Environmental Threats and Their Costs

The most common environmental threats to server rooms are temperature, humidity, water leaks, human error, intrusion, vibration, and power outage. Many of these threats, such as temperature and humidity, are related, which complicates environment monitoring and heightens the need for an automated, sophisticated system.

Temperature

Temperature is the main environmental threat to computer hardware. The generally accepted, ideal temperature is between 68 and 74 degrees Fahrenheit (20 to 24 degrees Celsius).

Excessive heat degrades network performance and causes downtime. As the temperature increases, a heat sinks fan works harder to cool the central processing unit (CPU). Continuous overworking causes the fan to fail, leading to a machine overheating. A machine shuts down when it reaches an unsafe temperature in order to prevent permanent damage. An administrator must then be located, day or night, go to the machine, and reboot it after it has cooled. Consequently, services hosted by a down machine are unavailable until it is restarted, which can take minutes or hours. If the server hosts critical services (e.g., e-commerce, user validation, email) that are not distributed to backup servers, revenues can be lost, users cannot login, and communications are interrupted. If the shut down is not done properly, data can be lost.

Excessive heat and rapid temperature changes also damage equipment. Rapid temperature increases can increase humidity, while rapid drops can cause water in humid air to condense on equipment. Together, heat and moisture accelerate the break down of materials used in microchips, motherboards, and hard drives, which is called premature aging. In worst cases, a machine won't shut down when the temperature exceeds safe levels, and circuits are damaged. Ultimately, heat-damaged equipment must be replaced, increasing the cost of network maintenance.

Controlling temperature is becoming more important and more difficult because of changes in equipment design and greater use of network services. New equipment runs hotter because it runs faster and does more work. Also, more circuits are placed closer and closer together, trapping heat in a smaller space. Smaller equipment also means that more equipment can be placed in the same space, usually packed tighter together. The increase in density of equipment causes a rise in the amount of heat dissipating in a rack cabinet. Increased network usage also increases heat, so as usage levels change during the day, so does the temperature and the need for cooling. For networks that operate near capacity 24 hours a day, every day of the year, there is little, if any, time for machines to cool down.

Humidity

When the temperature is between 68 and 74 degrees Fahrenheit (20 to 24 degrees Celsius), the relative humidity (i.e., the amount of water in the air) should be between 40% and 50%.

A high humidity level can produce the following problems in the server room:

- Condensation -- Condensation occurs when humidity levels are too high or when there is a rapid temperature drop. Water that condensates inside equipment causes rust, short circuits, or deposits of dirt and minerals that corrode equipment. Moisture absorbing circuit boards expand and contract with changes in relative humidity levels. Expansion and contraction of these boards can break microelectronic circuits and edge connectors. Finally, condensation increases heat levels. Deposits of dirt and minerals act like insulation that traps heat in equipment and prevents it from diffusing into the air.
- Fungus -- Persistent humidity levels above 60% and elevated temperatures promote the growth of fungi. These contaminate the air with dirt and spores, which clog a machine's airflow and promote heat retention and condensation. They also retain moisture and promote corrosion, which damage circuits and motherboards. Some fungi "eat" textile plastics (e.g., polyester) and PVCs, a phenomenon in which fungi breakdown the material used in these items. Most electronic equipment has some PVC materials, such as the PVC insulation used in cabling.

A persistent low humidity level can produce the following problems:

- ESD -- Electrostatic discharge (ESD) occurs in dry environments because there is not enough water to neutralize the charge buildup. ESD intermittently interferes with hardware and can cause system damage or temporary malfunctions.

- Plastic Breakdown -- Some plastics breakdown in low humidity environments, which is another form of premature aging.

Water Leaks

Proper planning moves equipment away from water pipes that might burst, basements that might flood, or roofs that might leak. However, there are other water leaks that are more difficult to recognize and detect. Blocked ventilation systems can cause condensation if warm, moist air is not removed quickly. If vents are located above or behind machines, condensation can form small puddles that no one sees. Standalone air conditioners are especially vulnerable to water leaks if condensation is not properly removed. Even small amounts of water near air intakes raise humidity levels and fill servers with moisture.

In addition, water from small pipe leaks can travel for long distances behind walls and continue for a long time before anyone notices it. Server rooms with raised floors are particularly vulnerable. All of the cables and wires for an entire network are concealed beneath floor panels. While this approach keeps cords safe from being accidentally unplugged, it makes monitoring their physical status difficult. Cables may be soaking in water for a long period before anyone notices. This situation breaks down insulation, and the loss of insulation causes signal leakage and performance degradation.

