Liebert®

THE 2004 LIEBERT AVAILABILITY REPORT

EMERSON™
Network Power

Introduction

How are factors such as increased connectivity and the convergence of voice and data impacting computer system availability requirements? And how are network and facility managers responding to these changes in light of demonstrated weaknesses in the U.S. power grid and rising equipment densities?

Those are the questions addressed by the benchmark Liebert Availability Survey. Results of this survey are presented in this report.

More than 500 professionals with responsibility for evaluating, specifying or purchasing systems that impact computer and network availability responded to the survey. Of the respondents, 49% represented companies with 500 or fewer employees, while 51% represented companies with greater than 500 employees. From an industry perspective, government and manufacturing were the best represented at 16% each, followed by information technology (11%), healthcare (10%), service (8%), and financial (7%). Other industries were represented by 5% or fewer of respondents.

Defining Availability Requirements

Availability refers to the percentage of time a system or network is available and capable of doing productive work. It is typically described as an annual percentage or number of nines. For example, a 'three nines" system is available 99.9% of the time, which translates into approximately 8.8 hours of downtime annually. Following is the amount of downtime per year represented by different levels of availability:

99%	87 hours
99.9%	8.8 hours
99.99%	52 minutes
99.999%	5 minutes, 20 seconds
99.9999%	31.5 seconds
99.99999%	3.2 seconds
99.999999%	.32 seconds
99.9999999%	.03 seconds

For IT systems, availability is a function of both the availability of power and the availability of network hardware and software ("netware"). Consequently, "total availability" is determined by multiplying power availability by netware availability.

Throughout the survey, respondents were asked to base their responses on how the question applied to critical systems. Critical systems are defined as those on which the organization relies to conduct business.

Total availability is determined by multiplying power availability by the availability of network hardware and software

The first question in the survey asked respondents to ***define the availability goals for their business critical computer systems.*** More than half (52%) indicated availability requirements of five nines or higher (less than six minutes of downtime per year). Results for this question are represented in Figure 1.

The follow-up to this question asked respondents to identify ***how the availability goal for their critical systems has changed over the last two years.***

Only 3% of respondents indicated that their availability requirements had gone down

during that time. Forty-one percent (41%) said their requirements stayed the same. If you remove the 26% of respondents that indicated that their requirements were already at 100%, only 18% of respondents are not experiencing pressure to increase system availability. Fully 55% of respondents said that availability requirements had increased over the last two years.

55% of respondents indicated that computer availability requirements had increased over the last two years

When asked to identify ***what is driving the change in availability requirements***, four factors were cited most frequently

- User expectations
- Increased network dependency
- Customer/partner requirements
- Escalating downtime costs

Barriers to Achieving Higher Availability

Respondents were asked to ***identify the barriers that are preventing them from achieving higher levels of availability.*** This was an open-ended question that elicited a wide range of responses; however, cost was by far the most frequently cited barrier.

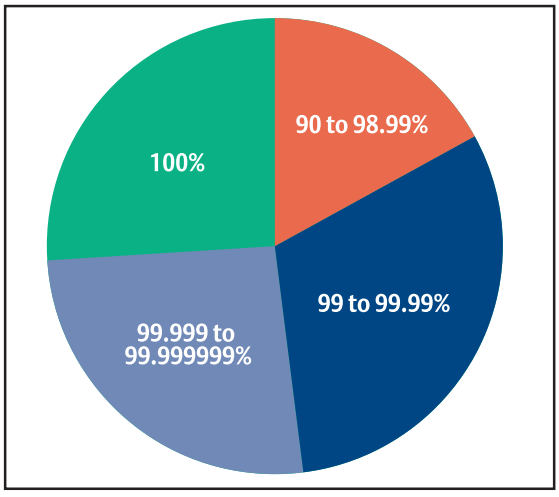

Figure 1. Defined availability goals for critical systems.

Respondents recognized that achieving higher levels of availability requires an investment. The investment may be in new servers, UPS redundancy or new security systems, but, for the most part, respondents felt there was little they could do to elevate critical system availability using only existing systems. .

