

Operating and Security Standards for Mainframes, Open Systems, and Telecommunications (Part 1 of 3)



By [Leo Wrobel](#)

Date: Sep 29, 2006

[Return to the article](#)

Business is messy enough without adding a disaster to the mix. In this three-part series, Leo Wrobel presents suggestions for developing standards to help your business prevent such messes in the first place, and for rapid cleanup and business restoration if something untoward happens despite your preparations.

Of Toilets and Technology

There's only one kind of disaster: the messy kind. If you've ever had water in a place in your building where it didn't belong, you understand what I mean by messy. Another example that comes to mind for me is a client whose cable risers had metal mesh floors that opened from one floor up and down to adjoining floors. These risers also contained water pipes just like yours probably do. To add to this issue, the cable risers were adjacent to the men's and women's restrooms. We cited this risk in *vulnerability analysis* that we performed for that client. We wrote the client up not so much because of the pipes but because if one of the restroom toilets backed up, the water only really had one place to go straight down the riser. Note to my readers: My wife and I know from firsthand experience that every kid backs up a toilet *a minimum* of three times during childhood. With our seven children, 21 episodes of backed-up toilets lent us a high degree of sensitivity to this issue. All kidding aside, we determined that water could be a problem for this client, particularly given the proximity to the risers and associated electronic equipment.

About three months after our report, we received a call one Monday morning that the client had sustained a disaster. It was water in the risers, all right, but not from the restrooms. Apparently one of the pipes inside the riser had sprung a leak early on Sunday. The water fell four stories to the bottom of the riser in the subbasement, to the only place in the whole organization that it absolutely *should not* go: the main UPS (uninterruptible power system). It was conveyed to me that the flash could be seen from the subbasement all the way to the third floor and all primary and backup power instantly went "poof." Imagine the impact of a hard shutdown on all of your mainframe, open, and telecommunications systems at this moment. Now multiply it by about 10, because this particular client was huge. Much to their credit, business was restored by end of day on Monday, but things were touch-and-go all day and it was several more days before their organization felt "right" again.

There are a few lessons to be learned by this example. One is about water. Another is about UPS and the false sense of security you may have, thinking that UPS systems don't fail. They do. This company eventually mitigated the future risk by mandating that outdoor electrical fixtures (that are *waterproof*) would become the standard for all future installations. Because of their disaster experience, this company created a new standard.

What Constitutes a Standard?

To put it in lay terms, *standards* are the things you document in advance to ensure that your recovery plan executes gracefully. A simple example might be a call list for personnel. Your recovery plan will prescribe that under certain conditions you call employees back to work, using a specific list of telephone numbers. But what ensures that the list is up to date? Indeed, what ensures that the list exists at all? This is what's documented in the standards. There are a number of different kinds of standards, such as the following:

- **Operating standards.** Housekeeping, backups, and other day-to-day practices
- **Security standards.** Passwords, intrusion protection, and the like
- **Standards geared solely to the recovery plan.** Call lists, procedures for emergency purchase orders where to get cash in an emergency, transportation, etc

Think about the example at the beginning of this article. What kinds of issues in your building, seemingly under your nose, are waiting to hit you some rainy Sunday afternoon? Figure 1 lists some of the more common considerations. In the following sections, I will address examples of all three kinds of standard:



Figure 1 Identification of 12 possible risk points inside a building.

Physical Installation Standards for Small Installations

Physical standards for small installations address such "common sense" items as routine housekeeping, which should apply to any good equipment installation. One item in this category would be physical access to equipment rooms.

We've heard many stories about how allowing unauthorized users into equipment rooms has wreaked havoc with users of technical systems. One story involves a drywall contractor doing a job for a company on a weekend. After completing the drywall job, the contractor used the connecting blocks on the telecommunication equipment located in the janitor's closet to clean the drywall mud off the trowels. The result was an extended outage the following morning after the drywall contractor was long gone. I heard about another experience from a professional I met at a seminar. She came in one evening to help clear up a problem, her young son in tow, and afterward was talking with her boss in the computer room. As the two adults chatted, neither noticed that the "off" switch for the main UPS was situated about two feet from the floor, right at eye level for the four-year-old. I will let your imagination fill in the rest of this story.

