Managing the Exposures and Efficiencies of a Physical Data Center

By Harris Kern's Enterprise Computing Institute

In the IT environment of today with virtual storage, virtual processors, and virtual networks, there is still the reality of managing the physical data center.

Major Physical Exposures Common to a Data Center

Most operations managers do a reasonable job at keeping their data centers up and running. Many shops go for years without a experiencing a major outage specifically caused by the physical environment. But the infrequent nature of these types of outages can often lull managers into a false sense of security and lead them to overlook the risks to which they may be exposed. Below are listed 15 of the most common of these.

1. Physical wiring diagrams out of date
2. Logical equipment configuration diagrams and schematics out of date
3. Infrequent testing of UPS
4. Failure to recharge UPS batteries
5. Failure to test generator and fuel levels
6. Lack of preventive maintenance on air conditioning equipment
7. Announciator system not tested
8. Fire suppression system not recharged
9. Emergency power-off system not tested
10. Emergency power-off system not documented
11. Infrequent testing of backup generator system
12. Equipment not properly anchored
13. Evacuation procedures not clearly documented
14. Circumvention of physical security procedures
15. Lack of effective training to appropriate personnel

The older the data center, the greater these exposures become. We have had clients who collectively have experienced at least half of these exposures during the past three years. Many of their data centers were less than 10 years old.

Preventative maintenance, testing, inspections, or any combination of these should occur once a year at a minimum. We have worked with some shops that have annual maintenance contracts in place for their physical facilities, including onsite inspections, but choose not to exercise them. Untested safeguards, un-inspected equipment, undocumented procedures and untrained staff are all invitations to disaster that are preventable.

A Word About Outsourcing

Outsourcing can cause another, non-physical type of exposure to a data center. Shops that outsource portions of their infrastructure services—co-location of servers is an example—often feel that the responsibility for the facilities management process is also outsourced and no longer of their concern. While outsourcers have direct responsibilities for providing stable physical environments, the client has an indirect responsibility to ensure this will occur. During the evaluation of bids and in contract negotiations, appropriate infrastructure personnel should ask the same types of questions about the outsourcer's physical environment that they would if it were their own computer center.

Tips to Improve the Efficiency of a Data Center

In addition to ensuring a stabile physical environment, data center managers have another responsibility that is sometimes overlooked. This involves ensuring efficiencies are designed into the management of their computer facility. The following are seven helpful tips to improve the efficiency of a data center.

1. Utilize well-designed physical layouts

A stable and reliable operating environment will result in an effective data center. Well-planned physical layouts will result in an efficient one. Analyzing the physical steps that operators take to load and unload printers, to relocate tapes, to monitor consoles, and to perform other routine physical tasks can result in a well-designed floor plan that minimizes time and motion and maximizes efficiency.

2. Factor future expansions into current floor plans

One other point to consider in this regard is the likelihood of expansion. Physical computer centers, not unlike IT itself, are an ever changing entity. Factoring in future expansion due to capacity upgrades, possible mergers, or departmental reorganizations can assist in keeping current floor plans efficient in the future.

3. Consider video cameras for security

Video cameras have been around for a long time to enhance and streamline physical security, but their condition is occasionally overlooked. Cameras must be checked periodically to make sure that the recording and playback mechanism is in good shape and that the tape is of sufficient quality to ensure reasonably good playback.

4. Analyze environmental monitoring reports

Environmental recording device also must be checked periodically. Many of these devices are quite sophisticated; they collect a wealth of data about temperature, humidity, purity of air, hazardous vapors, and other environmental measurements. The data is only as valuable as the effort expended to analyze it for trends, patterns, and relationships. A reasonably thorough analysis should be done on this type of data quarterly.

5. Inspect and maintain water and fire detection systems

In our experience, most shops do a good job of periodically testing their backup electrical systems such as UPS, batteries, generators, and power distribution units (PDUs), but not such a good job on fire detection and suppression systems. This is partly due to the huge capital investment companies make into their electrical backup systems — managers want to ensure a good return on such a sizable outlay of cash. Maintenance contracts for these systems frequently include inspection and testing, at least at the outset.

However, this is seldom the case with fire detection and suppression systems. Infrastructure personnel need to be proactive in this regard by insisting on regularly scheduled inspection and maintenance of these systems, as well as up-to-date evacuation plans.

6. Remove all tripping hazards

One of the simplest actions to take to improve a computer center's physical environment is to remove all tripping hazards. While this sounds simple and straightforward, it is often neglected in favor of equipment moves, hardware upgrades, network expansions, general construction, and—one of the most common of all—temporary cabling that ends up being semi-permanent. This is not only unsightly and inefficient; it can be outright dangerous as physical injuries become a real possibility. Operators and other occupants of the computer center should be trained and authorized to keep the environment efficient, orderly, and safe.

7. Ensure staff is prepared for natural disasters

The final tip is to make sure the staff is trained on preparedness for natural disasters such as floods, tornadoes, floods, hurricanes and earthquakes, particularly in geographic areas most prone to these types of disasters. Common practices such as anchoring equipment, latching cabinets, and properly storing materials should be verified by qualified individuals several times per year. Procedures involving evacuation routes, holding areas, and communication mechanisms should all be well understood and tested.

These seven tips are simple to apply and beneficial to use. When combined with the elimination of many of a data center's common exposures, it can make enhancing the efficiency of your facility a virtual reality.