

Operating and Security Standards for Mainframes, Open Systems, and Telecommunications (Part 2 of 3)



By [Leo Wrobel](#)

Date: Oct 6, 2006

[Return to the article](#)

In part 1 of this series, Leo Wrobel examined how to start developing standards to help your business prevent disasters - and recover from them, if necessary. This article explores the physical standards that should be addressed in every business standards document: physical security, theft deterrence fire prevention, and more

We continue this month with the second of three articles providing tips for developing your own operating and security standards. By the time you've finished reading this series, you'll have a handy "to-do checklist" of the common items to include in your standards, and some not-so-common issues that you may have overlooked.

Developing Your Standards

A standards document can be designed as an integral part of the disaster recovery plan, but my recommendation is to have the standards completely separate from the recovery plan, for essentially two reasons:

- The disaster recovery plan should be as lean a document as possible, making it easy to understand in the event of a disaster. Maintaining such leanness is difficult if the document is cluttered with numerous standards
- The standards document is not intended to be an emergency procedures list; instead it's designed to mandate changes in the day-to-day conduct of a business. Stated another way, standards are the changes you make to the daily operations environment: a) to prevent disasters from occurring; and b) to ensure that the emergency procedures you have in the recovery plan will be executed gracefully

In many ways, the standards document is the conceptual foundation for the recovery plan. Think of your standards as the foundation, justification, and support for the emergency procedures you're implementing.

Because the standards document should be written only with the support and participation of all affected departments, your company may want to consider forming an "Operating and Security Standards" committee. This group, consisting of perhaps a dozen members, would be tasked with determining very broad company-wide issues such as which vendors, software, and equipment the company will support. Consider these reasons:

- Absent an "official" listing of supported services and vendors, it becomes all too easy for end users to subscribe to or purchase every type of service and equipment available. This lack of control spreads the technical services departments very thin as far as knowledge level and support services are concerned, since it's impossible to be 100% proficient on everything. The answer lies in sticking approved and supported systems that are maintainable, but that also don't stifle productivity
- Bear in mind that the support limitations just mentioned can present a severe drain on resources in a disaster, when technical support departments must scramble to restore innumerable systems and software packages at a recovery center or alternate work location
- Admittedly, the end user needs flexibility in order to be productive and make money for the company. Therefore, you also don't want to be too rigid in your standards of supported software and services. It's all a question of tradeoffs, and that's why I recommend setting up a committee
- The standards committee provides a forum for users to introduce new technologies, and for these technologies in turn to be evaluated by qualified technical people in terms of cost, benefits, and organizational drain on resources. From the technical perspective, it's impossible to get too close to your customer. If there's a hot new technology that revolutionizes productivity in the workplace, you had best learn how to provide it; otherwise, your internal customer will get it elsewhere.

Standards that Everyone Can Use

Some standards apply equally to the mainframe, telecommunications, and open system environments. Physical standards are a good example. When devising physical standards, the recovery planner will be interested in everything that could cause a disaster *within the building*. Such possibilities include things like fire, water, intruder and various physical security items. This first phase of standards planning will be very familiar to people who are already well-versed in mainframe or general recovery planning, since the same kind of security and installation standards that apply to large computer room installations generally apply to large telecommunications and/or open system (LAN) installations. For example, the following areas deserve a critical look:

- Physical security
- Equipment theft
- Telephone cable entrance facilities
- Fire-retardant cable
- Fire suppression systems
- Halon systems

Let's briefly examine some of the details of these areas.

Physical Security

There are a number of people within any organization who *think* they own the building. I am not joking. The IT manager, since he or she "owns" the computer room, probably feels that he or she is the rightful "owner" of the building. The security person at the front desk also thinks that he "owns" the building. One of the issues that your standards document should address is the inevitable turf issues: Who will rewire the building? Who will provide security? Who decides who gets in and who stays home after a disaster? Who will provide physical security to a building that has sustained a disaster?