Cost was followed by hardware software/ problems, maintenance-related downtime, and problems with network connectivity. The fact that so many different issues were identified by at least ten respondents each illustrates how many factors must be managed to keep network systems available. Top results for this question are listed based on frequency of response.

- Cost
- Hardware/software problems
- Maintenance
- Connectivity
- Lack of backup generator
- Space
- Lack of management support
- Human error
- Security

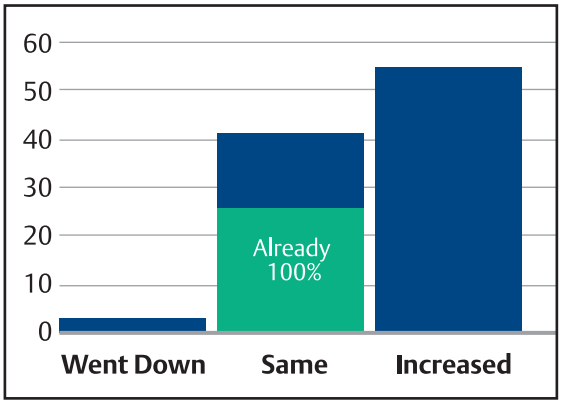

Figure 2. How has critical system availability changed over the previous two years?

Raising Availability: *Power System Redundancy*

Power system availability must be 100 times greater than the availability of network hardware and software to prevent the availability of power from negatively impacting total availability. High levels of power availability are achieved through redundancy. At the UPS level, this is accomplished through either N + 1 or 2N redundancy. Both allow any single UPS module to fail or be taken offline for maintenance without impacting the operation of the UPS system. N + 1 systems share a common power distribution unit and so include a single point of failure. Also, if too many UPS modules are used in an N+1 configuration, availability can be compromised. The 2N approach eliminates single points of failure and allows higher levels of availability to be achieved.

The difficulty of raising availability was also illustrated in the next question, which asked respondents to ***judge the likelihood of downtime from the following factors***:

- Software failure
- Hardware failure due to equipment age
- Hardware failure due to heat/humidity
- Power interruptions/failure
- Human/operator error
- Viruses or other security breaches

Seventy-nine percent (79%) of respondents considered downtime from human error to be possible or highly probable – the highest of any factor. This is in contrast to the small percentage of respondents who identified human error as an obstacle to achieving higher levels of availability in the previous open-ended question. This indicates human error may be a "forgotten" factor that deserves more attention in terms of system design and personnel training. Although human error will never be eliminated, its impact on availability can be minimized by reducing power system complexity and providing more thorough training.

Downtime from viruses, equipment age, software failures and power outages were also considered possible or highly probable by a majority of respondents. Results for this question are shown in Figure 3.

Downtime from human error, viruses, equipment age, software failures and power outages were considered possible or highly probable by a majority of respondents.

Measuring the Cost of Downtime

The next question in the survey asked respondents to identify the average cost per hour of downtime within their

