# The Essential Guide to Avoiding Network Outages

A total network outage can be an enormous disruption to an organization, and a stomach-dropping experience for IT executives and network administrators. Quality, speed and latency issues can certainly create trouble in their own right, but nothing compares to the upheaval of a communications-severing outage.

When an outage does occur, rapid service recovery is priority one, of course. Still, as the recovery effort is under way, a question lingers: could the problem have been avoided in the first place?

In many cases, the answer to that question is a resounding yes, according to Avaya research on outage causes.[1] Nearly two-thirds of outages resulting from the top five causes, and more than a third of all outages, could have been avoided by using industry-leading outage prevention practices. These practices, simple to implement and sustain, can dramatically reduce costly downtime and its potential impact on business results and customer confidence.

**Our analysis indicates that adopting industry-leading outage prevention practices can help avoid an average $385,000 revenue loss from an incident.[2]**

## The cost of an outage

Avaya Global Support Services conducted a detailed analysis of clients' emergency recovery service requests that involved actual communications outages over a three-month period. When combined with industry data on outage costs, the analysis indicates that adopting industry-leading outage prevention practices can help avoid an average $385,000 revenue loss from an incident.[2]

[1] Avaya analysis of client data conducted in 2014.

[2] An average 3.5-hour restoration time for specified outages multiplied by $110,000 per hour of revenue loss, based on estimates from "Datacenter Downtime: How Much Does it Really Cost?" Aberdeen Group, March 2012.

Nearly two-thirds of outages resulting from the top five causes, and more than a third of all outages, could have been avoided by using industry-leading outage prevention practices.

According to the Avaya analysis, the top five causes of communications outages — and the percentage of those outages that could potentially have been prevented had leading practices been followed — are:

1.  Power outage — 81%

2. Lack of routine maintenance — 78%

3. Hardware failure — 52%

4. Software bug or corruption — 34%

5. Network issue or outage — 27%

Interestingly, the relatively mundane factors of power and maintenance correlate more highly to the potential benefits of employing prevention practices than the complex mix of hardware, software and networks.

Though not itself a cause, a too common situation can compound the cost of an outage: lack of backups, sometimes for forehead-slapping reasons (see "*That's* why there's no backup?"). Average downtime from an outage requiring a software reinstall, when backups are available, is 2.4 hours. When backups are not available, average recovery time is 38 hours (more than 15 times longer), potentially adding millions more to outage-related revenue loss.[3]

## Leading practices for outage avoidance

Following are industry-leading practices and tools that organizations can use to reduce the potential for outages:

**1. Power outages.** Uninterruptible power supply (UPS) units are essential to keeping systems operating through lightning strikes, storms and other power disruptions. But are they adequate? UPS arrays should meet the specifications of the communications and networking systems they support, of course. But as organizations grow, so does the mix of gear relying on UPS systems. Adequate UPS systems, as well as proper grounding of sensitive equipment, are crucial. Audits can help determine if facilities can meet power demands and ward off problems. Your service provider should be able to provide the framework for periodic audits or even help you conduct them. Particular attention can be given to hardware that is approaching the end of manufacturer support (EoMS).

[3] Avaya analysis of client data conducted in 2014.

**2. Lack of routine maintenance.** Just as people understand that failing to eat right, exercise and avoid certain activities can worsen their health, most organizations know that poorly tended systems can fail from lack of proper care. Yet the high percentage of remediable outages (78%) attributed to poor maintenance[4] suggests organizations are underutilizing one of the best ways to maintain system uptime—upkeep. Most equipment emits telltale signs when a problem is approaching. Proactive health checks, disciplined system monitoring and observed maintenance schedules can aid in hearing the signal, helping improve the reliability of communications assets.

**3. Hardware failures.** Old equipment may chug along today, but it won't forever. Continued use of those "sweated assets" is an increasingly risky gamble with major consequences should they go bust. If replacement parts or equipment are not available immediately when they fail, the length of the resulting outage can be extended significantly while replacements are located and acquired. An organization needn't upgrade everything though. Proactive upgrades of equipment approaching EoMS, audits to verify system redundancy, system health checks, and failover strategies for critical systems can help reduce hardware-based outages.

### *That's* why there was no backup?

The pitfalls in outage recovery can be both painful and shockingly simple. An organization that had installed a CD backup for its communications infrastructure suffered a system-frying lightning strike. Unfortunately, no one had inserted a disk in the backup drive. System alarms issued repeated warnings, but no one either saw or acted on the alerts. (Another common mistake is leaving the same disk in the backup drive and continually overwriting previous data. If system data becomes corrupted, a company can end up overwriting the "clean" backup data with corrupted data, defeating the purpose of the backup.)

Had the infrastructure included sophisticated remote diagnostic technology, such as Avaya EXPERT Systems[SM], Avaya technicians would have been notified within 90 seconds of receiving an alarm generated from an Avaya platform and begun immediate problem diagnosis and resolution. In addition, the backup CD would have been securely in place when the lightning came down.

[4]According to the Avaya analysis.

**4. Software bugs or corruption.** While software vendors constantly release fixes and upgrades into the marketplace, not all organizations are eager to apply them. Some choose to let others occupy the upgrade frontlines and endure potential rollout hiccups, then follow along at a safe interval. This strategy breaks down disastrously, however, when an organization suffers an outage that would have been avoided with a fix it chose to postpone. A sound patching strategy and proactive patching to eliminate known issues can help maintain software performance and avoid software-related outages.

**5. Network issues or outages.** Jitter, delay and latency can be warnings of a possible network outage. In some cases, a simple audit of an organization's underlying network can identify where such conditions exist. A network diagram can prove indispensable in isolating an outage, speeding resolution by illustrating the relationships among pieces of equipment. And rigorous configuration control processes can help ensure that system changes and refinements do not inadvertently trigger outages and other problems.

## The path to outage prevention

The most effective way to deal with an outage is to prevent it. As the Avaya analysis shows, simple steps to address the five principal outage causes can go a long way toward prevention.

In working with clients, Avaya has also found that a comprehensive support services program such as Avaya Support Advantage Preferred, which includes Avaya EXPERT Systems℠ automated remote diagnostics, can dramatically reduce preventable outages. EXPERT Systems auto-resolve 85 percent[5] of alarms requiring service requests without human intervention. If the systems are unable to resolve a problem, they automatically forward relevant information to an Avaya technician. By taking advantage of these advanced diagnostic capabilities, organizations can equip themselves for proactive prevention, rapid resolution and continual optimization of communications systems.

[5]Based on Avaya internal metrics.