Powering Business Worldwide

White Paper

Ten Ways to Protect Your IT Infrastructure

Reduce Costs while protecting critical business systems.

If you have wondered how to provide serious protections on a small-business budget, this white paper is for you.

- Learn about power, cooling and security issues that put your IT systems at risk.
- Find out how to provide clean, conditioned, continuous power for critical systems.
- Understand how to select the right power protection strategies for your needs.
- Learn which cooling and security practices are best for your IT environment.
- Save money with optimized strategies while increasing IT reliability and longevity.

It's a hostile world for IT equipment.

In this age of critical computing systems and the Internet, business continuity requires that you protect your IT infrastructure from all the hidden threats of the typical facility environment. Every business, no matter how small or large is at risk.

Take power, for instance. You may only notice power disturbances when the lights flicker or go out, but your PCs, servers and network equipment can be damaged by many other power anomalies that are invisible to the human eye, and that degrade equipment over time.

What about heat? Your equipment rack or enclosure is probably packed with more high-density equipment than ever. That equipment is generating more heat in smaller spaces than ever, creating a sauna that could shorten the life of IT systems that are critical to your business.

What about human error? Even the most well-intentioned employee could unwittingly pull out a cable or power cord, misconnect devices or zap a component with static electricity.

Is the risk really worth worrying about?

You can worry now, or worry later. One choice is proactive, the other potentially painful. IT systems are at risk even in the largest data centers. Of 450 Fortune 1000 companies surveyed by Find FVP, each suffered an average of nine IT failures each year. About 28 percent of these incidents were caused by power problems.

The costs are high. According to Price Waterhouse research, after a power outage disrupts IT systems…

- 33+ percent of companies take more than a day to recover.
- 10 percent of companies take more than a week.
- It can take up to 48 hours to reconfigure a network.
- It can take days or weeks to re-enter lost data.
- 90 percent of companies that experience a computer disaster and don't have a survival plan go out of business within 18 months.

If you think the risk of a massive weather disaster like hurricane Katrina is slight, you're right. Only three percent of data loss incidents are caused by site disasters. Computer viruses only account for seven percent of data loss incidents. The most destructive influences on data centers actually come from much more mundane causes: software error (14 percent), human error (32 percent) and hardware failure (44 percent), frequently triggered by power problems, including power failure, power sages, power surges, brownouts, line noise, high voltage, frequency variation, switching transients and harmonic distortion.

That means that your greatest risks of data loss or system damage are preventable—or at least can be greatly mitigated.

In this paper, we'll show you best practices that will actually save money and could save you from the potentially devastating effects of downtime or equipment damage. Here are 10 practical and affordable steps any business can take to reduce the risks and enhance the reliability of IT systems.

1. Don't assume your business is too small for protective measures.

Power problems are equal-opportunity threats. They hit small businesses as often as big ones. Your PCs, servers and network are just as critical to your business as a data center is to a large enterprise. Chances are, you rely on more sophisticated and expensive data equipment than ever, and these systems run unattended much of the time.

Consider how much investment is at risk. Even a small server configuration and company LAN (local area network) represents an investment of tens of thousands of dollars. Even a basic server, such as a Compaq Proliant DL320, costs more than $2000. Figure on $7000 for a IBM Xseries 360, $15,000 for a Compaq Proliant DL590, $22,000 for an IBM Xseries 380, and $37,000 for a Sun Sunfire Blade System. Add operational applications, management systems, critical databases and networking equipment. Clearly the IT infrastructure is a significant company asset that deserves adequate protection.

Downtime is costly**.** Your IT hardware may be insured, but what about the potential loss of goodwill, reputation and sales from downtime? Consider the number of transactions or processes handled per hour, and multiply that by the value of each one and the duration of an anticipated power incident. Add the delays that inevitably occur when rebooting locked-up equipment, restoring damaged files, and re-running processes that were interrupted. Then add the cost of lost revenue from being disconnected from your suppliers, business partners, and customers.

Could your business absorb the cost of an extended power outage or IT failure? According to the US Department of Energy, when a power failure disrupts IT systems…

- 33 percent of companies lose $20,000-$500,000
- 20 percent lose $500,000 to $2 million
- 15 percent lose more than $2 million

A sound power protection strategy is cost-effective insurance.

2. Treat any IT equipment location as a data center.

A large enterprise will have a climate-controlled room with raised floor and all provisions for protecting IT equipment. For a small to mid-sized business, the rack environment just might be the data center. All the necessary components for power protection, cooling, security and so on must be housed within one or more racks or cabinets.

