# Facilities Security and Information Assurance[1]

**by M. E. Kabay, PhD, CISSP-ISSMP**
**CTO & MSIA Program Director, School of Graduate Studies**
**Norwich University, Northfield, VT 05663-1035 USA**

**Contents**

1 The Building Location ..... 2
1.1 Natural Risks ..... 2
1.2 Neighborhood Risks ..... 2
2 Designing the Facility ..... 3
2.1 Location Within a Building ..... 3
2.2 Labeling Facilities ..... 4
2.3 Layout ..... 5
2.4 Walls, Doors and Windows ..... 5
2.4.1 Walls ..... 6
2.4.2 Doors ..... 6
2.4.3 Windows ..... 7
2.5 Ceilings and Floors ..... 7
2.6 Placing Equipment ..... 8
3 Electricity ..... 9
3.1 Power Conditioners ..... 9
3.2 UPSs ..... 9
3.3 Generators ..... 11
3.4 Emergency Lighting ..... 11
3.5 Tamper-proof Enclosures ..... 12
3.6 Emergency Power Off ..... 12
3.7 Electrical Maintenance ..... 13
3.8 Accidents ..... 13
4 Air Conditioning ..... 14
5 For Further Reading ..... 15

[1] Some of this material was originally published in *The NCSA Guide to Enterprise Security* published by McGraw-Hill in 1996. I updated and expanded the material for columns in a series of articles published in my *Network World Fusion Security Newsletter* in 2000 and have combined those articles into this single document and updated them primarily for use in the MSIA program at Norwich University. Updated January 2008.

 

*In this white paper, I hope you will find useful information on how physical security can support the security needs of network operations centers (NOCs) and data centers (DCs). In many of my consulting assignments doing enterprise security reviews, I have seen serious physical security problems; I hope that this overview will help fill in some of the missing information.*

# 1 The Building Location

Physical security looks at aspects of the environment in which we work and where we place network components. If you're planning to build a new computer center or relocate your existing equipment to an existing building, you have an opportunity to make your building work for you instead of against you. By picking the right combination of location, structure and layout, you can decrease your vulnerability while increasing the usability and maintainability of your equipment.

We'll start with cases where we have a choice of placement for our facilities.

## 1.1 Natural Risks

If you're starting from basics, you can consider the geographical location of your new site. Study long-term weather patterns, including frequency of heavy winds (e.g., tornadoes, hurricanes, and monsoons), snow, and lightning. Unless you're devoted to a life of great excitement, the likelihood of earthquakes should play a role when siting a major data center.

## 1.2 Neighborhood Risks

If it weren't for personal experience, I'd be embarrassed to remind you not to situate your data center in a dangerous place. Sounds like motherhood-and-apple-pie. But consider the following:

One fine spring day, as I drove to a data center where I was due to start a security audit, I noticed a field of enormous storage tanks on my left. It looked like a science fiction movie: row upon row of spheres and cylinders holding millions of liters of gasoline, diesel fuel and home heating oil. I was startled to find, upon following my directions, that the data center was directly across the road, no more than 200 meters away.

As I parked my car, I noticed a freight rail road crossing diagonally immediately behind the building. The tracks were still bright, so the railway was still in active use.

Finally, just as I was about to enter the building, I heard a passenger jet screaming across the sky just above, flaps out, heading for a landing at the regional airport.

Now that was a poorly situated data center.

Before choosing the building which will hold your corporate offices or data center, examine the neighborhood. Avoid

- flight paths for the local airport
- nearby chemical or explosives plants
- neighboring elevated highways
- railway freight lines.

Look out for

 

- mine shafts
- toxic waste dumps
- sources of dust and smoke (e.g., industrial incinerators)
- new or planned building activity (the vibration of pile drivers will harm your systems).

How easy would it be to reach the site in an emergency?

- Is there redundant road access?
- Are there several sources of help to fight fires?
- Is there police support and emergency rescue within easy reach?

Examine the socio-economic profile of the proposed location.

- Are there poor areas around the site?
- What's the crime rate?
- Is it improving or declining?

A participant in one of my courses reported that their corporation decided to move their headquarters one day after the new CEO took over.

Someone had shot at him in the parking lot on his first day at work.

On the other hand, some corporations and other organizations explicitly include contribution to their community as a goal; for example, AtomicTangerine training sessions ("boot camps") focus on helping selected non-profit organizations to upgrade their Web sites.[2] Perhaps instead of running away from a troubled area, we can help improve the socioeconomic conditions there by providing work, support for schools, and volunteer efforts to support other social action.

