

DISASTER RECOVERY

JOURNAL

The Journal Dedicated to Business Continuity Since 1987

Contamination: The Undetected Disaster

By Mark Sher

FIRE...this word strikes fear into the minds of Disaster Recovery/Contingency Planners--why?

Most risk reduction/management planners perceive fire as a major threat the ongoing transmittal of electrons through microchips and integrated Binary-code circuits, the basis for all operating systems. A fire could also melt tape and/or disk media where all critical information is stored.

The perception of fire as a major threat is real to many. The cause of most fires, however, may be more of a surprise--particulate and gaseous contamination, in addition to being the major cause of equipment failure in data centers around the world, is also the leading cause of fires in the computer room. According to the N.F.P.A. (National Fire Protection Agency), the majority of computer room fires start internally inside of equipment. From this statement, one could draw several hypotheses:

1. Hardware manufacturers make inferior quality electrical components that frequently fail and catch fire.
2. The power supply to the hardware is of such poor quality spikes, surges, etc. that the equipment ignites.
3. The equipment is starved for air-flow (dirty filters restricting proper cooling) or actual arching (short-circuiting) of circuitry (IC and PC boards).

Taking into account the stringent reliability tests hardware manufacturers have in place as well as the vast amounts of money spent by end users for switch gear, UPS, and line power conditioners, the only plausible hypothesis is number three.

Yet, contamination is almost always the hidden, overlooked factor when developing the Disaster Prevention plan, which is arguably the most important facet of contingency planning.

The majority of risk reduction strategies are based on what the reasonable individual perceives as threatening. The disasters that have the greatest perception of danger, such as fire, earthquakes, chemical spills, hurricanes, floods, etc., are generally the most visible threats that come to mind. Many MIS professionals do not perceive the danger in contamination, especially for those cases in which it is not visible to the naked eye. This lack of awareness accounts for laser printers, bursters/collators, and other contaminant-producing devices still being installed ten feet away from CPUs, DASD, and switch gear.

Even though the United States Government has seen fit to write Federal Standard 209/A-D to regulate, measure, and educate Federal employees on contamination and its detrimental effects in various types of environments, little has been done to educate MIS professionals about the harmful consequences of contamination in Electronic Data Processing environments.

While most hardware vendors acknowledge the problems caused by contamination and spell out per-emptive measures to take in Hardware/Machine Installation Planning Guides, the implementation of these measures is left up to the end user or sometimes a General contractor with little or no data processing knowledge. Hardware vendors are placed in a curious situation in that their goal is to sell as many units as possible. If vendor A tells a client that my hardware requires a dust free environment, vendor B typically will say that my hardware is made to run in a business environment and does not require a special dust-free environment. This real-life scenario is the reason that contamination requirements are not prerequisites for hardware installation. When the question does arise, it typically is put on the back burner until it is too late and a fire or costly downtime has occurred.

There is a plethora of information, articles, studies (some scientific, some not) concerning contamination; however, it is disjointed and does not appear to be relevant unless an expert is deciphering the sometimes cryptic messages in the documentation. One of the best sources for this type of information is ASHRAE (American Society of Heating, Refrigeration and Air Conditioning Engineers).

SOURCES AND IMPACT OF CONTAMINATION

Airborne contaminants harmful to sensitive electronic devices can be introduced into the operating environment in many ways. Improperly sealed concrete slabs supply a continuous source of extremely abrasive cement (crystalline) particulate; loose or rocking floor tiles as well as improperly maintained air handling equipment (A/C compressors) generate metallic (ferrous) particulate; printers of all types (laser printers being the main culprit) generate contaminants; outside air produces hydrocarbons; and combustion engines and manufacturing processes also exacerbate the environment. Data center personnel contribute to contamination as well from hair, lint on clothing, and contaminants tracked in on footwear. Other sources may be more unusual, such as the maintenance personnel at a major bank that dumped sawdust underneath the raised floor to absorb moisture, originating from air handler condensation.

The correlation between contamination and disaster or hardware failure is left up to conjecture for the most part. Therefore, environmental contamination, the cause for more revenues lost through downtime than all other man-made and natural disasters combined, is often purposefully overlooked due to cost-cutting or by lack of knowledge.

