Six Environmental Concerns Every Data Center Needs To Monitor

Put A System In Place That Can Help You Track, Regulate & Address Critical Areas

When it comes to properly monitoring your data center environment, "if you don't monitor or measure it, it will not improve," says Jeanne Ziobro, senior product manager, DCIM, at Raritan (732/764-8886; www.raritandcim.com). Before you can measure or monitor a system or process, you need to know what is important to monitor in your facility. Some of the following tips and advice may seem run of the mill, but they should serve as a reminder about how to maintain your mission-critical equipment and anticipate problems that arise during operation.

Monitor: The Premises

Paying attention to minor changes that happen to the environment and equipment in a data center is paramount, but security and room surveillance are just as important. Jeanne Ziobro, senior product manager, DCIM, at Raritan (732/764-8886; www.raritandcim.com), says using security cameras and/or door locks on cabinets will prevent unauthorized access to equipment. In addition, Ken Koty, sales engineer at PDU Cables (866/631-4238; www.pducables.com), says it's important to have video surveillance, and the doors accessing the server room should have some form of card reading access to record who and when someone is entering different areas of the data center.

Monitor: Temperature & Humidity

Temperature fluctuations are one of the primary variables that environmental monitoring systems should observe. Notably, there is a cause and effect scenario that's important to pay attention to.

"As the temperature increases, computer equipment begins to experience performance problems and, when unaddressed, will eventually lead to shutdown, failure, and equipment damage," says Ken Koty, sales engineer at PDU Cables (866/631-4238; www.pducables.com). "Know your average or typical temperatures throughout the data center. Know where the hot spots are and monitor them. If not addressed, these will be the first areas to experience equipment shutdown."

Similarly, Ziobro says it's critical to maintain proper cooling to prevent overheating of IT equipment and "to monitor your thermal envelope to prevent overcooling and energy waste and avoid hot spots."

Koty also says that tolerating a high humidity degree puts you at risk of condensation and water collection that can create possible shorts in sensitive electrical equipment, which can eventually lead to equipment failure and damage.

Monitor: Power Systems & UPS Battery Rooms

Michael Sigourney, president of AVTECH (888/220-6700; www.avtech.com), says

that in addition to temperature changes, power can impact efficiency and reliability more than most other threats that have to be addressed.

Pay attention to what Koty calls "power anomalies" such as sags and spikes that can foreshadow any future power-related issues. "Power consumption (PUE) utility feeds and all critical components such as UPS systems and diesel generators and diesel fuel levels in storage tanks should be monitored," he says. "For UPS battery rooms, a battery monitoring system should be in place that not only monitors "each string of batteries as a whole, but also each individual battery," says Koty.

Monitor: Airflow/Cooling & Obvious Hazards

Proper airflow and air quality monitoring are key to ensuring your systems don't get overheated, which means you can expect temperature monitoring to overlap with these two environmental considerations. According to Koty, monitoring of airflow and cooling systems should be viewed as an early warning system for high temperatures in a data center. "Higher temps within the cooling systems or decreased airflow would suggest cooling problems that, if not addressed, will lead to higher temps on the data center floor," he adds.

Water, smoke, and fire are other basic environmental threats that can wreak havoc on your data center, so it's wise to prepare by installing water sensors to identify leakage and other water problems and smoke detection systems to suppress a fire that could break out and cause catastrophic damage before you realize it.

Monitor: By Using The Right Software

You need to have accessible and trustworthy monitoring applications to know that your measurements and readings are reliable.

"The monitoring interface is something people seldom talk about, and it's becoming critical as teams grow and work from disbursed locations," says Sigourney. "Having powerful software, whether on the network or in the cloud, allows managers access when they want it and with the data trending and tools they need to make valid decisions and respond from anywhere."

Practically speaking, Sigourney says this interface should have sensors (whether built-in or external), and it will typically be responsible for the electronics, network connection, data logging, alerting, and more.

More than anything, taking the next step forward in implementing an environmental monitoring system is the right step. Remember that everything doesn't have to operate flawlessly from the beginning; it just needs to have the basic monitoring components so you're not surprised by any environmental changes.

"Get a solution in place today and build on it over time. Do not wait for the perfect plan or until a disaster occurs. Experts say that one in three facilities will go down more than twice a year for four hours or more. Protect your facility now from the unexpected by proactively monitoring. Don't wait until it is too late and it costs you time, money, and business," Sigourney says.

Monitor: For Everything Else

Tanja Lewit, CEO of Kentix Innovative Security (844/536-8492; www.kentix.com), says when you're examining the environment and physical monitoring, the reality is that a lot of things can happen, and the things that do happen are not the types of events you would expect. "It's the unanticipated human error: the food or beverage spill; the dropped toner cartridge because you thought the data center was a good place for a copier; the accidental power shutoff because your server room is packed; the security blunder that happens because you don't have an easy solution for revoking access control in place," she says. "That's why you need an environmental monitoring tool that monitors continuously, watches for events you determine are outside of normal, and alerts you immediately and easily so you can react."

BONUS TIPS:

Whatever You Do, Plan

Procrastination and ignorance can ultimately put your data center at risk, especially if you delay the purchase and implementation of environmental monitoring equipment. Michael Sigourney, president of AVTECH (888/220-6700; www.avtech.com), says each quarter organizations need to invest some extra budget dollars into monitoring products in the same way you would invest in an insurance policy. "Most of the time, when environmental monitoring products warn of a pending threat, they recover their investment in minutes. Basically, a manager should analyze, seek advice, plan, and implement. Once a plan is in place, test the plan periodically. Don't wait for a disaster. Be proactive and plan, test, and modify as requirements change," he advises.

Consider DCIM

Combining environmental monitoring with a data center infrastructure management (DCIM) solution can help you maximize what your alert systems can do in terms of prevention. Jeanne Ziobro, senior product manager, DCIM, at Raritan (732/764-8886; www.raritandcim.com), says a DCIM solution along with environmental sensors "can inform managers of a water leak within the data center and allow them to send in the appropriate personnel to avoid a problem before mission-critical IT equipment is harmed." Furthermore, this dual-system approach can help managers make decisions about air circulation and warn them of unauthorized entrance into the data center.