

The Causes of Outages

March 2013

There are many published statistics that characterize the causes of downtime. A troublesome aspect of these studies is that they vary all over the place. Though they generally focus on the same vulnerabilities – hardware, software, network, human, and environment, the contributions of each of these faults does not seem to converge into any meaningful numbers.

To add our own input to these studies, we analyzed over 250 outages reported in our Never Again series. The outage reports were all drawn randomly from the press over the last seven years and so should represent a reasonably accurate cross-section of downtime triggers.

Sometimes, an outage is a complex interaction among a primary cause and one or more contributing causes. For instance, if a maintenance technician pulls the wrong board to replace a failed storage-array controller, thus taking down the entire storage array, the primary cause is a human error; but the contributing factor is a hardware fault. The failure of the controller board did not cause the outage. The maintenance technician caused the outage, but he would not have been the cause if the controller board had not failed. We take multiple factors into account in our analysis.

Distribution of Outage Causes

The analysis of our 254 reported outages yielded the following distribution of outage reasons:

Outage Cause	Proportion of Outages
Hardware	15%
Software	19%
Network	21%
People	12%
Environment	21%
Miscellaneous	12%

Distribution of Outage Causes
Table 1

Clearly, none of these causes are predominant. Let us take a closer, more detailed look.

Hardware

All of the hardware outages were caused either by a server failure, a storage-system failure, or a power-supply failure. Their relative occurrences are shown in Table 2:

Hardware Fault	Proportion Of Outages
Servers	65%
Storage	30%
Power Supplies	5%

Distribution of Hardware Faults
Table 2

Software

We separated software failures into upgrade faults (in which a fallback procedure was not successfully executed), failover faults, and software bugs. The distribution of software faults is shown in Table 3:

Software Fault	Proportion Of Outages
Upgrades	30%
Failover Faults	14%
Software Bugs	56%

Distribution of Software Faults
Table 3

Environment

Almost all of the environmental faults were power outages. Other environmental failures were caused by cooling failures, storms, fires, avalanches, explosions, and a sinking building:

Environmental Fault	Proportion Of Outages
Power	72%
Cooling	4%
Storms	11%
Fire	6%
Avalanches	3%
Explosions	2%
Sinking Building	2%

Distribution of Environmental Faults
Table 4

Power outages were generally triggered by the failure of the primary power source followed by the failure of the power backup facilities. Backup failures included generators that wouldn't start, insufficient generator capacity, fuel exhaustion, transfer switch malfunctions, and flooding.

Miscellaneous

The bulk of miscellaneous faults were caused by capacity overloads that took down systems and by cyber attacks:

Miscellaneous Fault	Proportion Of Outages
Capacity	41%
Cyber Attacks	44%
Other	15%

**Distribution of Miscellaneous Faults
Table 5**

Cyber attacks included DDoS (Distributed Denial of Service) attacks, hacking, and malware infections.

The “Other” outages included:

- Two inadvertent fire alarms. One was a false alarm that closed down the data center for four hours. The other destroyed disks due to the high level of noise.
- A theft involving breaking through a building wall and stealing networking equipment.
- A sting operation in which the FBI confiscated all of the data-center servers for several days.
- A set of tapes lost by FedEx.

These are outages that were caused by events that were probably unimaginable.

People

We save “people” for last. Human errors that directly caused an outage accounted for 12% of all outages (Table 1) and included maintenance errors, incorrect operator commands, and poor planning.

However, people were involved and must share the responsibility for many other faults, including failover faults (lack of testing), upgrades gone wrong (improper fallback planning), software bugs (programming errors), power failures (improper maintenance of power backup facilities), capacity planning, and cyber attacks. Given all of the above, our reported incidents indicate that people contributed in some way or another to almost 60% of all outages.

Summary

Based on these results, it seems that a reasonable rule of thumb for the causes of outages is that software, networks, and environmental factors each account for about 20% of all outages. Hardware faults are responsible for about 15% of outages, and people and miscellaneous factors account for 10% to 15% each. Miscellaneous factors are almost evenly split between capacity overloads and cyber crime.

Miscellaneous Fault	Proportion Of Outages
Hardware	15%
Software	20%
Network	20%
People	15%
Environment	20%
Miscellaneous	10%

**An Outage Rule of Thumb
Table 6**

However, even though the human factor directly caused only 10% to 15% of outages, people were a contributing factor in 60% of all outages. Clearly, the weak link in data-center availability is people.

If any of our readers would like a copy of our detailed analysis, in which each outage is characterized and indexed to the Never Again article that describes the outage, please let us know at editor@availabilitydigest.com. We will be glad to share it.

Our thanks to Digest subscriber Keith Evans of Gravic, Inc., for encouraging us to undertake this research.