How many small telecommunications installations does your company have inside or located with the janitor's closet? Surprisingly, this setup is prevalent within companies, and a cause for concern when unauthorized or uneducated people have access to technical equipment. As a rule, equipment should be installed in a location other than a janitor's or custodial closet, and it should be secured and locked to prevent access to anyone other than authorized persons.

A second issue to consider in basic physical standards is housekeeping. A no-smoking policy should be strongly encouraged within the equipment room, for example.

Other considerations should include standards for fire extinguishers of the appropriate type(s), and posting of instructions for use of the extinguishers. Reasonable precautions should be taken to ensure that the temperature of the room conforms to manufacturer's specifications for the equipment, and that the room does not get unduly hot or cold. Also, power to the unit within the equipment room should conform to manufacturer's specifications, in terms of spikes, sags, brownouts, blackouts, and type of power.

The general condition of the room should also be evaluated, in terms of whether the room is too damp or too dusty.

It's generally relatively easy to devise a set of standards for non-mission-critical equipment in small installations. Your standard should say something like this:

The company bought this equipment, the shareholders paid for this equipment, and it is our responsibility not to let the equipment be stolen, broken, wet, or otherwise incapacitated.

In reality, except for the possible exception of a maintenance contract, little needs to be done to protect non-mission-critical small installations, unless the equipment supports a truly mission-critical function. As a general rule, equipment for large installations has a tendency to be mission-critical because it supports many more users, thus making a failure more costly to the organization. This issue is discussed next.

Physical Standards for Large Installations

Large equipment installations of all types present an entirely different sort of problem and should be protected much more intensively. The remainder of this section deals with physical and environment standards for large or mission-critical installations

Access to Equipment Areas

The standards document should bar all unauthorized individuals from equipment rooms and computer centers unless they have a documented reason to be there. This restriction includes other employees as well as visitors of all types. The room should employ additional protection, such as locks on the door, cipher locks, and other improvements. Just like the computer center, any large glass areas in the building should be considered for either reinforced glass or masonry to prevent damage from outside sources or intrusion.

General Housekeeping

In terms of housekeeping in the large network installation, a number of items should be mandated. This includes a ban on eating, drinking, smoking, or open flames of any type within the large network location.

Evaluation of Power

Power and environment for large network locations must be tested thoroughly. In areas where mission-critical applications are supported by large-scale systems, the use of such precautions as uninterruptible power supplies should be considered seriously.

Fire Protection

Fire extinguishers, fire alarms, Halon, etc., for any large-scale system should be on a par with or equivalent to those of large computer centers, which provide similar functionality in terms of mission criticality. This rule includes your PBX room and other telecommunications installations. Your standards should address smoke and particle detectors, fire escape plans, moisture detectors, dry-pipe sprinklers, Halon systems, and other miscellaneous items. You may also need to include such steps as labeling water pipes for fast shutoff in the event of a leak in the equipment room. Other items that we've seen in such plans typically include sheets of plastic or equipment covers, which can be thrown over equipment quickly in the event of any type of water problem in the building.

Change Control for Mission-Critical Equipment

Any mission-critical equipment (mainframe, open system, or telecommunications) should employ change-control management, including a list of persons authorized to make major software changes. Such standards should also include procedures for the password protection of maintenance functions, particularly those accessed from offsite. Procedures should be in place that require a full backup prior to any major software changes, to allow for fallback in the event that something goes wrong.

Disposal of Confidential Materials

Other items may also be included in the physical standards section, such as how to dispose of confidential materials. It's imperative that anything containing an access code or other confidential information be shredded, just like in the computer room, to avoid the chance of that data being intercepted by "dumpster dives," who delight in going through corporate trash and selling items of value to the highest bidder.

Coming Up

Next month, part 2 will present more tips for developing your own standards document. With any luck, by the end of the series you'll have a handy auditor's checklist of the common items to include your standards (as well as not-so

common items you otherwise may have overlooked). See you next month