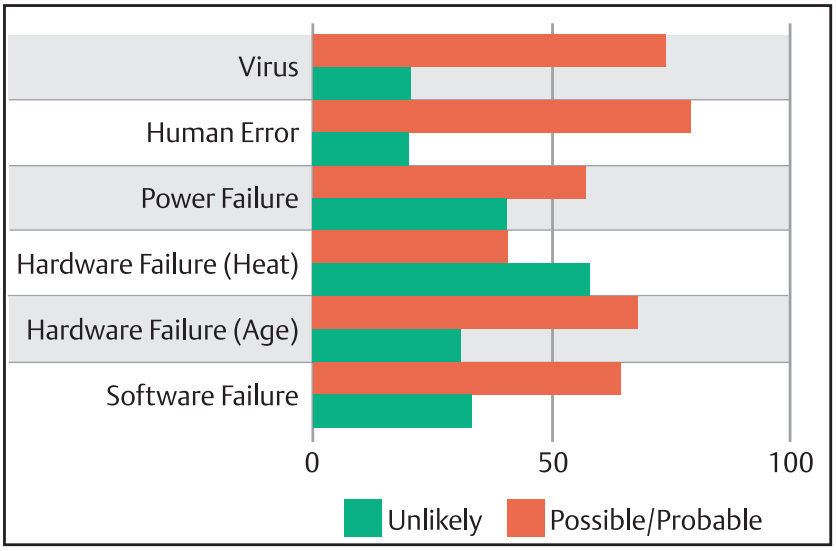

Figure 3. The probability of occurrence for various causes of critical system downtime.

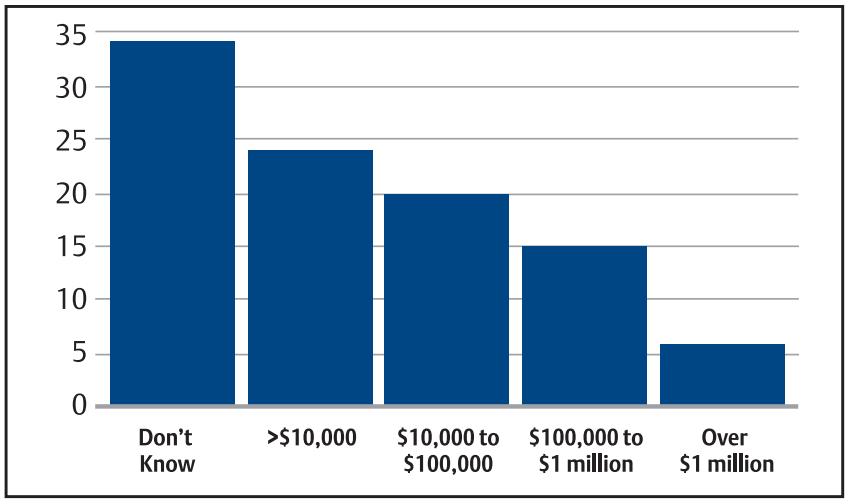

Figure 4. Average cost per hour of downtime

Computer system availability depends upon a variety of factors...Many of these are firmly within the traditional realm of the IT manager, while others have been managed primarily by facilities managers.

organization. Responses were distributed fairly evenly from under $10,000 to $1 million, with 6% of organizations having costs per hour of greater than $1 million.

Significantly, 34% of respondents indicated they did not know the average cost of downtime for their organization. Results for this question are shown in Figure 4.

Who Is Responsible for Availability?

Clearly, computer system availability depends on a variety of factors and systems, including computer system hardware, operating and application systems, security systems, and power and environmental support systems. Many of these are firmly within the traditional realm of the IT manager, while others have been managed primarily by facility managers. Consequently, respondents were asked to ***identify who has responsibility for critical system availability in their organization.***

Raising Availability: *Understanding Downtime Costs*

Knowing the cost of downtime makes it easier to justify investments required to achieve higher levels of availability.

Also, downtime costs should be considered relative to overall operating revenue or profitability. A loss of $30,000 due to power-related downtime is relatively insignificant for an organization with annual operating revenue of $3 billion. That same loss may prove very significant to a business with an operating revenue of $3 million.

Not surprisingly, IT management bears the brunt of the responsibility, although facility managers are still "highly or ultimately responsible" in the majority of organizations represented by the survey.

Facility managers assume some responsibility because they often specify and manage power and environmental systems within a building, including those that support critical systems. Results for this question are shown in Figure 5.

The follow-up to this question addressed ***the level of involvement in specifying the support systems that computers depend on for their availability.*** As seen in the results in Figure 6, there is a close correlation between responsibility for system availability and level of involvement in the purchase decision.