Whatever you decide, be sure to re-evaluate your physical location periodically and take appropriate action to protect your corporate resources.

# 2 Designing the Facility

## 2.1 Location Within a Building

In the March 1993 session (Atlanta, GA) of the Information Systems Security course I taught, a participant reported that a major company installed millions of dollars of computer equipment, electrical power conditioners and air conditioners on the 11th floor of an office tower. One Monday morning, the staff arrived to discover no 11th floor--and no 10th floor--and no 9th floor. The company had neglected to consult a structural engineer before loading the building with all that equipment. Luckily, no one was hurt in the collapse; however, damages ran over $100 million.

Access to the computer center should allow easy installation of equipment yet protect that equipment and its operators against physical assault. The ground floor seems too easy to attack; underground is susceptible to flooding. In the movie "Die Hard," we see a Hollywood

[2] See Kabay, M. E. (2000). A new recruit writes home from boot camp. < http://www.acm.org/ubiquity/views/m_kabay_2.html >.
See also < http://www.neads.org >

 

conception of a computer center: near the top of an office tower and entirely surrounded by glass. Since some computer equipment (or support equipment such as large-scale air-conditioning units) is larger than freight elevators can handle, the units have to be lifted into place using building cranes. The higher the computer center, the more expensive the crane. In case of fire, there may be a longer lead time for your staff to shut off the equipment and make their way to safety than if they're high up in a sky-scraper.

The second floor seems like a good compromise.

Place the network center or computer room far from hazardous areas. One story circulating in the security field tells of a security auditor in the U.K. who wondered about the vibrations he felt in his feet every now and then. "Oh that?" responded the data center manager, "That's just the lorries with the petrol." The computer room was directly over the passageway through which trucks carrying fuel oil regularly rumbled. Not a low risk situation.

High security vaults are required by law to have no external walls. That is, they are completely inside their building with corridors completely surrounding them. This design makes it much more difficult to punch holes into the data center without having anyone notice. And in case you doubt that a frontal assault on a computer center is likely, some automatic teller machines have been removed holus bolus by thieves operating back hoes and forklifts (it does make one wonder about why no one thought it odd to see a forklift trundling along with an ATM in the middle of the night).

When I was teaching in Africa in the 1970s, I recall thieves simply ramming their way into houses with trucks or cutting through the roof to enter secured buildings. And back in the Spring of 1995, one of the participants in an online "Computer Crime and Countermeasures" course told us about how a series of smash and grab attacks had been made on a local company known to have installed large numbers of new workstations. The criminals simply crashed through the wall and made off with the equipment in the minutes before the police could respond to building alarms. Maddeningly, the criminals apparently watched and waited until the victims had replaced all the equipment and did it again! They were dissuaded from further repetitions by having a 24 hour guard mounted on the site.

## 2.2 Labeling Facilities

One of the perpetual debates in INFOSEC is the value (or worthlessness) of what practitioners call "security through obscurity." The question is whether one can improve security by hiding information. For example, does it help to hide the details of an encryption product so that no one can easily find the algorithm? Dr Dorothy Denning enunciated what many of us call Denning's Law: that the strength of a cryptographic algorithm must not depend on its secrecy. A corollary of Denning's Law is that the validity of an implementation of a strong cryptographic algorithm can best be evaluated when the details of that implementation are accessible. In other words, distrust proprietary implementations of cryptography – there may be mistakes concealed in the object code that would leap out at (and be fixed) if the source code were made available for inspection.

Well, it's a long way from cryptography to building layout and physical security, but there is a connection. Some aspects of the layout may fruitfully be concealed to make the job of the attacker harder; however, some of the information about buildings ought to be available to improve emergency response.

 

Specifically, once you've built the computer room, be sure the local fire department knows exactly where it is. Keep your plans, including layout, up to date and coordinate with the fire marshals in your municipality.

However, there is no reason to mark the computer room with special neon flashers that read, "THIS WAY TO MILLIONS OF DOLLARS OF VULNERABLE EQUIPMENT." When I led a delegation of Japanese data center managers to visit the headquarters of EDS Inc. in Dallas in 1991, I was much struck by the anonymity of the equipment rooms. We walked through immense corridors with identical, boring metal doors, each marked with a numbering scheme. They all looked as if they could be broom closets. Then we'd open one up and find vast gleaming, sterile chambers of white tiles with and filled with huge CPUs – silent titans standing in rows with blinking red and green eyes. Today, I suppose, the same processing power would fit into someone's desk and look like a boring little box with a few holes and slots scattered around the surface.