When selecting the physical framework—rack or enclosure—in which to deploy IT equipment, you'll want to evaluate a number of considerations:

- **Access control**. Open racks leave equipment vulnerable to accidental or intentional misuse. Enclosures with locking entries provide physical protections from unauthorized access and other environmental hazards, and permit more deployment options.
- **Thermal management**. Central air conditioning can only go so far in overcoming the heat output of today's dense rack environments. Enclosures can be equipped with fans to keep temperatures within acceptable levels throughout the equipment.
- **Power protection**. Power protection and battery backup can be provisioned in compact, rackmount units to protect racks and enclosures from power problems.
- **Power distribution**. Power distribution units can be mounted on shelves or in side channels to distribute power throughout one or more racks, taming the tangle of power cords that would otherwise be necessary.
- **Cable management**. Look for options that provide for a neat, well-organized arrangement of cables that will not impede airflow or enable cables to be accidentally unplugged.
- **Flexibility**. The enclosure should accommodate rack-mounted or shelf-mounted equipment, linking of bays into larger units, graceful management of unused space, and the option to roll the entire unit to another location as needs change.

- **Monitoring**. Chances are, IT equipment is expected to run unattended most of the time. A monitoring/management system provides good visibility and control of the IT environment from anywhere, over the company network.

3. Beware of hidden threats in apparently 'healthy' power.

Public utilities are not required to provide computer-grade power—and they don't. IT equipment is damaged by subtle anomalies that users never see, such as sags, surges, spikes, brownouts, line noise, frequency variation, switching transients and harmonic distortion. A business on typical utility power is subjected to these hidden power problems every day and complete outages several times a year.

Look beyond generators and surge suppressors.
These are band-aid solutions for systemic problems.

- *Backup generators* address power outages but provide no protection against the eight other power disturbances. Furthermore, critical systems can lock up in the 10-30 seconds it takes to switch to backup power. Generators themselves can create harmful power effects when switching between utility and generator power.
- *Surge suppressors* address the power surges, but have no effect on the under-voltage and variance conditions that can erode equipment health over time or zap it in an instant.

Uninterruptible Power Systems (UPSs) go beyond these power-protection strategies while presenting a compelling business case in any commercial environment. UPSs protect your IT systems by:

- *Conditioning incoming power* to smooth out the sags and spikes that are all too common on the grid and other primary sources of power *Providing ride-through power* to cover for sags or short-term outages (30 – 60 minutes, typically), by selectively drawing power from batteries, backup generators and other available sources.

4. Determine the level of power protection you need.

Whatever the application, there's a UPS configuration available to provide the required performance and features, at a price point to suit all budgets.

What type of UPS is appropriate for your needs?

Do you *need to protect personal and small office computers?*
If so, a standby UPS probably serves the need. These UPSs run off normal utility power until they detect a problem; then they switch to battery backup. There is plenty of time to save work in progress and gracefully shut down equipment.

If you need to protect critical enterprise devices or those protected by redundancy and alternate routing, you might choose a line-interactive UPS. These UPSs regulate voltage up or down as necessary to smooth out irregularities in power (without draining batteries), and protect equipment from line "noise." These UPSs provide more protection than standby UPSs, and therefore are useful in data racks, communication systems and workstation groups.

If you need to protect mission-critical equipment— such as essential application servers or communication networks—the only real choice is a double-conversion UPS, which completely isolates equipment from raw utility power to deliver the cleanest power. That makes this type of UPS the best choice for critical IT equipment, such as mass storage devices, server farms and data networks. Today, some 95 percent of UPS dollars are invested in online systems.

What UPS strategy is best for your business?

One UPS can protect a single device, a rack of devices, or several racks of equipment. A UPS can be deployed at an employee's desktop, in the IT rack or enclosure, or at main power distribution points. For server rooms where there are several racks, it is common to choose a centralized solution instead of separate power protection for each rack, because this approach is typically more cost-effective.

How much UPS capacity do you need?

The mean value for rack power consumption in corporate computing environments is about 1kW. However it is becoming more common to load racks with power requirements between 1.5 and 3 kW. As equipment gets smaller, blade servers become more popular, and space constraints require companies to pack racks more fully. Will see racks will require far more power in the future. A rack full of 1U blade servers can potentially draw 20kW or more.

UPSs can be configured for a broad range of output capacities, and multiple units can be deployed to accommodate loads up to megawatts. In a modular architecture, you can add or remove components as needed. In fact, the system should be designed to permit individual modules to be taken off-line for maintenance without removing the load from conditioned power.