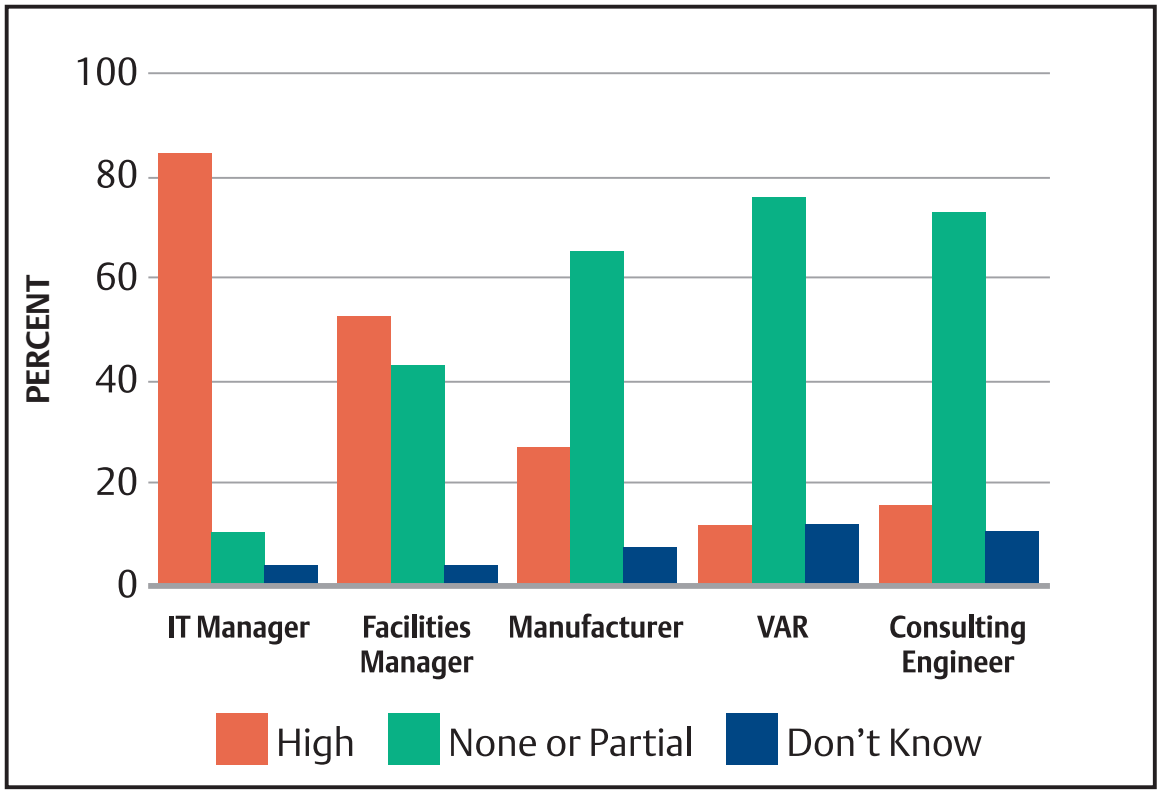

Figure 5. The level of responsibility for assuring computer system availability.

