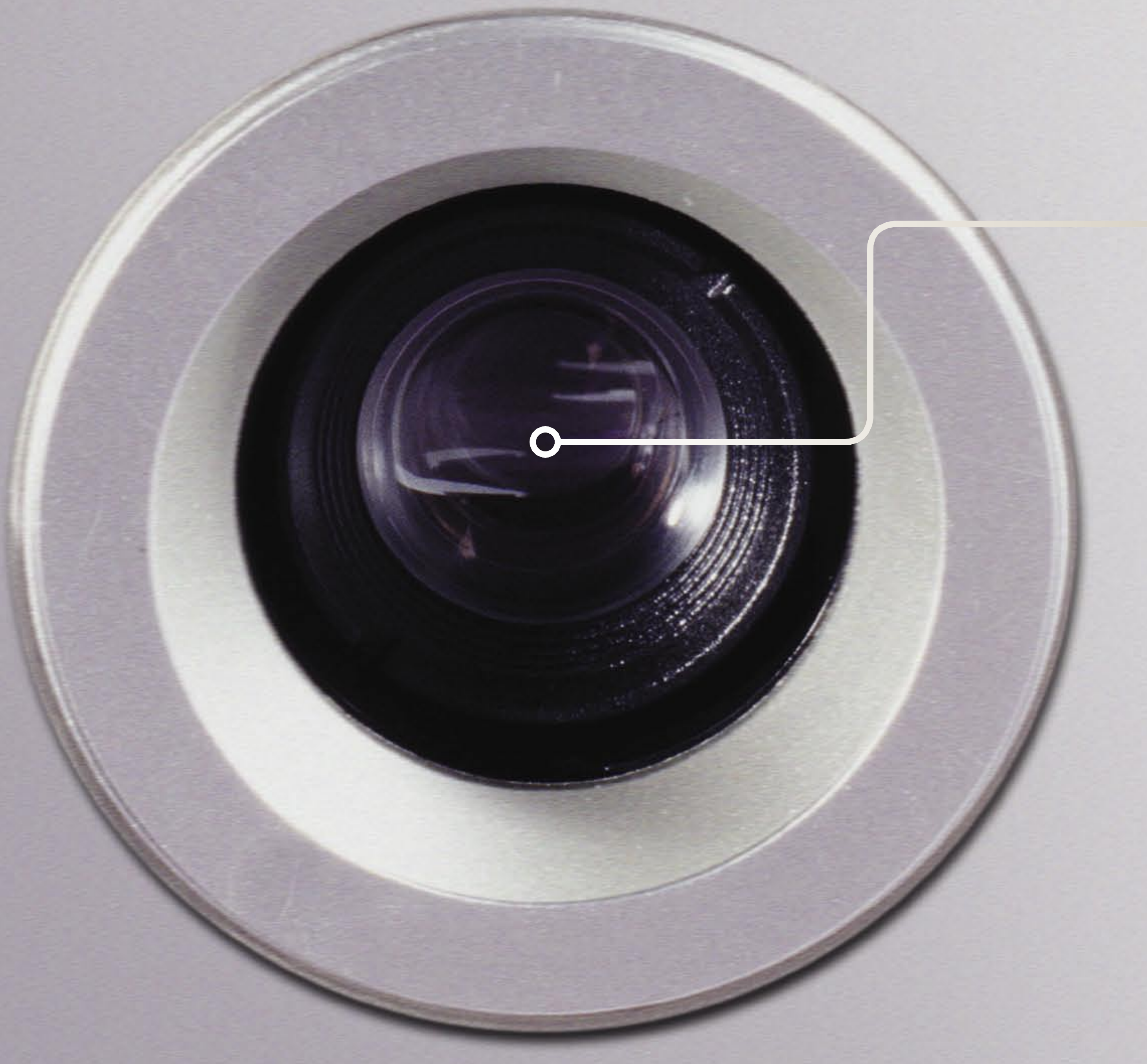
KEEPING



A CLOSE WATCH

Cameras, locks and other devices help ensure physical security for your site and its equipment

The physical security of your onsite IT equipment—and of notebooks, projectors and other gear that employees take out of the office—is as important as network and data security. Theft, fire, overheating or water damage are as much realities as computer viruses, spyware and network intrusions, and can be as or more disruptive to operations and your company's bottom line.