Physical security is very important for a number of reasons. For example, if your job is related to information technology, you know that there are graceful ways to shut something down, and there are ways that keep you busy for a week afterward fixing corrupted files. Unauthorized persons in your building could wreak havoc on technical equipment by shutting something down unintentionally. And even true authorities could cause damage were you aware that the fire department will cut power to your building immediately after taking charge of it? Doesn't it make sense to post directions for the fire department in key locations about who to call, and how to shut down the equipment gracefully? Might your IT staff's cell phone numbers be included on the posted sign?

Starting to see the point? If you think an idea makes sense, the standards document is *the* place to make that idea into a policy.

Equipment Theft

As systems become more and more distributed, Intel-based "open" systems are becoming common in today's decentralized environments. Unlike the IBM systems of the past, these systems tend to "get legs" and often end up in pawnshops. Ditto laptops and Palm Pilots. Regardless of department, nobody wants their equipment to be ripped off. For that reason, part of the physical security process should include a "parcel pass" system to ensure that the person leaving your building with a laptop computer or other equipment really is *entitled* to leave with that equipment, by documenting the fact that he or she came in with it. The successful parcel pass system includes a mechanism whereby a user coming into your facility "signs in" his or her notebook computer, PDA, or whatever. Your security system should also include a check of briefcases or any carrying cases large enough to hide small equipment.

Think PDAs are a trivial concern? This could be a costly mistake. What would happen if a high-level employee's PDA is stolen? Can't imagine? Well, suppose the CEO of your company dropped his or her PDA in an airport. How much sensitive information about your company (private phone numbers, for instance) would suddenly become public? What would the liability be to the company for such things as insider trading?

Telephone Cable Entrance Facilities

Without telecommunications, your organization is toast. The physical audit of your facility should therefore include all cable entrance points into and out of the building. It makes little sense to pay a lot of money for diverse cable access, only to bring this cable through *the same building penetration* into your facility. Any place the cable comes in, in a common location, is an obvious point of failure, including sabotage from people working in the building, fires, or any number of other causes. Therefore, it's a pretty good idea to have your telecommunications people assess these input/output locations for single points of failure. The situation is similar for cable that goes between floors. All facilities between floors should be fire-stopped with a fireproof material to keep a fire in an equipment closet below one floor from spreading to another. And all of these facilities should be locked and secured from unauthorized personnel.

Fire-Retardant Cable

Inside the building, fire-retardant telecommunications cable should be specified when possible (it's required by local building codes in most places anyway). Traditionally, the standard has been Teflonable; however, another popular material used for fireproof cable is Kevlaroyes, the same material used in bulletproof vests. In older locations, many of the cables are probably made of polyvinyl chloride (PVC) in other words, plastic. When burned, PVC creates noxious fumes; add water, such as from a sprinkler or a fireman's hose, and you've created hydrochloric and sulfuric acid compounds.

It's a good idea to have a fire extinguisher in all cable closets, along with instructions prominently posted so that people are well versed with the use of the extinguisher. A no-smoking policy is common today in many companies but it's an absolute necessity in a cable vault. Cable vaults can produce hydrogeas, which is very combustible when mixed with oxygen. (Remember the Hindenburg?)

Fire Suppression Systems

There are three primary means of fire suppression within large commercial buildings:

- Carbon dioxide systems
- Sprinkler systems
- Halon

Carbon dioxide is effective in fighting fires because it interrupts the combustion cycle by removing the oxygen from the air. There are two problems with carbon dioxide systems, however:

- **It might kill you.** **an obvious concern.** Carbon dioxide removes the oxygen from the air, so people cannot be in the room with it. Therefore, carbon dioxide is primarily used in unmanned areas.
- **Thermal shock.** Any Vietnam-era veteran will remember that the quickest way to cool a six-pack of beer is to put it in a garbage can, get a CO₂ fire extinguisher, and give the six-pack a good long blast. The beer ends up nice and cold because the carbon dioxide in the extinguisher comes out at 150 degrees below zero. While that's an amusing image, it graphically illustrates a point: Even if people are asphyxiated in an environment with carbon dioxide, they'll probably suffer thermal shock because of the cold. That's another reason why carbon dioxide isn't used in areas where people need to work.