The theory was that anyone who needed to know where the computers were knew where they were; why help anyone else locate such an inviting target?

## 2.3 Layout

Within your data center, try to put separate functions in different compartments. For example, keep printers away from consoles, disk drives, processors, patch panels and server racks: the paper is a fire hazard and the paper dust gets into your air filters.

To ensure that you don't wipe our your backups if there is a disaster in your NOC or DC, put tape vaults and data safes far away from your disk drives. However, you can reasonably have a local fire-proof safe or vault for the convenience of operators as long as the tapes stored there are not your latest backups.

Put your access-control equipment into a separate, high-security area, not with the rest of the computers. Security measures should reflect the potential exposure (consequences) of compromise; since access to the security equipment compromises everything else, it makes sense to guard it even more strongly than other components of your networks and systems.

Position your phone switches away from the computer room so that a single attack cannot put your entire operation into jeopardy. This suggestion follows the principle of reducing the number of single points of failure – more humbly known as not putting all our eggs in one basket.

The lower the traffic through a secure perimeter, the lower the risk of failure. Accordingly, try to keep your operations personnel comfortable inside the secure areas surrounding your equipment as much as possible; for example, include rest rooms, eating areas and office space for the staff who run your production systems within a tightly-controlled space inside the perimeter. This recommendation does not mean that you should forbid staff from leaving the secured area on their off time – that's their perfect right. However, the availability of such facilities will be convenient for some of the staff some of the time and will contribute to lowering the risk of intrusion and increase the speed of response to emergencies in the NOC or DC.

## 2.4 Walls, Doors and Windows

When I was in Africa in 1976-1978 teaching at the *Université nationale du Rwanda* in Butare, Rwanda, I remember thieves used to enter the houses of the rich *abazungu* (foreigners) by

 

ripping the doors from the walls using pickup trucks and chains. This experience greatly influenced my view of the importance of walls, doors and windows for security: they are weak spots in the perimeter.

### 2.4.1 Walls

When you build an enclosure for expensive and critical equipment, be sure they're substantial walls, not mere drywall partitions. Reinforced concrete that runs from slab to slab is best. Be sure the design allows for no crawl spaces around the wall above a drop ceiling or below a raised floor.

Check your plans and forbid any closets in the walls of your NOC or DC; they are weak spots and also provide concealment should anyone decide to punch through the wall using drills or explosives.

Finally, if your security needs are usually high (or if you have been watching too many action movies), talk to your architect about the design of the outermost walls of your building. Avoid chases (decorative indentations on the side) and other features such as rusticated stone that could make it easier for assailants to use mountain climbing techniques to climb your building.

### 2.4.2 Doors

Have as few doors as possible. You must know and obey all the safety regulations which mandate the number of exits you must include for protection of human life. Your architect will know what the law requires. However, only one door should be used for entry and normal exit. All the others should be used as emergency exits only. All doors should be equipped with crash bars and alarms and decorated accordingly. You can even buy signs that read, "DOOR IS ALARMED," (which always make me want to pat the door and reassure it that everything will be OK).

Choose heat-resistant doors (solid metal or thick metal with a structurally-sound core) and avoid any glass if at all possible. If safety regulations require glass panels to prevent smashed noses, insist on multiply-laminated bullet-proof, shatterproof small panels. Glass is a weak point anywhere in the secured area.

Installing a door that would make your local bank proud will be pointless if the frame is so weak that it – and the door – can be pried out of the wall with a crowbar. Door frames should be anchored solidly in the wall; if possible, bonded to the structural members of the wall. Door hinges should be on the inside of the secure area so they can't be dismantled. Choose hinge pins that are welded into place – not the ones that can be unscrewed and removed by anyone with a home tool kit.

Protect door locks with astragals (a lovely word meaning the edge-plates that prevent nasty folk from inserting credit cards, screwdrivers and chisels into the latch and forcing the door open). I have seen many sites which use astragals which extend from top to bottom of the door to provide maximum protection.

Don't use motion or simple proximity sensors to unlock or open doors into secure areas. Sliding doors controlled by such sensors – like those used in many public buildings – can generally be opened from the outside simply by pushing a sheet of paper through the rubber gaskets and waving it about.

 

### 2.4.3 Windows

Don't put windows in your network and data centers. I've already pointed out that there should be no outer walls in your computer room, let alone windows. Windows are physically weak; their frames are weak; and they let too many people see how you've laid our your equipment – including your security equipment.

I recall one manufacturing site where I stopped next to the floor-to-ceiling windows around the computer console room and stared at the five meter banner on the wall. It had huge numbers printed on it. I asked, "That's not the main modem number, is it?" Yup. So much for dial-in security.

