



Monitoring the Computer Room's Physical Environment

A white paper from Sensaphone, Inc.

SENSAPHONE[®]
REMOTE MONITORING SOLUTIONS

Introduction

Nearly all small- and medium-sized businesses rely on a computer network to maintain operations, communicate with staff and conduct other day-to-day activities to keep the business running. Housed in small isolated rooms, or even closets, the computer network is actually the lifeblood of a business.

Each of those rooms presents an environment where a lot can go wrong — and things often do. Servers crash. Fires damage equipment. Air conditioning systems fail. Intruders sabotage systems. Water pipes break. The possibilities are endless. These scenarios will wreak havoc far beyond a computer room and the equipment. A malfunctioning computer room affects productivity, nerves and, most importantly, a company's bottom line. Regardless of its cause, and an organization's response, unexpected downtime impacts both profits and reputation.

The economic loss due to unplanned downtime reaches substantial amounts when factoring in lost productivity, new equipment requirements, repairs, installation time and other associated costs. Estimates place the cost anywhere from \$30,000 to more than \$6 million per hour depending on the industry involved and the depth of the disrupted operation. For example, a brokerage firm may face a greater impact than a manufacturing facility.

Clearly, small business owners and IT managers are aware of such dangers and stay informed on the most up-to-date methods for protecting their equipment and data. However, many overlook a relatively inexpensive yet effective way to monitor their computer room's physical environment. They can actually proactively track and

monitor physical conditions that impact equipment operation the most — temperature, power, humidity and more — as part of an organization's overall security plan.

This paper addresses the greatest environmental threats to the functionality of small to medium computer rooms and presents the time and cost savings associated with the integration of a [remote monitoring system](#), limiting the impact of service interruptions organization-wide.

Threats to the physical environment

Spyware detection, antivirus software and firewalls are familiar solutions that protect a computer network from unwanted technical intrusion. As technology progresses, such software will become even more effective at protecting data integrity by blocking access to hackers, disgruntled employees and anyone else with the potential to inflict damage.

Outside of the virtual world, in a computer room's physical environment, conditions like excessive heat, fire, smoke, water damage, physical intrusion, high humidity levels and more can snarl a network's effectiveness for days or weeks at a time. Compromising conditions within the walls of a small computer room ripple across an organization's operations on a global level. Luckily, the application of an advanced remote monitoring system provides IT professionals with the ability to track environmental conditions and respond to small changes before they have the opportunity to alter network activity.

Left unchecked, excessive heat can quickly bring a fully functional computer room to a screeching halt. Whether in a rack system or standalone unit, each server, monitor and other piece of equipment create heat. As servers become more

powerful, their heat output increases as well. The trend of bundling servers adds further strain to an already stressed environment.

The average PC uses about 300-400 watts of electricity, converting nearly all of it into heat. Depending on the room size and the number of PC and server units, internal temperature can rise rapidly. Excessive heat can begin to damage a unit's internal mechanisms. At first, heat can cause a unit to slow down. If left unchecked, this can ultimately lead to destruction and loss of data, and consequently, downtime. Each rising degree in temperature significantly increases the probability of a server crash.

To combat the heat, computer room operators, particularly in small- to medium-sized companies, typically rely on the building's air conditioning system to maintain safe temperatures. In those scenarios, if a problem with the AC unit is detected, it can already be too late to undo the damage to computer room equipment.

Luckily, more and more IT stewards are realizing that their computer rooms require more protection than a single, building-based air conditioning unit offers. Instead, they are moving toward the installation of dedicated AC units with ample backup, and for obvious reasons. Should the building's AC system fail, the dedicated unit would maintain the room temperature, protecting vital data and equipment. Conversely, the building's main air conditioning system could serve as a short-term backup should the dedicated AC unit fail. It's not an ideal solution, but it does allow managers time to seek solutions that are more permanent.

Today's corporate landscape is littered with companies that have experienced such a computer room nightmare — a failed cooling unit — and the resulting equipment damage and unpredicted downtime.

Turner Studios in Atlanta, Ga., serves as a [prime example](#). The facility houses production for live broadcasts of NBA games, Atlanta Braves baseball games, the weekly TV segment “Dinner & a Movie” and more. Turner Studios also houses facilities and resources for all of the Turner Entertainment Networks worldwide.

Early one morning, an air cooling unit failed in a critical room containing complex, expensive and vital computer-graphics equipment used for daily operations. A remote monitoring system allowed the studio to avoid a full equipment failure. The system alerted a broadcast engineer to the temperature change before it caused problems. Had the rising temperature gone undetected for even a few hours, Turner Studios would have needed to spend hundreds of thousands of dollars to replace the damaged equipment and return to production.

The computer room atmosphere is vulnerable. Local weather, human error and even rodents can be enough to alter environmental conditions in the room. Those sources can lead to power interruptions, humidity, fire and smoke, water, unwanted intrusion and more. Many of these factors are uncontrollable and simply unavoidable.