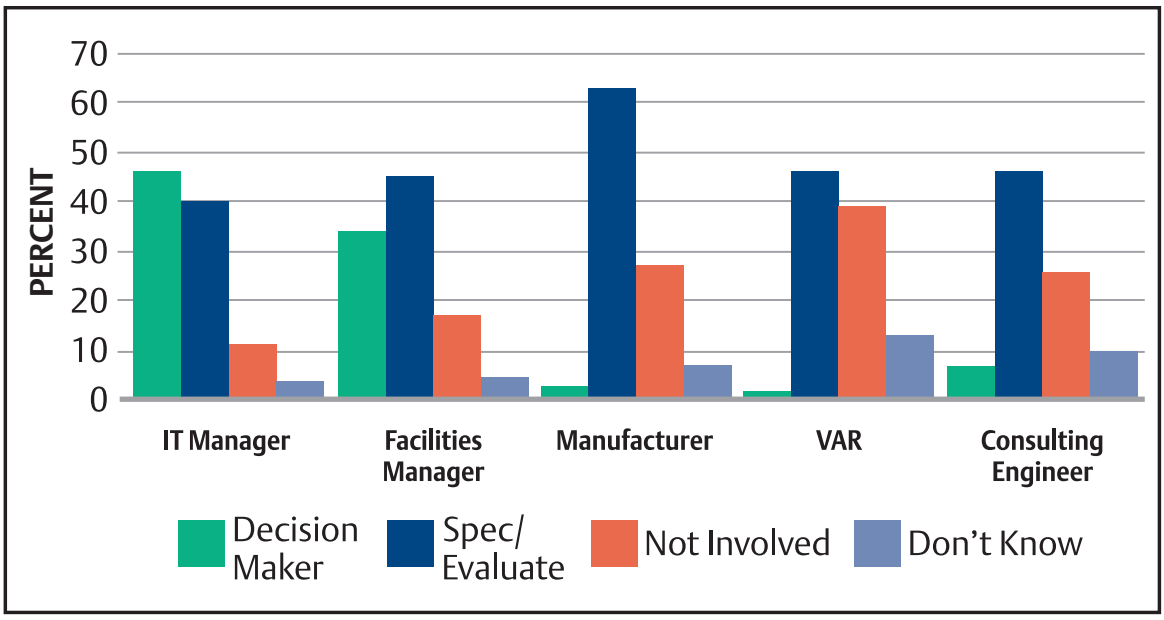

Figure 6. The level of involvement in the specification, selection and purchase of computer support systems.

Raising Availability: *Getting the Right People Involved*

IT managers understand information technology systems. Facility managers understand the electrical and HVAC systems that IT systems depend on to achieve desired levels of availability. That makes coordination and cooperation between facility and IT personnel essential. Ideally, facility management has visibility into the IT planning process and provides support and expertise in regard to power and environmental requirements of new systems as needed by IT. In high availability applications, IT and facility managers work together to achieve business objectives.

Raising Availability: *Online on the Network Edge*

Double conversion UPSs are standard in the data center, but many organizations have opted for lower-level UPS protection on the network edge. This threatens network availability. New business applications and increased connectivity, coupled with more sensitive communications devices, have made online UPSs as important on the network edge as they are in the data center.

The type of UPS impacts the level of protection the UPS can provide.

The Foundation for Computer System Availability

The final questions asked respondents to ***identify the systems currently in place to protect critical systems against power problems and environmental hazards.***

Regarding power protection, 93% of respondents had at least a basic UPS system in place to protect against power disturbances and brief outages. The most common type of UPS used by respondents was the line interactive UPS at 36%. Ten percent (10%) of respondents use passive standby, or "offline" systems, while 22% rely on online double conversion systems. A relatively high 22% of respondents did not know what type of UPS system they had.

The type of UPS impacts the level of protection the UPS can provide. Passive standby systems provide the least protection followed by line interactive systems. Online double conversion systems provide the most complete protection and

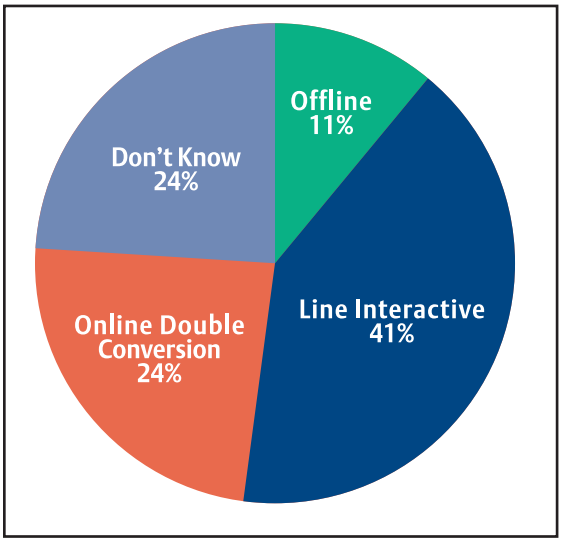

Figure 7. Type of power protection used.