IC and/or PC board malfunctions

Fine particulate acquires an electronic charge as it is pushed through the air handlers in the data center environment. This results in particulate seeking out oppositely charged surfaces (circuit boards) to electromagnetically plate over. Since particulate--even paper dust--becomes conductive when exposed to a moist environment (RH in data environments ranges from 45%-72%) or when heated to a liquid state, the result of contamination can be short circuits (IC or PC board failure). The best-case scenario is a momentary outage--but if a power control board were to take a hit, the amount of data

lost and/or processing time lost could be disastrous.

Data Loss

Another indication of particulate or gaseous contamination is a pattern of I/O (tape) errors or disk read/write errors. In older (removable media) disk drives, these problems may result from a buildup of contamination on the media itself that interferes with the reading of the disk by a read/write head. In the newer fixed and sealed disk drives, contamination may not permeate the absolute filters on the drive housing, but clog them instead. This may cause the internal operating temperatures to rise, resulting in platter warping or warble. If not corrected, the end result of both of these situations is the crashing of the disk drive. This phenomenon is aptly compared to a Boeing 747 flying three feet off the ground at full throttle suddenly encountering a tree, house, or boulder. Mass destruction is guaranteed in both scenarios--a catastrophic wreck of the jet, and a severe loss of data, up to 21GB, for the disk drive.

Loss of data due to contamination is a disaster that can be easily averted once the threat is realized. Unfortunately, the MIS managers and Disaster Recovery Contingency Planning staff very rarely perceive the threat of particulate and/or gaseous contamination--something they cannot even see--until a disastrous or costly event occurs. Many people are starting to realize the importance of creating browned out or blacked out CPU and/or DASD rooms. What is driving this "new" concept in Data Center design? It could be that the people who build and design microchips and integrated circuits, because they know that contamination has a detrimental effect on this type of technology, are telling the salespeople in the computer industry that it is crucial to maintain a clean environment to guarantee the longevity of your equipment.

WHAT TO DO

The time to access the level of contamination in your data or critical electronic environment is now. Waiting for a fire or costly loss of data or processing time is not sound proactive planning.

Evaluating your environment can be done in several different ways, from the white glove, a petri dish, or scientifically using state-of-the-art monitoring equipment. The best way to get an accurate assessment on the condition of the environment is to have tests conducted by having experts who are cognizant of the direct cause and effect relationship between contamination and the different types of hardware failures.

Be wary when choosing a company to perform an environmental assessment for your organization. It is critical to compare the services requested item by item. Many end users find out the hard way that what they thought they were purchasing is not what they end up receiving. Take the following scenarios:

- * One contractor used a buffing machine and/or wax or a ROTO wash (water injection) type of machine to recondition floor tiles even though every tile manufacturer explicitly states never to use this type of equipment on laminated tile surfaces.

- * Another end user was surprised to find temporary laborers performing delicate decontamination procedures in their shop, despite being told previously that trained technicians would be performing the service. (NORMAL TYPE) To avoid this situation, ask for a list of technicians 30 days prior to the commencement of work.

- * A company that purchased air filtration equipment discovered that the technology utilized by the product was harmful to electronic environments.

* A data/technical cleaning company was hired to perform an encapsulation of the cement slab in an on-line data center and sealed all of the cables to the concrete.

All of the above cases have happened to many uneducated end-users. There is no industry standard to ensure the competence of an environmental maintenance company. Planners should listen carefully to the descriptions offered by the vendors about how they approach contamination control, reduction, and elimination. One should also ask why certain steps are being taken during the process and seek a hardware manufacturer and/or a prior client, recommendations. Above all, be very careful of the vendor who simply states that "we do what they do for less."

Environmental contamination is not perceived to be as dangerous as a hurricane or earthquake, but it can result in the same dollar loss of processing time. This very moment, the problem may be building from a momentary glitch to a periodic annoyance and, ultimately, to an unplanned, costly shutdown to critical information systems. Although contaminants are too small to see, the potential damaging consequences to your organization are too big to ignore.

Mark Sher is President of CCI Technologies, an Environmental Engineering company, with several offices throughout the U.S. He has contributed to a number of articles and spoken at a variety of educational forums.

This article adapted from Vol. 4 No. 1, p. 50.

[*DR World Main Index*](#) / [*Return to DRJ's Homepage*](#)

Disaster Recovery World □ 1999, and Disaster Recovery Journal □ 1999, are copyrighted by Systems Support, Inc. All rights reserved. Reproduction in whole or part is prohibited without the express written permission from Systems Support, Inc.