Unfortunately, many executives who worked with computers in the 1960s and 1970s or who base their standards on Hollywood movies still think that "vision panels" make their data center look more impressive. If you are faced with this retrograde attitude, try a graduated approach to getting rid of these vulnerable spots in your defenses. Offer the decision makers a choice between, say, concrete, brick or bullet-proof safety glass. Alternatively, you can strap the executives down and force them to watch endless loops of Bruce Willis surviving the destruction of the Glass House in the movie "Die Hard."

If you cannot get approval to remove the windows in your computer room, install vertical blinds and keep them closed all the time except when there are important official visitors pressing their noses to the glass. Install security glazing (shatterproof metal-reinforced glass), and perhaps gratings securely attached to the walls. Install breakage sensors and connect them to the main building alarm systems. Aim motion sensors and closed-circuit television cameras at the windows. Move equipment whose presence should be secret away from the windows. Install a few dummy security cameras and motion sensors just to keep spies and intruders guessing.

There are a couple of other reasons why high-security sites do not permit windows in their NOCs and DCs. An obvious point is that external windows offer opportunities for snipers to attack individuals. More subtly, windows vibrate as people talk; using laser interferometers, it is possible to measure those vibrations and reconstitute the sound waves that caused the vibrations. Thus an exterior window provides an easy way for industrial or other spies to eavesdrop on conversations from an observation post far away in another building. However, don't try to persuade your top officials to give up their corner offices – some advice is just too unpleasant to bother presenting to upper management when the risks are low. I think that such advice might get you sent to the staff psychiatrist in most organizations.

What might work is to suggest that a window-rich office is perhaps not the best place to discuss top-secret strategic plans with catastrophic consequences of unexpected disclosure. People talking about make-or-break information would do well to do so in sealed rooms with no windows. The key is to be reasonable and not to apply security rules unthinkingly.

## 2.5 Ceilings and Floors

Practically all offices these days have drop ceilings; i.e., acoustic tiles are suspended from the actual ceiling. This design provides for a place where electrical and communications wiring can be laid out of sight. This crawl space must not extend without interruption into the data center. Within the data center, the drop ceiling should include smoke, heat and water sensors. This is

 

especially important when there are other floors above the NOC or DC and there is a possibility of water leakage.

Most information processing centers have raised floors because of all the cabling and power cords required for processing equipment and peripherals. The floor tiles are laid on a framework about 18 inches (~50 cm) off the actual floor. These tiles must be fire-resistant, easy to keep clean, and strong enough for the loads that will be placed on them. For access to the under-floor area, the tiles are raised using suction cups. Perforated tiles are part of the air-conditioning and fire-suppression systems and are raised using hooks.

The under-floor area must be kept scrupulously clean. Gas-based fire-suppression systems discharge high-pressure gas through the under-floor. If that area is dusty, the entire computer room will be filled with a cloud of dirt when the gas discharges.

In some cases, operators have used the under-floor as a storage area, sometimes for things that don't belong in the computer room at all (e.g., in one case I personally noted, soda pop). Such foreign objects interfere with the air-conditioning system and cause access problems in emergencies.

## 2.6 Placing Equipment

In recent years, computer equipment has become increasingly tolerant of environmental conditions. Midrange and many mainframe computers are now air-cooled, survive temperatures from cold to hot, and run on regular 110V current. Nevertheless, some people abuse their systems. Some years ago, while I was hanging my coat in a hall closet one day on a visit to a client, I noticed blinking green and red lights down among the boots and galoshes. I moved some heavy winter coats out of the way and discovered a network server. Startled, I asked my host what it was doing in an unprotected hall closet. It seems that they ran out of room in the computer center and the server was installed in the hallway. "It doesn't need special conditions," he chirped. No, but its on/off switch was open to anyone who wanted to try bringing the network down, and I doubt that the engineers had planned on seeing their design spattered with mud, water and salt.

In many smaller organizations, I have noted with dismay that electrical power cord extensions are looped helter-skelter around the bottoms of desks and partitions. Aside from the problem of tripping over these cords and crashing wildly about one's office, these folks run the risk of unplugging their own computer, causing an occurrence of the notorious power-cord-out-of-the-socket "virus" that occasionally amuses technical support staff.

A related problem with poor wiring practices is that many users and even some NOC managers don't label their cables. The consequences are most serious when people have to move their equipment; either they spend precious time under pressure trying to label their gear or they just unplug everything and hope they get everything right when they reassemble their systems.