To determine the actual power requirements to be protected by the UPS, you could…

- **Get information from equipment nameplate ratings**, but this is a costly method resulting in wasted infrastructure dollars.
- **Use actual power measurements**. This method yields the most accurate readings, but in-service numbers won't be available if you are planning or expanding an IT infrastructure.
- **Check the manufacturers' Web sites** for the equipment you have. If power data isn't available there, request it from the manufacturer. This is the most practical and recommended way to get realistic figures on power consumption.

5. Provide for backup power during utility outages.

Assess how much battery runtime you need. During an outage, you need enough battery runtime to gracefully shut down systems or switch to backup generators. Modular UPS designs enable you to add internal and external batteries to increase runtime as more equipment is added to the load.

When the outage hits, selectively shed loads. When power outages extend beyond the limits of backup systems, power management software can orchestrate the selective, sequential shutdown of loads. For instance, the system could shut down power to non-critical devices (Load Segment 1), thereby extending battery backup time available for critical devices (Load Segment 2).

6. Protect IT equipment from overheating.

Climate control has always been a big concern for IT managers of large data centers. It's expensive to provide air conditioning for a data center full of heat-generating equipment. However, heat dissipation is an equivalent concern for small to mid-sized businesses, because the data room may be a single enclosure.

As equipment continues to shrink and become more dense, it generates more heat than ever within the enclosure. This heat must be removed, because high temperature will cause electronic equipment to falter and fail before its time. In fact, 60 percent of hardware downtime is heat-related*.

What's the best way to handle equipment heat output? In a February 2006 Ziff-Davis Media study, 21 percent of respondents said that power consumption and cooling issues force them to leave some rack space unused—an average of 18 percent of available space left empty. That might not sound like a big deal, but every unused position in a rack has a hidden cost associated with it, especially if the data center is near capacity.

The organization would prematurely have to consolidate servers, or replace servers with more modern and thermally efficient designs, or expand the data center along with its power and cooling systems. All of these measures signal an incipient heat problem that must be addressed.

For most small to mid-sized businesses, the most effective solution is convection cooling—in other words, fans.

Door-mounted fans on the enclosure offer some compelling advantages. Without occupying any rack unit space, this type of fan evenly distributes cool air in a horizontal flow from front to rear in the enclosure.

- If heat output from equipment placed lower in the rack could rise within the enclosure, you can attach exhaust fans to the rear door of the enclosure to help remove this heat.
- If there is empty space in the enclosure, and you're concerned that hot air from the back of the cabinet could circulate back into the cabinet, you can add blanking panels to partition off the unused space in the enclosure.
- If the enclosure is very densely packed with high heat output equipment, you can install multiple fans on the front doors.

Note: Roof fans are often used to remove hot air out of the top of the enclosure and toward the ceiling, perhaps into a hot air return for the air conditioning units. This solution is better for the building AC system but can be worse for the equipment. The trouble is that most rack-mounted equipment is designed for front-to-rear airflow, not a bottom-to-top airflow. The result can be improper cooling within the rack/enclosure.

7. Protect IT equipment from unauthorized access.

As mentioned earlier, nearly one-third of data loss incidents are caused by human error. A human flipped the wrong switch, bumped into or spilled something, tripped over a power cord, dislodged or misrouted an equipment cable, touched a sensitive component while carrying a static charge—or otherwise misused the equipment.

And that's just the accidental incidents. What about intentional misuse of equipment—and theft? Today's high-dollar servers are so compact that they could be removed from the building in a briefcase. When you consider the magnitude of the IT investment, and the value of the data and applications that ride on it, you can appreciate the critical importance of protecting it from unauthorized access.

Enclosures provide access control options such as lock-and-key, electronic control, RFID local readers and access cards. You can devise an access-control strategy to match the requisite level of security. For example:

- Keys can be matched to individual cabinets, multiple cabinets of a certain type (such as containing networking equipment, telephone company equipment or servers), or any other combination desired.
- Electronic control can provide multiple types of access, such as remote control, timed control, card reader control or a combination of all of these methods.

Diversified access-control strategies enable you to manage access at the level of function and/or individual, while a top-level administrator keeps a master key.

8. Manage cables for efficiency and airflow.

Cable management is easy to overlook but important in the overall welfare of the IT system. With IT devices smaller than ever —often served by duel or triple power supplies—a single rack of equipment might produce 40 or more power cords to manage, plus associated service cables and patch cords. Poor management of these cables can lead to damaged cables, performance degradation and costly downtime. On the other hand, good cable management prevents those risks and makes it easy to manage a constantly changing environment. Proper bundling and routing provides easy access and identification for these changes—and eliminates the potential havoc caused by re-routing the wrong cables.

