Facilities Management

By Harris Kern

This article discusses the major elements associated with managing the physical environment of an infrastructure.

Major Elements of Facilities Management

If we were to ask typical infrastructure managers to name the major elements of facilities management, they would likely mention common items such as air conditioning, electrical power and perhaps fire suppression. Some may also mention smoke detection, uninterruptible power supplies (UPS) and controlled physical access. Few of them would likely include less common entities such as electrical grounding, vault protection and static electricity, among others. Figure 1 shows a comprehensive list of the major elements of facilities management.

Figure 1 Major Elements of Facilities Management

1. Air conditioning
2. Humidity
3. Electrical power
4. Static electricity
5. Electrical grounding
6. Uninterruptible Power Supply (UPS)
7. Backup UPS batteries
8. Backup generator
9. Water detection
10. Smoke detection
11. Fire suppression
12. Facility monitoring with alarms
13. Earthquake safeguards
14. Safety training
15. Supplier management
16. Controlled physical access
17. Protected vaults
18. Physical location
19. Classified environment

Temperature and humidity levels should be monitored constantly, either electronically or with recording charts, and reviewed once each shift to detect any unusual trends. Electrical power includes continuous supply at the proper voltage, current, phasing and the conditioning of the power. Conditioning purifies the quality of the electricity for greater reliability. It involves filtering out stray magnetic fields that can induce unwanted inductance, doing the same to stray electric fields that can generate unwanted capacitance, and providing surge suppression to prevent voltage spikes. Static electricity affecting the operation of sensitive equipment can build up in conductive materials such as carpeting, clothing, draperies and other non-insulating fibers. Anti-static devices can be installed to minimize this condition. Proper grounding is required to eliminate outages, and potential human injury, due to short circuits. Another element sometimes overlooked is whether UPS batteries are kept fully charged.

Water and smoke detection are common environmental guards in today's data centers as is fire suppression mechanisms. Facility monitoring systems and their alarms should visible and audible enough to be seen and heard from most any area in the computer room and when noisy equipment such as printers are running at their loudest. Equipment should be anchored and secured to withstand moderate earthquakes. Large mainframes decades ago used to be safely anchored, in part, by the massive plumbing for water-cooled processors and by the huge bus and tag cables, which interconnected the various units. In today's era of fiber optic cables, air-cooled processors and smaller boxes designed for non-raised flooring, this built-in anchoring of equipment is no longer as prevalent.

Emergency preparedness for earthquakes and other natural or man-made disasters should be a basic part of general safety training for all personnel working inside a data center. They should be knowledgeable on emergency powering off, evacuation procedures, first-aid assistance and emergency telephone number. Managing data center suppliers in these matters is also recommended.

Most data centers have acceptable methods of controlling physical access into their machine rooms, but not always for vaults or rooms that store sensitive documents, check stock or tapes. The physical location of a data center can also be problematic. A basement level may be safe and secure from the outside but be exposed to water leaks and evacuation obstacles, particularly in older buildings. Locating a data center along outside walls of a building can sometimes contribute to sabotage from the outside. Classified environments almost always require data centers to be located as far away from outside walls as possible to safeguard them from outside physical forces such as bombs or projectiles, and from electronic sensing devices.

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. Figure 2 lists the most common of these. The older the data center, the greater these exposures become. I 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 ten years old.

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

Figure 2 Major Physical Exposures Common to a Data Center

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 re-charge 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

Tips To Improve the Facilities Management Process

There are a number of simple actions that can be taken to improve the facilities management process. These are shown in Figure 3. Establishing good relationships with key support departments such as the facilities department and local government inspecting agencies can help keep maintenance and expansion plans on schedule. This can also lead to a greater understanding of what the infrastructure group can do to enable both of these agencies to better serve the IT department.

Figure 3 Tips To Improve Facilities Management

1. Nurture relationships with facilities department.
2. Establish relationships with local government inspecting agencies, especially if considering major physical upgrades to the data center.
3. Consider use of video cameras to enhance physical security.
4. Analyze environmental monitoring reports to identify trends, patterns and relationships.
5. Check on effectiveness of water and fire detection and suppression systems.
6. Remove all tripping hazards in a computer center.
7. Check on earthquake preparedness of data center. (devices anchored down, training of personnel, tie-in to disaster recovery)

Video cameras have been around for a long time to enhance and streamline physical security. Occasionally overlooked is the quality of the tape, the recording and the playback mechanism to ensure playback is possible. These should all be periodically checked. Another item to check is the environmental recording device. Many of these are quite sophisticated and 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.

In my experience, most shops do a good job at periodically testing their backup electrical systems such as UPS, batteries, generators and power distribution units (PDUs), but less so on fire detection and suppression systems. This is partly due to the huge capital investment electrical backup systems require, and managers wanting to ensure a return on such a sizable outlay of cash. Maintenance contracts for these systems frequently include inspection and testing, at least at the outset. But 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. This also includes up-to-date evacuation plans.