Sometimes people plug their computer systems into a power bar in their neighbor's cubicle without informing anyone. When the neighbor innocently cuts the power on their own system by hitting the main switch on the power bar, the electricity-borrower has a power failure too. Another problem occurs when people run out of sockets in their cubicles and decide to lay an extension cord out into a hallway to tap into a handy socket there – and naturally, without bothering to label the wires. These arrangements inevitably result in what ought to be a

 

predictable loss of power when a building cleaner innocently unplugs the power cable to power their floor polisher.

Some common-sense recommendations:

- Don't subject your valuable, sensitive and critical equipment to inappropriate environmental stresses.
- Organize your equipment cables so that they don't tangle each other or passers-by.
- Label your cables clearly using color coded tape or printed labels.
- If you must use electrical outlets outside your immediate control, lock the plugs into place if possible or at least label them clearly so that others don't inadvertently cut power to your systems.

# 3 Electricity

No electricity, no computing. Given that simple principle, it makes sense to have good electrical power and a mechanism for working without external power – at least, long enough to allow a *graceful shutdown* (in contrast with losing everything that was in RAM when the power stopped).

## 3.1 Power Conditioners

According to research by field service organizations as far back as the 1980s, almost half of all service calls on PCs are related to bad electrical power. Power fluctuations such as brownouts (transient low voltage), spikes (transient over voltage) and line noise (waveform deformations) can physically damage sensitive electronic equipment. Even surges on phone lines can damage modems and PC boards. At a very minimum, nobody should be running a computer without a surge suppressor in the power circuit; the cost is negligible compared to the assurance that a fuse wire will melt or a breaker will trip instead of having your precious equipment do the melting and breaking.

## 3.2 UPSs

Power outages cause down time, but the more serious threat is that power interruptions during a critical phase of posting data to disk will cause data corruption. If a disk drive goes down while data are being written into a file, one or more records can be damaged. Parity checks or cyclic redundancy codes on the disks can usually pick up and sometimes correct errors. However, if the computer is updating a directory structure when the power disappears, there can be serious trouble. Directory structures include database or file indexes and system directories such as the DOS File Allocation Table (FAT). Damaging even a small part of these structures may make large amounts of data inaccessible. Recovery of data may require painstaking retrieval of section (cluster, sector) after section of individual files.

Luckily, in recent years more operations are using fail-safe disks (e.g., RAID, Redundant Arrays of Inexpensive Disks) with automatic mirroring and recovery. The occurrence of irrecoverable disk errors is low in such systems.

Midrange and mainframe computers have long had their own internal electrical-power conditioners and uninterruptible power supplies (UPSs). Less powerful, less expensive systems did not. However, users have placed critical applications on servers, work stations and microcomputers; alternative power supplies and line conditioners are now required components

 

for most production systems – and if you depend on your data and your PC to accomplish whatever you consider critically important, then your system is a production system.

UPSs run the power from the mains into a transformer which keeps batteries charged; output power comes from direct current (DC) rectifiers which convert the battery power into alternating current (AC). UPSs provide excellent-quality power and good insulation from power-line fluctuations.

For PCs, work stations and servers, UPS units in the 0.4-1.2 KVA (kilovolt-ampere) range are sufficient; they range in cost from about $75 for a little device about the size of a large surge-suppressor that gives you just enough time to shut a PC down gracefully to over $1,000 for a sizable unit that can power your entire office. Keep in mind that you have to plan for peak loads, not just the average power drain. Big laser printers, for example, can run at 700 watts while warming up yet function on standby at a mere 100 watts. Older, physically larger disk drives take much more power while spinning up than while running normally. However, modern tiny, ultra-dense drives (e.g., 500 GB on a 1.5" spindle) require so little power anyway that they're no longer an issue.

In my office, I run two 0.9 KVA UPSs connected to a power conditioner. All my essential gear is connected to the UPSs: processor towers, monitor, phone, and even one lamp. I don't put the printers or the stereo system on the UPS. Many people will deliberately exclude their printers from the calculations for their proposed UPS. They can live without the printer when it loses power. At worst, given the automatic spooling that's normal on modern operating systems, they may have a single damaged page to reprint when they start the job up from the spool files.

The less load you put on the UPS, the longer it will last during the power outage. If you're lucky you will not only be able to avoid catastrophic errors but may even keep working productively until the power comes back.

