ITWatchDogs

512.257.1462
www.itwatchdogs.com
sales@itwatchdogs.com

How to Protect Your Data Center from Environmental Threats

Introduction: Physical Dangers Just as Important as Cyber-Threats

Viruses, spyware, and network threats get most of the attention, but environmental factors like heat, humidity, airflow, smoke, and electricity can be equally devastating to server room equipment, and thus to a company's IT operations.

To get a sense of the danger, let's take overheating as an example. Servers generate high levels of heat, and the facility must be kept cool to ensure optimal performance. The warmer it gets, the more likely equipment will overheat and malfunction. In fact, an increase from 68°F (20°C) to 86°F (30°C) can reduce the long-term reliability of electronic equipment by as much as 50 percent.[1] And when air conditioning fails, temperature can skyrocket in a matter of minutes. In February 2009, Duke University Professor of Physics Robert G. Brown explained that heat weakens electronic components like power supplies, motherboards, and memory chips, so even if they don't fail immediately, they become more susceptible to failure over time. [2]

"The one time our server room overheated drastically, reaching 85° to 95°F (30-35°C) for an extended period of time…we had node crashes galore, and a string of hardware failures over the next three months—some immediate and obviously due to overheating, some a week later, two weeks later, four weeks later," Brown writes.

In this white paper, we'll discuss the danger that environmental threats post to server room equipment, outline a comprehensive environmental monitoring strategy, and explain how environmental monitoring products from ITWatchDogs deliver an end-to-end solution for prevention and early detection of environmental issues.

No Company Is Immune

Depending on the size of a company and its industry, downtime can cost tens of thousands of dollars per hour. For example, if your Web site is down and visitors choose a competitor, you've lost both the immediate transaction and the opportunity for their repeat business. If the outage causes your company to break a service-level agreement with a customer, the associated fees and potential lost business add up quickly.

Every server room and data center—even those of household-name companies and sites—is vulnerable to environmental damage. In March 2010, Wikipedia suffered a two-hour outage when one of its server clusters—located in a European data center—overheated. The company was able to reroute traffic to a North American data center, but a glitch in its DNS server tools caused Wikipedia address resolutions to fail globally.[3] Think about how many users were frustrated by this outage. According to 2008 statistics, Wikipedia receives between 25,000 and 60,000 page requests per second.[4] Multiplied by 2 hours, that's at least 180 million failed requests due to overheated servers.

Lost business aside, you must also consider the cost of replacing expensive servers. In September of 2007, an overheating condition at St James Hospital in Leeds destroyed £1 million worth of server equipment.[5] The negative publicity surrounding the incident also impacted the facility's credibility and public image.

Can your operation afford a large-scale server failure?

What's clear is that companies of every size must protect their IT investments from environmental threats like overheating, power outages, and excessive moisture—all of which may result from flooding, condensation, leaks, or malfunctioning/poorly configured air-conditioners.

Smoke conditions can also lead to serious equipment damage, in case alarms are triggered during off hours and personnel aren't available to remediate or respond quickly. If a smoke alarm triggers an 'emergency power off' (EPO) device, for example, cooling systems could go offline and leave servers susceptible to overheating.

[1] http://www.bicsi.org/pdf/winter_2010/Jeff_Miller.pdfs

[2] http://www.openxtra.co.uk/articles/skimp-server-room-ac

[3] http://www.pcmag.com/article2/0,2817,2361778,00.asp#

[4] http://www.nedworks.org/~mark/reqstats//reqstats-monthly.png

[5] http://www.theregister.co.uk/2007/09/27/leeds_server_overheat

Environmental Monitoring Is the Key

In a typical server room, a wall-mounted thermostat measures room temperature and controls the air conditioning. Individual servers now come with built-in temperature sensors that issue alerts if the level of heat surrounding the individual unit rises above a certain threshold, or if an internal fan breaks down. Isn't that enough to ensure safe operating temperatures?

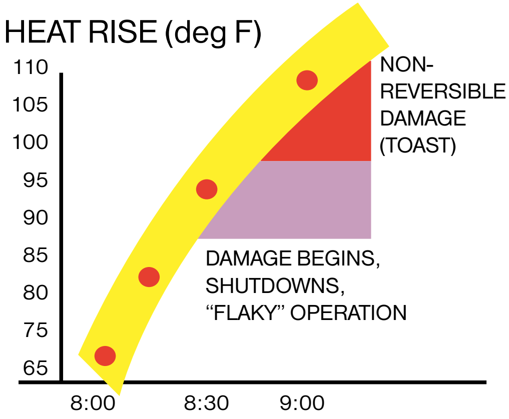
The short answer is, no. Data center temperatures vary widely from one zone to another. Even if the overall room temperature is 68°F (20°C), the area near the output vents may be 5 degrees cooler, and the area behind server nodes may be 5-10 degrees warmer. Airflow problems could create higher-temperature pockets of still air in some aisles, creating hot spots that can damage sensitive components.

A better approach involves temperature/humidity/airflow sensors installed on or near individual racks and critical devices. Logging and graphing these measurements over time can help administrators spot trends, such as temperature spikes during peak operating hours or fluctuations when the building's HVAC systems are throttled back on weekends.