Sprinkler systems are very effective at fire suppression. More and more commercial buildings are requiring sprinkler systems to be installed even if one of the other two options (Halon or CO₂) is used, and regardless of whether electronic equipment is being installed. There are generally two schools of thought with regard to sprinkler systems:

- "Thou shalt never run water over electronic equipment."
- "Go ahead and install sprinkler systems over the equipment; it can still be restored."

Most of us have heard the first axiom, so let's consider the second. In situations today where equipment gets wet, engineers for the equipment or cleanup companies pull the boards out of the equipment, dip them in special solutions, and use a blow dryer to dry out the inner guts of the equipment. They're actually pretty good at this solution. In fact, there are advantages and disadvantages to this approach. The advantage, obviously, is that it's much cheaper to revitalize wet equipment than it is to replace it. The disadvantage is that equipment restored in this fashion can be trouble-prone in the future.

Generally speaking, sprinklers don't leak. They're pressure-tested and installed according to very exacting

specifications. The problem is that people cause most disasters, and disasters involving sprinklers are no exception. In equipment rooms with a 10-foot clearance for sprinklers, it's almost guaranteed that someone will try to roll a 11-foot crate through that clearance area. I've also seen instances of people crang through a suspended ceiling (perhaps to pull cable) and stepping on a sprinkler pipe, causing a leak.

One way of avoiding these types of problems is to use some type of dry-pipe, pre-action, or pre-charged sprinkler system. Here's how they work:

- A dry-pipe sprinkler system doesn't actually store water overhead in the equipment room; as the name implies, the dry-pipe keeps the water out of the equipment room until the fire alarm is tripped. An electromechanical device and a valve located outside the equipment room keep the water safely away until it's needed. When the first alarm system trips, the valve opens, allowing the water into the pipe inside the equipment room. Then, when the filament for the sprinkler system melts, the water comes out.
- Pre-action and pre-charged sprinkler systems work similarly to the dry-pipe system, some using an inner gas inside the sprinkler system to hold the water back, and others using a valve. For more information on these types of sprinkler systems, contact your company's authorized fire prevention supplier.

The place to define all of this information? Again, in your standards document.

As mentioned earlier, specialists are available to help in the event that your equipment does get wet. One company that specializes in these types of emergency restorations is [BMS Catastrophe](#) in Ft. Worth, Texas. Another, [SERVPRO](#), is a nationwide franchise. Either can professionally restore equipment to operating condition. They can be called after a disaster and after your insurance has kicked in, I might add to clean up the mess. Their numbers should be prominently displayed in your recovery plan and standards document.

Halon Systems

Halon was a great, albeit expensive option for fire protection, but it's falling out of favor due to environmental concerns. Halon works in much the same fashion as carbon dioxide systems, with one major exception: Because breathing it or being exposed to it is not harmful, Halon can be used in rooms with humans. Rather than taking the oxygen out of the air, or displacing the oxygen as carbon dioxide does, the Halon molecule interrupts the combustion cycle required to sustain a fire. Therefore, it's possible for people to remain in the room and still breathe normally during a Halon discharge.

If you have Halon in your equipment area, however, beware: Halon *not* effective against very deep-rooted electrical fires, like those that can start below your raised floor. These kinds of fires require very little oxygen to burn. Furthermore, Halon is only going to get more expensive. It is a CFC, like those used in commercial refrigerants, and as such it impacts the ozone layer in the atmosphere. Halon is being phased out, and what's left is becoming prohibitively expensive.

Summary

By now, you should be clearer on the types of things that need to be in the physical standards portion of your standards document. Next month, we'll look at operational standards, and consider changes you need to be making *now* in your working environment to ensure that your recovery plan executes gracefully.

See you next month!