The size of the batteries in your UPS and the drain by your systems determine how long the UPS can keep your system going. At a minimum, you need time for a graceful shutdown; five minutes is ample to allow you and your users to exit from application systems and shut down all peripherals and processors. If there is a reason to continue operating your system during a power failure (e.g., to protect the security computer that controls your physical access control systems), you may have to order extra batteries (for hours of operation) or a generator (for continuous operation as long as the fuel lasts).

Not all UPSs allow for addition of extra batteries, so examine the specifications carefully if you are thinking of providing extended run-times. Some systems are made to be completely customizable, with rack-mounted batteries that you can order and add at any time without fuss.

Just in case anyone reading this has the bright idea of hooking up one UPS to another, don't. The second law of thermodynamics ensures that all you will do is waste the battery power of the first unit as you try to charge the second one. You *can* run two or more UPSs in *parallel* – as when you attach different equipment to different UPSs.

It's a good idea to do a dry run with your new UPS: you really want to have a clear idea of just how long you are going to have once the external power fails. I have timed how long I can run without external power: almost exactly 30 minutes for my setup. At that point, the tolerable repeating beep from the UPS turns into an annoying whine; I save my work to disk, exit from my

 

application, fire up the file transfer software and get the current working documents over onto my portable computer so I can keep working once all the power is down. Then I immediately shut down the main system.

### 3.3 Generators

If you use only a portable computer, you already have a UPS: your batteries. With three batteries for my portable, I can count on around 10 to 15 hours of continuous (well, occasionally interrupted for battery exchange) operation. In my office, though, I don't need to worry about that limit: I also have a 7 KVA electrical generator that supplies my house and office. Now, you have to understand that this is not a general recommendation for everybody's home office; I live out in farmland northeast of Montpelier, Vermont, and we can have power outages lasting days when the ice breaks the power lines. Worse still, we have a 130-gallon tropical fish tank that cannot fall below 75 F without starting to kill our fish. The $1500 generator and the $1,000 wiring job to put in a transfer switch just made sense for us. More to the point for this article, I definitely can run the portable computer's power transformer from the generator power without problem.

For larger, more critical applications, you should evaluate large-scale UPSs which can be hooked into your office or building electrical system. Systems for loads ranging into the hundreds of KVA can cost from $2,000 up into the $100,000 range. Some units include gasoline or diesel generators and heavy-duty flywheels or large isolation transformers to smooth out the rough waveform of the generators' output.

Never run electronic equipment directly from generators without checking the power quality carefully. If you have the gear in-house, you can check power quality directly with the appropriate power-line monitors. Otherwise, see if your friendly neighborhood computer supplier has a power-line monitor they use for site qualification studies. When I worked for Hewlett Packard in the early 1980s, we would routinely install a monitor that printed out reports on the fluctuations in power to determine if we would allow our precious equipment to be installed without an external power conditioner. The reason: long experience had taught HP that bad power equals increased repair calls – and with a fixed-cost service contract, you can understand how seriously we took this kind of environmental report card.

Ordinary household generators of the kind sold in hardware stores for your country cabin can destroy your computer equipment within seconds. In my case, I discovered that the household generator I use has such a jagged (sawtooth) waveform that it could not be used to supply my UPS without a power conditioner.

The manufacturer explained that they have had trouble hooking domestic generators up to their equipment unless the generator is running at no more than one-third its rated capacity. In other words, in order to use their equipment, we are expected to buy a generator three times larger than we would normally expect to need. I was not pleased, but I didn't replace my generator, either.

Keep these problems in mind if you are shopping for a generator and avoid the hassles of trying to hook up incompatible devices.

### 3.4 Emergency Lighting

Common sense (as well as workplace safety regulations) dictates that you install adequate emergency lighting for all work areas and escape routes. After the bombs exploded in the World

 

Trade Center in New York in February 1993, thousands of people had to feel their way through smoke-filled, pitch-black stairwells. It seems the emergency lighting system was controlled by computers that had been blown up by the explosion in the parking garage. Independent lights with their own batteries would have saved time and reduced injury in that disaster. Portable flashlights supplied to emergency marshals would have helped, too.

### 3.5 Tamper-proof Enclosures

Now that you've spent all this money on electrical power equipment, how about protecting it all from tampering? Keep all electrical junction boxes, breaker panels and main switches under lock and key. In one hospital information security evaluation a decade ago, I recall bringing the head of the intensive care unit into the hallway and pointing at a panel on the wall. "What's that?" I asked. She shrugged and said, "I dunno; an electrical panel, I guess." "Open it," I said. She did (it was unlocked). When she saw the labels on the breakers her pupils dilated and she looked horrified: those breakers controlled the precious equipment in her ICU – respirators, controlled-injection pumps for intravenous drips, heart monitors, external heart pacemakers – the works. If someone had tripped those unguarded, unprotected breakers, some of her patients would have died instantly. Moral: if you care about your electrical power, you have to protect junction panels just as strongly as any other component in the circuit.