With comprehensive monitoring in place, if an internal fan breaks or an air conditioning unit fails, the spike in operating temperature will be noticed quickly. Probes with internal microprocessors are easy to configure and highly reliable. Similar sensors can track humidity and moisture in the air and the floor, and measure the temperature and rate of air flowing along different paths in the server aisles.

Even sound sensors can help in the early detection and remediation of component failures. For example, a fan that is wearing out may get louder over time, which could be spotted at an early stage on a device that graphs relative measurements. A properly calibrated sensor would send out alerts for either condition and help IT staff resolve the issue rapidly.

The benefit of microprocessor-based sensors is that they can be monitored via Web browser, without requiring proprietary software installations. With a Web-enabled monitoring system, you can measure temperature, humidity, airflow, water leaks, power, door/cabinet position and more, setting alert thresholds and escalation schemes in case an anomaly is detected.



As time elapses and heat rises, sensitive IT equipment begins to show signs of damage.

Optimal sensor equipment can send alerts in numerous formats, including SNMP (Simple Network Management Protocol) traps for integration with network monitoring software, e-mail messages to pertinent staff, text messages (as an added layer of protection if an admin is away from his or her computer), and even voice calls via a relay-controlled auto-dialer.

Best Practices for Optimal Monitoring

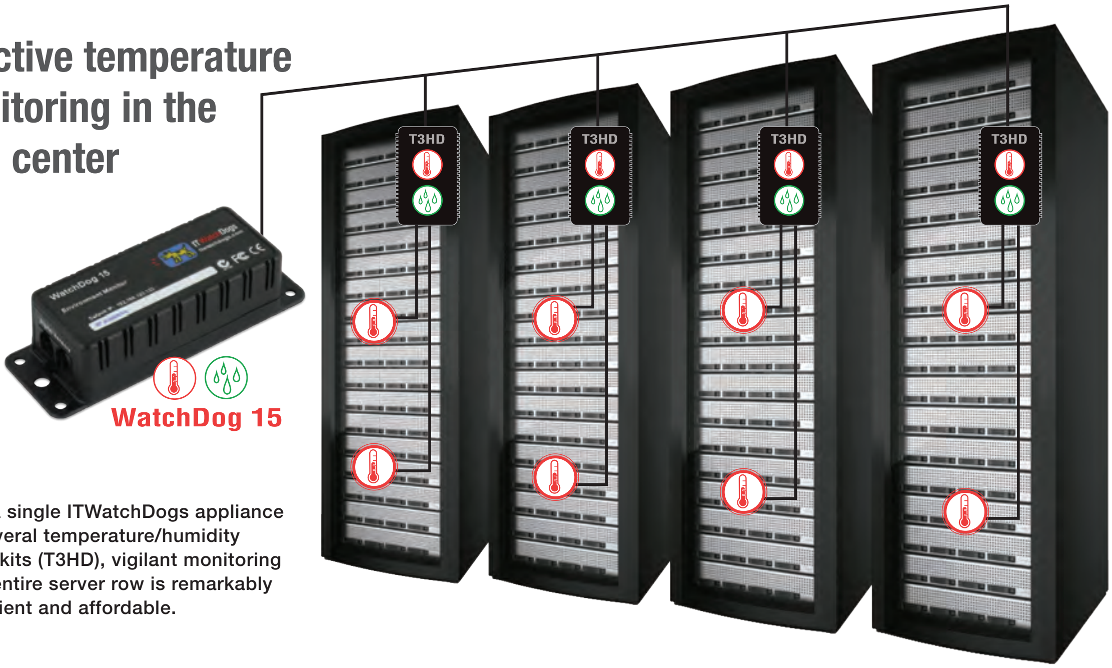
Heat: An optimal environmental monitoring strategy includes multiple temperature sensors. These should be placed on top, middle, and bottom of individual racks to measure the heat being generated by equipment, and at the air conditioning system's intake and discharge vents, to measure efficiency. Probes should also be placed around critical devices, because the temperature inside a rack-mounted device could be as much as 20 degrees higher than the surrounding area. A probe near the room's thermostat can help monitor what the thermostat is 'seeing' as it controls the air conditioner.

You can also use a hand-held thermometer to determine where the hottest spots are in the server room, and then set up sensors in those areas to get an 'early warning' when temperatures rise.

Once these sensors are in place and being monitored centrally from a browser, emergency alert policies should be set up to ensure that the right personnel are informed of potential problems.

Remediation procedures should also be mapped out ahead of time. Service contracts with an air-conditioning repair company ensure rapid response, and you should make sure the company offers 24-hour service.

Effective temperature monitoring in the data center



Using a single ITWatchDogs appliance and several temperature/humidity sensor kits (T3HD), vigilant monitoring for an entire server row is remarkably convenient and affordable.

The logs that track temperature over time are also helpful, in that IT managers can review them over a weekly or monthly span and analyze them for spikes that occur during off hours. In addition, testing the sensors every month is an important step to making sure the system will function properly when an event does occur.