Human Error

Administrators/personnel can unknowingly create environment problems in server rooms by:

- Adjusting the heat or air conditioning while working in the server room and forgetting to reset it when they leave
- Placing boxes in front of vents "temporarily" and forgetting to move them, which blocks airflow
- Moving equipment, which changes the room's airflow and causes hotspots
- Bumping equipment, which changes the direction of vent baffles and causes the exhaust of one machine to blow at the intake of another machine
- Installing new equipment, unaware that it creates more heat than the old equipment
- Failing to put blank panels behind empty rack shelves, which inhibits air from flowing up.

Similarly, cleaning crews sometimes close doors that should be left open for ventilation, thus increasing the temperature and reducing airflow.

Intrusion

Intruders, such as disgruntled employees and industrial spies, often strike at the most critical yet vulnerable points: the physical devices that store and control access to data. The small and delicate nature of modern computing equipment makes it easy to damage or steal; hard drives are compact enough to carry out in a briefcase, backpack, coat pocket, or purse.

Less sinister, but just as potentially harmful, are animal intrusions. Rodents, insects, birds and even larger animals have found their way into highly sensitive areas to wreak havoc upon equipment. Tiny contaminants, such as fur, dust, and dander, can cause component failure. Mice and rats chew through cable.

Vibration

Too much movement loosens connections within the server housing unseating boards and chips. Vibration can also damage the hard drive disk, which rotates at extremely high speeds. Being bumped or moved can cause the platter, where the information is stored, and the head, which reads the information, to physically connect, causing scratches that permanently harm the disk drive.

Generally, vibration comes from mundane sources: being too close to halls or walkways, or being moved or bumped. Good space planning can keep shocks to a minimum, but IT staff should still monitor the situation. Some vibrations, such as those generated by a failing air conditioner, actually serve as warnings. Most machines vibrate more as performance worsens, so tracking fluctuations in equipment vibration becomes an important means to predicting failures.

Power Outage

Power outages, “brown outs,” and voltage dips and spikes represent big problems for computing equipment. A simple hiccup in power levels, let alone a lightning strike, can cause servers to fail. In best-case scenarios, this costs precious time before rebooting. In worst-case scenarios, circuitry is irreparably damaged and must be replaced.

Weaknesses of Current Monitoring Practices

In a typical business, three groups monitor the environment: network administrators, security personnel, and facility maintenance employees. Network administrators often rely on a single thermometer and subjective notions about "comfort" to control the temperature of server rooms and data centers. In addition, security personnel and facility maintenance departments monitor areas outside of the server rooms. These three groups usually attempt to coordinate their efforts, but they maintain separate systems and practices. Ultimately, network administrators are primarily responsible for protecting hardware.

This approach has the following weaknesses:

- Not recognizing all threats - Damage caused by the environment can be subtle, unseen, or attributed to other causes. Accelerated equipment aging due to heat or condensation occurs over years and is often written off as a natural process (i.e., "equipment just wears out"). Condensation, rust, and heat damage is usually hidden inside machines, out of administrators' sight.
- Inconsistency - Administrators check room thermometers only when the environment feels hot or cold to them. Unfortunately, the sense of a "comfortable" temperature and humidity level varies from person to person, so problems are not always recognized.
- Gaps in monitoring - Environment threats occur 24 hours a day, seven days a week. But administrators are not always in the equipment room, especially on nights and weekends. Depending on staffing levels and schedules, server room environments can be unmonitored up to seventy percent of the time during an average week.
- Responsibility gaps - Another gap occurs because of shared responsibility. Water leaks and intrusion are monitored by maintenance personnel, security officers, and network administration. Frequently, one group will not monitor an area because it thinks another group already controls that area. Or one group will detect an incident but fail to inform all of the other groups. Consequently, vulnerabilities develop and potential problems are never investigated until it is too late.
- Inability to track environmental changes - Temperature and humidity levels constantly increase and decrease. Without a log of conditions, administrators cannot identify problems caused by these changes. Often, these problems continue for days or months, while time and money is wasted investigating false causes and solutions.
- Focus on catastrophes, not daily problems - Current practices avoid catastrophes, such as broken water pipes or power outages that shut down air conditioning systems. But they do little to protect from threats that slowly damage hardware or promote preventative maintenance, such as detecting gradual temperature increases that indicate a need to clean fans or air filters.

An effective server environment monitoring system addresses the weaknesses in the current practice of having personnel monitor the environment.