For example, even if data on stolen machines isn't abused, the financial impact of such losses can still be significant. California law SB 1386 mandates that any company that does business in the state must notify residents impacted by any security breach, while the Health Insurance Portability and Accountability Act (HIPAA) levies fines of up to a quarter of a million dollars for violation of physical security—a hefty price to pay for a small- to medium-sized business. Luckily, several cost-effective solutions are available.

IP Video Makes It Easier to Watch for Trouble

Surveillance is a key component of security. But you can't put a human watcher everywhere all the time—it's too expensive, often not possible and doesn't provide a record of what happened.

The solution is video monitoring. Video cameras allow companies to monitor activity and even traffic and weather conditions at doorways, elevators, shipping and receiving docks, reception areas, parking lots and more.

Until about a decade ago, video surveillance used closed-circuit television (CCTV) cameras, connecting to a central monitoring area via video coax cable to a central security center that held banks of monitor screens.

However, while the cameras were comparatively inexpensive, and the recorders easy to use, installing and integrating the cameras often cost more than the actual cameras, and the systems' flexibility was limited. In general, you either recorded continuously, or not at all. Also, searching could be time-consuming, and you had to be in the security center to view current images.

Digital video, using IP video (or "Internet") cameras, is changing all that. Unlike a Web cam, which needs to be plugged into a PC, an IP video camera includes an embedded CPU and Web server software, and can plug directly into your local area network (LAN). Cameras can cost anywhere from under $200 to $2000 each, depending on the features and environmental ruggedness you need. They work with the same Ethernet wired and wireless LANs and wide area network connections that data and Voice over Internet Protocol (VoIP) gear already use. They can be easily monitored from any location, even offsite, and images can be instantly forwarded to police or other organizations if necessary.

About 1.5 to 2 million video cameras have been installed annually in the United States over the past thirty years, according to Chris Chute, senior analyst, World Wide Digital Imaging Program, IDC. Because of the trend to greater security surveillance, coupled with these new monitoring technologies, "The overall market will grow about 7 percent on average over the next several years, to about 3.3 million new cameras per year," Chute predicts.

Fortunately for companies who already have CCTV cameras installed and want to migrate to digital video, they can preserve their camera investment. Converter boxes let CCTV video signals be digitized, allowing not only more efficient storage, but also application of video software features, such as motion detection.

More Flexible Surveillance

Having cameras in place is only part of the monitoring process—somebody has to be able to watch one or more views. Management software tools can add value to your solution; for example, Sony's RealShot Manager software lets your company manage multiple cameras from any workstation on the network. You can define what times you want video to be recorded or what events trigger recording. (Axis and NetBotz also offer management tools.)

Digitized video offers other advantages over traditional analog ▸

video. "Software lets you save images only when something happens, like detecting motion," says Robert Muehlbauer, national channel manager, Axis Communications Inc. "This makes it much easier to find things, for problem resolution."

Today's IP video cameras also let you control the size and frequency of output. "The video of an event doesn't cripple the network, but streaming video can," says Tom Goldman, general manager, NetBotz, a wholly owned subsidiary of APC. Since 30 frames per second of VGA output produces enough to fill a T1 line, the ability to minimize bandwidth consumption is important, especially for budget-conscious businesses monitoring remote sites. One way to reduce bandwidth is to set cameras to only transmit when changes are detected; some cameras also support saving their video to a local storage device, which can then be remotely accessed as needed.

> "Studies show that the number-one source [of network downtime] is due to people's actions...usually just something like mistakes in hooking up a cable. Video data lets you look back and see who was doing something around the time the failure occurred."

Two other technologies are helping drive the deployment of IP video cameras, namely Power over Ethernet (PoE) and wireless network connectivity.

Also known as 802.3af, PoE lets LAN cabling carry electric power in addition to network traffic. PoE can provide enough DC power—up to about 15 watts per wire—for low-power devices like wireless access points, RFID scanners, keyless entry systems, IP video cameras and smoke/fire detectors. PoE can significantly reduce the cost to install and maintain the cameras, and enable cameras to be placed in a wider range of places.

Wireless network connectivity makes it possible to install and remotely control IP video cameras in places where electric power is available but network cabling isn't, such as outside buildings, parking lots and campus areas.

Axis' Muehlbauer notes that IP video cameras can be used for more than just security purposes: "For example, a store could check on traffic during the day in relation to promotional sales."