Water: Moisture and humidity sensors should monitor for leaks inside cooling equipment, potential leaks that come from nearby pipes, or water caused by a flood or disaster. Water sensors should be placed at the lowest point (wherever water would tend to puddle) on the floor, and underneath any pipe junctions. Air-conditioning condensation trays should also be equipped with sensors to detect overflow.

Power: Electrical failures can cause air-conditioning equipment to shut down even while an uninterruptible power supply (UPS) ensures that servers stay up and running—a sure recipe for overheating a server room in short order. The best approach is to monitor current coming into the data center, and arrange for an orderly shutdown of IT equipment in case power is knocked out. The hour or two of downtime is far preferable to the widespread device failures that would result from an overheating condition.

Smoke: Smoke alarms can trigger power shutdowns. Also, they're usually not tied to an alerting system that contacts IT personnel. Alarms may be noticed by facilities managers—or the local fire department—but the maintenance of sensitive server equipment is not their top priority. Here, the best approach is to wire the smoke alarms directly into the climate monitoring and alerting system, essentially extending the functionality of the climate sensors to the smoke alarm.

Doors: A final concern for data center monitoring is unauthorized entry. Dry-contact sensors that detect the opening and closing of a door should be installed at the room entry points and on the doors of server and UPS cabinets. On a busy day, these sensors can send alerts numerous times and present a time-consuming irritation, but managers can configure alerts to account for weekday vs. weekend operations, work hours vs. overnights, and other factors to help reduce the number of alerts sent and pinpoint unusual activities.

IP cameras are another fairly easy component to add to a monitoring solution. They provide real-time surveillance of sensitive areas in the data center and tie into the Web-based console, so administrators can get a first-hand look at the environment wherever they may be.

The ITWatchDogs Solution

When you're considering an environmental monitoring solution for your data center, ITWatchDogs provides a comprehensive portfolio of sensors and appliances.

The ITWatchDogs family of monitoring devices provides remote monitoring of environmental parameters in data centers and server rooms. They track temperature, humidity, leaks, power supplies, door position and more. ITWatchDogs' wide variety of models and options fit different requirements and room sizes, but all are based on standard hardware and software and monitored via a Web browser.

The environmental units are designed to take up very little space; the largest models are 1U high rack-mount units, the smallest is only 4 inches long by 1.5 inches wide and deep. Models with built-in Power over Ethernet (POE) capability are available.

All the products have a wide range of on-board sensors; most models allow 16 or more remote sensors to be connected as well.

All ITWatchDogs' climate monitors have a built-in Web server that automatically generates sensor data logs and graphs, without any need for external software. All management and monitoring tools are accessible securely via Ethernet or the Internet. The monitors have SNMP agent software to integrate with popular networking management tools, and they support SNMP v1, v2c, and v3. Some models include low-voltage relay outputs that can be used to activate a strobe light, an alarm, a backup air conditioning unit, or an auto-dialer. ITWatchDogs offers highly reliable auto-dialer devices for both GSM and analog phone systems, with independent backup-power batteries that allow them to make phone calls to your IT and service personnel even in the event of a power failure.

What to Look For in an Environmental Monitoring Solution

A solid environmental protection solution should include sensors that are easily deployed throughout the data center, connected to a monitor with a built-in Web server for easy access and communication. It should also deliver:

- Secure, browser-based access
- Comprehensive logs and graphical analyses of environmental factors over time
- Multiple account levels, to ensure that IT staffers or clients see only what they're authorized to see
- Multi-level alarm policies with escalation, so admins can set alert thresholds and contact lists for prompt response
- Multiple notification media, including e-mail, SMS text message, SNMP alerts, and telephone auto-dialer.

Requirements aside, the solution should not charge subscription fees for tech support and software updates. A long-term data center management and monitoring solution is critical to preserving your IT investment, but it should not generate recurring expenses that degrade ROI.

Lastly, ITWatchDogs stands behind its products, with firmware updates available free on its Web site and technical support available free for life. Support is provided by the same engineers that designed and engineered the devices themselves, so questions and problems are resolved quickly and authoritatively.

Conclusion

Data center equipment is very sensitive and susceptible to environmental damage from excessive heat, moisture, and unauthorized access. Power outages that knock out cooling systems can lead to overheated servers in a matter of minutes.

Simple thermostats and server-based temperature sensors aren't enough to ensure comprehensive protection. IT organizations need temperature and water sensors throughout the data center and at specific strategic locations near potential trouble spots. They also need door sensors and IP cameras to alert administrators in case of unauthorized entry and provide real-time views of the space. They also need comprehensive management tools to tie the data from these sensors together into a cohesive display, and to set alarm parameters in case a threshold is exceeded.

ITWatchDogs provides a full line of environmental sensors that deliver exceptional protection and alerting functions without requiring any proprietary software installations or update subscriptions. Regardless of your data center's size or complexity, ITWatchDogs has a cost-effective monitor and sensor solution that will reduce risk and enable smoother IT operations for your company.

To learn more about ITWatchDogs
and its line of monitors and sensors, visit
www.ITWatchDogs.com