Controlling the Uncontrollable

What computer room operators *can* control is the severity of any particular incident. A remote monitoring system, when installed and used correctly in a computer room environment, can quickly detect subtle changes in conditions and alert appropriate personnel. Individuals can then assess the situation and act accordingly, many times with the opportunity to be proactive.

In more advanced remote monitoring systems, software programs enable built-in responses to certain conditions, allowing IT managers to shut down equipment when pre-programmed thresholds are crossed. Monitoring systems also allow access to

critical computer room operations through remote locations. With the proper monitoring system and Internet access, IT personnel can manage responses to alerts from anywhere and protect their valued resources.

Placement of computer room monitoring sensors is another extremely important element of a successful monitoring program. Sensor placement goes a long way in maximizing the effectiveness of a monitoring system's ability to protect sensitive equipment. A temperature sensor located within an individual rack system, for example, will accurately monitor the temperature within that rack. What it does not monitor is the room temperature itself. If multiple servers, PCs and racks are used, it is imperative that managers place additional temperature sensors around the room, adding additional layers of protection.

Another example is the proper placement of a water sensor. Water on the floor can damage computer equipment beyond repair along with the room's floors, walls, carpeting, etc. Inappropriate placement of a water sensor, even just several inches above the floor, would prevent it from doing its job. It would take the largest of floods to trigger an alarm, and by then, it would be much too late.

Another factor controllable by IT managers is their response time. When done properly, alarm thresholds are set well below levels that may cause damage to the computer equipment. Still, IT managers must avoid the trap of feeling too secure when an alarm does sound. Diligence is required when responding to alarms, whether remotely via the Internet or in person. In order to minimize damage, speed is key.

Choosing the right remote monitoring system

Identifying the appropriate monitoring system will depend on the specific requirements of a computer room. Here are a few factors to consider when selecting a remote monitor:

Inputs

How many inputs do you need? Each different condition you wish to monitor (e.g., temperature, power, humidity, water on the floor, etc.) requires its own input. Look at the number of inputs available on the remote monitoring system under consideration. Be sure to factor in any future requirements of computer room or network growth, equipment upgrades and more. Consider staff changes, too. If cuts are planned, a remote monitoring system could help soften the impact. Plan ahead by selecting a model with more inputs than needed, or select a model with the capability for future expansion.

Notification

Available alert notifications may appear to vary little from one remote monitoring system to the next, but there are subtle differences. Consider the reach of the communications. Will you be notified regardless of your location? Additionally, multiple communication interfaces, including Ethernet and standard telephone interface, guarantee early notification before a problem turns into a disaster. Relying on email notification alone may not be advisable if your network has already shut down. Consider options in addition to email, like voice or pager.

Status Checks

Can't stop thinking about your network? High-end remote monitoring systems give you on-demand access to your infrastructure, either via the Web or through phone updates. The status of all monitored environmental conditions is at your fingertips.

Data Logging

Sometimes data history can prove valuable in identifying patterns and trends in environmental conditions. Advanced monitoring systems allow users to access saved data for graphical, database and auditing purposes. Analyzing data samples may lend insight to larger issues, preventing problems before they arise. One example is the logging of temperature trends. If the room's temperature fluctuates little, there are likely no issues. However, if the temperature logs show slow, steady increases, it could be a sign that the unit is having trouble keeping up with demand. Regardless of the reason, once it is brought to attention, a problem can and needs to be checked.

Intangibles

Other things to consider when deploying a remote monitoring system for a small- or medium-sized computer room include:

Scalability. Can the system grow to meet your needs without breaking the bank?

Installation. Is it plug-and-play for quick install or are vendor technicians required, which drives up costs?

Peripherals. Be sure to determine which sensor accessories are included with the initial purchase and ask about their design. Are they provided by a third party or were they designed specifically for the remote monitor under consideration? Is there a variety of accessories available to meet different monitoring conditions? The answer can go a long way in reducing future headaches.

Monthly Fees: Committing to a remote monitoring unit is a simple step compared to becoming involved with a vendor long-term. Even highly advanced monitoring systems are available free of monthly fees. Unless IT professionals need a service to

monitor them while they monitor their own equipment, a hassle-free purchase with no strings attached may be their best option.

Return on investment. For any manager spending money, clearly establishing a return on that investment is a “must” when reporting to superiors. When considering a remote monitor, determine the value of the equipment that needs protection and how much the organization is willing to pay for that security. It is also important to revisit this part of your management plan on a regular basis. As equipment needs change, so too does the ROI. That is simply because a remote monitoring system will often outlive a network server. If you have no need to upgrade the monitoring system, then the ROI just went up.

Protecting Profits

In today’s world, protecting a computer network is synonymous with protecting profits. With so many environmental threats and security dangers, *not* monitoring a computer room is taking an unnecessary risk, and too much is at stake. The right monitoring system will work with your organization to prevent data disasters and let you focus your efforts on the task at hand — doing business.

About the author: Bob Douglass is the vice president of sales and marketing for Sensaphone, Inc., manufacturer of the complete line of Sensaphone remote monitoring systems. For more information, visit www.Sensaphone.com or call 610-558-2700.