If you have to install additional power cables, ensure that they're pulled through protective ducts or manifolds, not left lying about in the suspended ceilings where anyone can get at them. And document all the switches and breakers correctly and readably so that people can make intelligent decisions in an emergency.

Label your UPS and power conditioners plainly with warning signs to prevent unauthorized equipment from being added to the circuits. In the May 1993 session of one of my Information Systems Security courses, a participant reported that an operator plugged a vacuum cleaner into the nearest electrical outlet, overloaded the UPS, and took down the LAN for a few minutes. That nearest outlet happened to be in the server's UPS, but the staff member had no idea that there was anything special about that outlet. You can't blame people for errors when you've failed to provide both training and proper labeling.

### 3.6 Emergency Power Off

Be sure that there are at least two "panic buttons" (more properly known as the Emergency Power Off or EPO) in your computer room: one at each end and both near exits. The EPO cuts off all power to everything in the computer room except the lights. These switches should be protected against accidental use; for example, you can choose switches covered with a spring-loaded flip-top cover or models with the button at the bottom of a one-inch finger-sized tube. Install a phone within reach of each EPO for rapid communications in an emergency. Put a long extension cord on the handset of that phone or provide a cordless phone for use only in an emergency (cordless phones are not secure and should not normally be used for business communications). [3]

It is especially important that the EPO shut down the power to your air conditioning equipment in case of a fire: ventilating an area threatened by fires is a really bad idea.

[3] For an extended discussion of the EPO, see Kulkarni, A. & S. McCluer (2005) "Understanding EPO and its Downtime Risks." APC White Paper #22. < http://www.apcmedia.com/salestools/ASTE-5T3TTT_R2_EN.pdf >.

 

In one apartment building where I lived many years ago, a visitor had trouble opening the electrically-operated door and therefore pulled the nearest handy lever – the fire alarm. To prevent this sort of error, label panic switches clearly; e.g., "MASTER POWER CUTOFF." In general, my experience running a large data center convinced me that every single switch, electrical receptacle, and data communications plug ought to be labeled understandably and clearly. I don't think you can easily overdo labeling inside an operations center.

### 3.7 Electrical Maintenance

Keep fuses handy in all the right sizes for all your electrical gear, including the power supplies. Make sure that your staff knows exactly where those fuses are kept. Run drills to make sure that their response to an electrical emergency is exactly what you have decided makes the most sense.

Every time you order modifications to the electrical system or find out that your building is having such modifications, be sure to check that the grounding is correct. Especially when your midrange or mainframe systems use three-phase power, it's crucial that the correct wires carry the ground. While you're at it, verify that your building is properly grounded in case of lightning strikes. This precaution is especially important throughout the great plains of North America.

Be sure that your facilities crew are absolutely clear on which circuits may NOT be interrupted for routine work on the power system. Losing power because an electrician tripped a breaker is just as much a problem as any other kind of power loss. And it's worse if some untrained, unaware person shuts off power from your standby power systems – and the RISKS FORUM DIGEST is full of reports of that kind of incident.[4]

### 3.8 Accidents

What would you do in case one of your colleagues touched a live 120V wire and their hand clenched rigidly onto the power source? If you don't know instantly, you have a problem; I suggest you also ask your colleagues to find out if the problem is widespread in your organization. Not knowing what to do in such an emergency could cost one of your friends his or her life.

One hopes that there would be an easy way to cut the power: that's one of the purposes of the panic button we discussed in the last contribution to this sub-series.

But if someone were in the process of being electrocuted in your computer room and for some reason you didn't have a panic button, what would you use to move them off the live wires? You're supposed to use a non-conductor such as wood or plastic. Some data centers have a wooden cane for this purpose hung on the wall along with fire extinguishers and other emergency equipment. Don't forget to train your staff, though, or the cane will simply sit on the wall while several people electrocute each other in turn. And issue a firm injunction against all Charlie Chaplin imitations during working hours.

If for some reason you want to shut off your computer equipment automatically or to shutdown and start it up remotely, you can install inexpensive switches to do both. There are even switches with serial ports that allow a computer to send a signal which will power down all systems on the switch. Thus your system could shut itself off at the end of its nighttime processing.