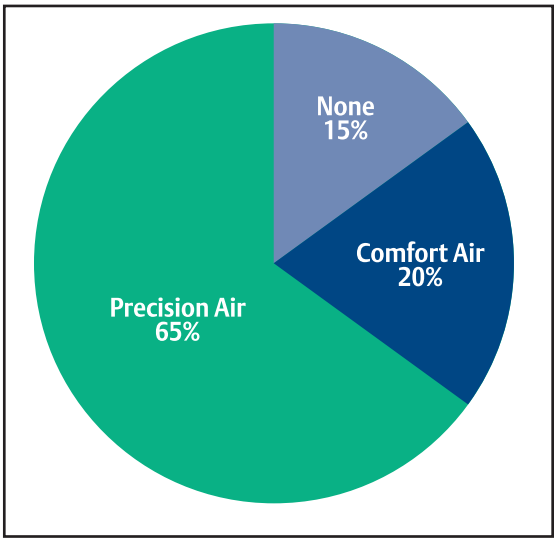

Figure 8. Type of environmental control used.

also provide the best performance working with backup generators. Experts suggest that networks or systems expected to achieve high levels of availability be supported by online double conversion UPS systems.

Regarding environmental protection, the majority of respondents utilized precision air conditioning systems, which are designed specifically for computer system support, rather than general comfort air conditioning. Twenty-nine percent (29%) rely on comfort air conditioning to keep computer systems operating in appropriate environmental conditions. Comfort cooling systems are poorly designed to meet the requirements of computer systems.

Conclusions

Network and facility managers are under increasing pressure to provide higher levels of availability of business critical computer systems, with 26% of respondents already expected to deliver 100% availability. This despite a range of possible threats that include power outages, software and hardware failures and viruses and worms.

A number of barriers were identified; yet a relatively high percentage of respondents (34%) did not know how much an hour of downtime costs their organization. This limits the ability to evaluate the return on investment of systems that could deliver higher availability.

Raising Availability: Managing *Heat: The Quiet Killer*

The effects of heat on electronic equipment are well-known, but often under-appreciated. Every time a computer system operates in temperatures above 85 degrees F., its lifespan is reduced. Relying on building air conditioning to cool computers leaves them vulnerable during times the building air conditioning is shut down, including off-hours and cold seasons. Dedicated precision air conditioning systems are essential to achieving high levels of availability.

Primary responsibility for computer availability typically rests with IT management, although facility managers bear some of the responsibility in a majority of cases due to their involvement and expertise with power and environmental systems that form the foundation for computer system availability.

Opportunities exist within the support system infrastructure of many organizations to reduce the impact of these systems on total availability.

Opportunities exist within the support system infrastructure of many organizations to reduce the impact of these systems on total availability. Upgrading UPSs from passive standby or line interactive to double conversion systems, adding UPS redundancy and using precision cooling where appropriate are all measures that can be taken to help ensure support systems do not negatively impact total system availability.

Real-time support system monitoring combined with a proactive approach to service can ensure support systems continue to provide the levels of availability required to support critical systems in the networked age.

About Liebert

Liebert, an Emerson Network Power company, is the world leader in systems that protect the availability of computers and other sensitive electronics. Liebert delivers unparalleled protection of critical systems through a complete range of power, environmental and monitoring systems that are tailored to application requirements by a network of local representatives that average better than 16 years of experience in the industry. Liebert Global Services is the world's largest service team dedicated to the maintenance and on-site repair of critical computer support systems. For more information on Liebert, visit www.liebert.com.

Emerson Network Power is an Emerson business that provides a full spectrum of reliable power solutions, including inbound power, connectivity, power supplies, power systems and precision cooling, backed by the largest global services organization in the power industry. For more information, visit www.emersonnetworkpower.com.

Liebert Corporation
1050 Dearborn Drive
P.O. Box 29186
Columbus, Ohio 43229
800.877.9222 (U.S. & Canada Only)
614.888.0246 (Outside U.S.)
Fax: 614.841.6022
www.liebert.com

Printed in U.S.A. 0704 WP402