Secondarily, proper cable management is required to maintain the proper thermal control that we discussed earlier. Keeping cables out of the way of air flow maximizes the cooling ability of the enclosure. Therefore, the rack or enclosure should be designed for good cable management practices. For example:

- Open, unobstructed side and bottom channels provide easy access to cables.
- Access holes in the roof of the enclosure support overhead cable management.
- Cable accessories make it easy to separate, organize and protect cables.
- Power distribution units (PDUs) distribute power throughout a rack or enclosure, so you don't have a tangle of power cords feeding to utility sources.

To minimize accidental misrouting of cabling, it's a good idea to segregate cables by type of cable, service and source/supply.

9. Protect IT equipment from environmental hazards.

The performance and lifespan of IT equipment can be compromised if the environment is dirty, damp, hot or insecure. How hot is it inside the enclosure? Did a technician leave the door open? Is condensation putting equipment at risk? Did a blown capacitor spill acid? If your IT equipment is out of sight, you won't know.

Consider a UPS that inter-works with an environmental monitoring probe. With this plug-in device and a standard Web browser, you can monitor the ambient temperature and humidity of the remote environment where the UPS is located, as well as the status of additional contact devices, such as a smoke detector or open-door sensor. When user-defined thresholds are exceeded or contact status changes, the probe automatically logs the event and notifies key personnel by email, mobile phone, or pager.

10. Proactively monitor the operating environment.

Although UPSs are typically rugged and reliable—some delivering a useful life of 20 years or so—they do require ongoing monitoring and support. Power management systems continuously monitor and diagnose the state of the grid, batteries, and power sources, together with the condition of the UPS's internal electronics.

Some management systems also provide predictive analysis of potential trouble (for example, current leaks that foreshadow the imminent failure of a capacitor or the insulation on a wire) and automated notification and alarms through email, pagers, and the Web.

Add another layer of protection with comprehensive service plans that offer preventive and corrective maintenance, with remote monitoring and 24x7 service availability.

Bringing IT all together
Representative strategies for power, cooling and security.

Even within your air-conditioned offices, it's a tough world for electronic equipment. Utility power cannot be taken for granted. Neither can other elements of the IT environment. But businesses of all sizes can take 10 proactive steps to create a secure environment for IT equipment.

Here are some recommended combinations of approaches for businesses of different sizes:

Business Size	Power protection	Thermal dissipation	Security
Large business (1000+ employees)	• Facility-wide central UPS • Data center UPS • Individual distribution within racks • UPSs for PCs	• Computer room air conditioning • Floor and ceiling plenums	• Controlled access to data center • Possible controlled access to building
Medium business (100-999 employees)	• Local UPS to support the equipment room • Individual UPS within each rack/row	• Possible room air conditioning • Supplemental enclosure assistance or fan	• Possible controlled access to data center equipment room • Locking access enclosures
Small business (1-100 employees)	• Individual UPS within each rack	• Building central air conditioning • Supplemental enclosure assistance or fan	• Locking access enclosures

With judicious decisions about cooling systems, environmental control, power protection, cable management and monitoring systems—integrated into a well-configured rack or enclosure—you can reduce costs and downtime while resolving the most common threats to IT systems.

About Eaton

Eaton is a global leader in electrical control, power distribution, power protection and industrial automation products and services. Through its Power Quality Solutions Operations, Eaton delivers a broad range of infrastructure solutions for your IT systems:

- **UPS products**—Rackmount and freestanding power protection systems for applications from the simplest desktop to the largest government, healthcare or industrial facilities.
- **Enclosures**—Attractive, secure and functional enclosures for data centers, wiring closets, office environments and warehouse spaces.
- **Power distribution**—Rackmount ePDUs to streamline the distribution of power throughout a data center, rack or enclosure.

- **Power reliability**—Generators and advanced battery technologies to provide backup power, paralleling gear to create redundant UPS configurations, power quality audits to assess and improve power conditions.
- **Services**—Maintenance plans and extended warranties, 24x7 support, remote monitoring and diagnostic services, turnkey project management and electrical contracting and system integration—350+ customer support engineers in North America.

About the author

Carl Walker, Product Manager, Eaton Electrical, Power Products Division

Carl Walker, BSEE, is product manager for Eaton's Power Products Division, managing Single Phase Series 3 and Series 5 UPSs for IT and telephony markets. Carl has more than 25 years of experience in power protection applications and has contributed to articles to industry publications such as *Electrical World Magazine* and NCTA (National Cable Television Association)

For more information, contact Carl at carlwalker@eaton.com or 619.692.6557.

* www.cbsnews.com