[4] http://catless.ncl.ac.uk/Risks/

 

Contrariwise, there are switches that sit on the phone line; when they sense a modem or FAX signal, they can turn on the power to whatever equipment you connect to them. For those people who insist on powering off their equipment overnight, some switches can even be programmed with a timer so that your system can be up and running in the morning when you arrive at work.

However, it is my understanding that shutting off the power to computer equipment is not recommended unless you intend to leave it off for an unusual length of time. The way it was explained to me by an electrical engineer is that the repeated thermal contractions and expansions caused by powering off computer systems actually causes more harm than simply leaving everything on standby. One of the consequences of the shrink/expand cycles seems to be that improperly-installed chips with cold-solder joints can actually work themselves loose enough to start causing intermittent problems. This advice was bolstered by the study to which I alluded earlier, in which a large firm with several thousand PCs that were divided into always-on and shut-off-at-night groups. The study supposedly showed that powering down at night and powering up in the morning was correlated with increased hardware problems.

Unfortunately, I have lost the reference to this study and, despite a serious effort to locate the information in my databases and on the Web, am unable to find the original report. However, other, more recent, documents do support the view that repeated power-on/power-off cycles are harmful for electronic gear.[5]

# 4 Air Conditioning

Concentrations of computer system equipment (host processors, LAN servers, disk drives, system printers, tape backups, multiplexers, and so on) can use so much energy that regular office air-conditioning (A/C) fails to dissipate the heat. Ideally, temperatures in your computer center should be 66-73 F (19-23 C). Midrange and mainframe systems still produce so much heat that A/C failure can rapidly lead to high temperatures.

Each component of your computer system usually has its own temperature sensor that can cut off power at the upper end of the temperature range. In addition, computer rooms have their own global thermostats and cutoff switches.

In the data center where I worked as Director of Technical Services in the mid-1980s, an A/C unit failed one day. A new operator noticed the rising temperature but didn't realize the cause. He looked about for the room thermostat and noticed a temperature dial in the ceiling. It was set at 90 F (32 C). He turned it down to 70 F (21 C) and immediately lost power all over the computer room. He had changed the overtemp power cutoff.

That day, we labeled every single dial and switch in the computer room.

Relative humidity should be maintained from about 45 to 55% to prevent static electricity buildup (if too dry) and condensation or curling paper (if too humid).

Air pressure in the computer center should be slightly higher than in surrounding office areas so that air tends to flow out of the equipment area when doors open (especially in an emergency, positive pressure helps keep smoke and dust away from the electronics).

[5] See for example *Upgrading & Repairing PCs, Eighth Edition* (QUE), Chapter 8, "Power Supplies," Section "Leave it on or turn it off," http://cma.zdnet.com/book/upgraderepair/ch08/ch08.htm#Heading11

 

The computer room A/C should be separate from that for the rest of the building. You need to be able to control ambient conditions yourself under normal circumstances.

Protect the external air intakes to reduce the risk of a gas attack or tampering with your A/C. Make sure that the ductwork is non-combustible and that it does not provide a crawlspace for unauthorized access to your computer room. Sometimes it seems that every movie involving penetration of a secured area includes an obligatory scene in which heroes or villains crawl undetected through the A/C ducts. In every case, access to the ducts is relatively easy and is accomplished by removing a flimsy grate without using tools.

Link your A/C units to the fire-suppression control systems. The panic button that cuts power to your computer equipment should include the A/C equipment. In case of a fire, the last thing you need is the A/C continuing to pump fresh air into an enclosed area at risk.

The perforated tiles in your raised floor are part of the A/C system and fire-suppression systems. A/C engineers lay these tiles in patterns that control air flow within the computer room. These tiles must not be displaced at random. In some data centers, operators move the tiles about without considering the effects on air flow; in one case reported by a student in my Information Systems Security course, operators decided they didn't like the tiles, so they moved them all over to the far corner of the computer room. This spontaneous redesign of the A/C system produced Arctic conditions in one area and tropical temperatures in the other. The operators were on their way to generating a model of the global atmospheric wind patterns.

Although I've mentioned this in a previous section, I urge you to make sure that the floor under the raised tiles is kept clean and free of extraneous materials. The area next to an A/C outlet is often very cool; however, is not an appropriate cooler for soft-drinks and beer ☺.

## 5 For Further Reading

Bosworth, S. & M. E. Kabay (2002), eds. *Computer Security Handbook*, 4th Edition. Wiley (ISBN 0-471-41258-9).

Platt, F. (2002). "Physical threats to the information infrastructure." Chapter 14 in Bosworth & Kabay.

Platt, F. (2002). "Protecting the information infrastructure." Chapter 15 in Bosworth & Kabay.