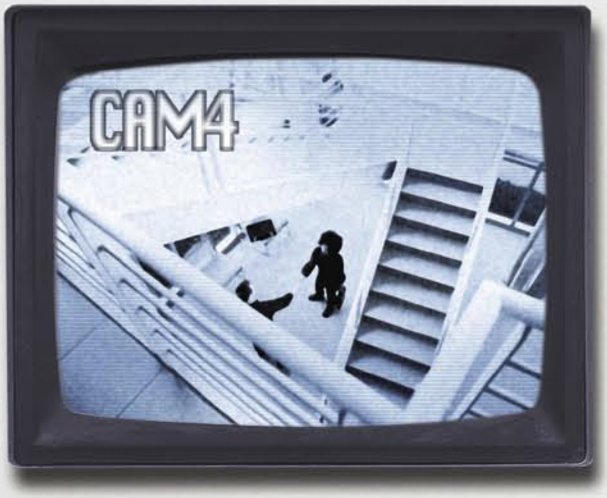
Video can also play an important role in reducing network downtime, adds NetBotz's Goldman. "Studies show that the number-one source is due to people's actions—usually not malicious, just something like mistakes or failures in hooking up a cable. Video data lets you look back and see who was doing something around the time the failure occurred. Previously, you had to go through a long checklist to figure out what had been changed."

Monitoring More Than Just Video

Many of today's digital video cameras include I/O ports in the back, allowing other sensor devices to be connected, monitored over the network, and trigger the camera to detect increased activity and start recording. Also, alternate solutions are available that can monitor different types of activity independent of an implemented video camera solution.

Avocent offers environmental monitoring products that monitor smoke, temperature, humidity and airflow. These sensors can be used to detect conditions too small for a site's HVAC department to detect, says C.C. Fridlin, director of product marketing, Avocent Corporation. "If you lose a fan bank on a power supply or a server, the heat in that rack can build to the point where a server fails; a room-level temperature monitor may never see this. So you have to watch the microclimates as well, for point problems you'd otherwise never know about until things start failing."

Temperature, according to Fridlin, is the big indicator of problems, although if you're using water cooling, you may



also want to include water detectors. "But simply putting a temperature monitor at the top of every rack is good enough for most," Fridlin says.

Third-party sensors can also monitor for hydrogen sulfite—an indicator of battery leakage—or carbon dioxide.

You may also want to monitor temperatures and other conditions, such as fan speeds, inside key servers and other devices. Intelligent Platform Management Interface (IPMI) features—included in nearly half the servers shipping in 2005—make it easy to do this. IPMI also lets you remotely power devices on and off without needing remote-control power strips.

"IPMI lets you look inside a box, determine the internal voltage, check the fans and fix it before the device goes down," says NetBotz's Goldman. "If you know that a router's internal fan has stopped working, for example, that means it's likely to overheat and shut down soon."

Another way to physically secure computers in an office setting is by putting them behind locked doors or even another location, and connect them to keyboards, mice and displays using KVM switches—for many, a much simpler and more cost-effective solution than buying thin-client boxes for each station.

This approach helps secure IT assets, and can also allow administrative access without physical access, according to Avocent's Fridlin. "You have a small appliance at the desk, and the machine can be under lock and control."

Keeping Equipment Safe In and Out of the Office

As computers and certain peripherals get increasingly portable, they become targets for theft. While data on these systems should be protected from misuse by encryption, making these systems theft-resistant is also important.

"Often, the device needs to be usable while locked, like computers used in garages, warehouses and places where contract employees are coming and going," says Michael Greco, director, U.S. product marketing, Targus International.

APC, Kensington, PC Guardian, Targus and others offer a range of locks and alarms, which fit into security slots or, in some cases, devices' video ports to help secure equipment.

"If you try to rip out a video port lock, you'll damage the motherboard, which can render the notebook unusable," says Targus' Greco.

Insurance payout is another reason to use locks. "Many insurance companies now won't cover theft from your vehicle if the computer wasn't physically locked down," says Richard Harris, vice president of sales at PC Guardian.

For IT departments, Targus offers "serialized" versions of its combination lock products, on which the combinations are preset, and can be checked online on Targus' secure site. "This avoids the need for IT to keep track of combinations or have to cut locks if the user forgets the combination," says Greco. "And there's no need to issue keys."

Notebook vendors including IBM and Sony now offer fingerprint readers built into some of their notebooks, replacing external fingerprint readers. These biometric add-ins can be set to lock other people out of specific files or folders, or from any use of the notebook.

Carrying cases have also evolved to provide extra protection for portable equipment and particularly for LCD screens.

However, experts stress that locks and other measures are no substitute for vigilance. "All these products are merely deterrents, to make a would-be thief go to the next, less-locked-down computer," says PC Guardian's Harris.