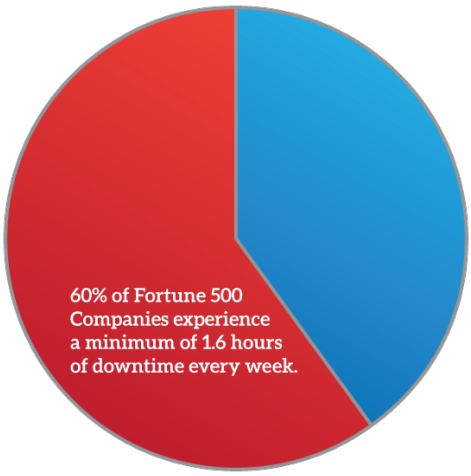
Three Ways System Downtime Affects Companies and Four Methods to Minimize It

Aberdeen Group reports that the average cost of downtime per hour is a staggering $163,674.

Source: Aberdeen Group, (2013, August 16). "Downtime and Data Loss: How Much Can You Afford?" http://www.aberdeen.com/Aberdeen-Library/8623/AI-downtime-disaster-recovery.aspx



A new study quantifies the true effects of downtime on an organization.

Downtime happens. Every organization experiences it with today's unpredictable IT environments. However, the frequency of downtime, and the duration that critical systems are unavailable has become far too acceptable to organizations these days.

A recent Globalscape survey of 283 IT professionals and end users found that nearly 90 percent of organizations have unexpectedly lost access to critical systems, and nearly a third deal with downtime issues every month.

A Dun & Bradstreet study found that nearly 60 percent of Fortune 500 companies experience a minimum of 1.6 hours of downtime every week.[1]

But more alarming than the frequency of downtime is the devastating effect it has on businesses, customers, and employees.

This report addresses the core areas where downtime hits organizations hardest, and outlines four immediate and actionable steps IT executives need to take to improve the availability of their mission-critical systems.

Three Ways Downtime Cripples Companies

#1: The Bottom Line.

When core systems are unavailable, productivity suffers. And while lost files or the inability to send email may not have an "assigned" value, per se—organizations lose money every minute a core system is unavailable.

[1] Arnold, A. (2010, April 20). Assessing the Financial Impact of Downtime. Retrieved from: http://www.businesscomputingworld.co.uk/assessing-the-financial-impact-of-downtime/

Globalscape found that, of the enterprise employees who estimated the financial cost of downtime on their organization, 60 percent said that a single hour without critical systems costs their company between $250,000 and $500,000—and one in six reported that one hour of downtime can cost $1 million or more.

While it's difficult to calculate the exact cost of lost productivity caused by downtime, one thing is certain: the more senior the employee, the greater the financial loss. Of the executive-level employees recently surveyed by Globalscape, 100 percent have experienced downtime, and 56 percent said it happens at least once a month. That translates into big bucks for businesses.

#2: Data Loss.

When critical systems unexpectedly go down, the risk of losing important information and communication increases.

Nearly half of all employees surveyed said they've lost important data and emails when core systems have gone down. The issue is even worse among mid-sized companies: 62 percent of employees surveyed said they've lost data as a result of downtime. And, perhaps surprisingly, senior-level executives appear to be the hardest hit. Of those surveyed, 75 percent said unexpected downtime has caused them to lose important communications and data.

Depending on the type and amount of data lost, the effects can be crippling, affecting everything from sales and customer service to compliance, security, and productivity.

#3. Security and Compliance.

More than 50 percent of IT professionals said their workforce has been unable to send or receive critical and timely files due to system availability issues. Not only is this frustrating for end users, according to 76 percent of IT execs recently surveyed, but it's dangerous, considering the information-sharing behavior of today's employees.

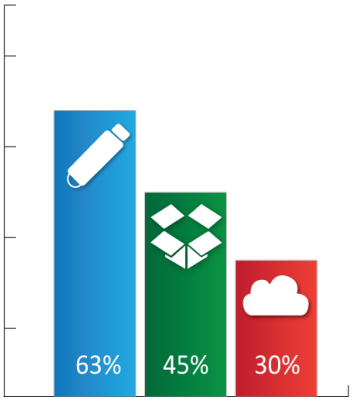
According to the recent report, Dangerous File Sharing Practices Put Sensitive Corporate Data at Risk, when internal technology comes up short, employees regularly turn to consumer-grade tools to send and access confidential information:

> 63 percent of employees have used remote storage devices, like USB drives, to transfer confidential work files

> 45 percent of employees have used consumer sites like Dropbox and Box.net to share sensitive business information

> 30 percent of employees have used cloud storage services for work-related files

When employees use consumer-grade alternatives, frustration and productivity issues quickly evolve into serious security and compliance vulnerabilities, repeatedly putting organizations and their customers at risk.



Downtime Disasters: Active-Passive Clustering Can't Cut It

Despite what end users may think, IT isn't often at fault when core systems go down. More likely, servers become overloaded, shutdown, and require manual intervention before the system is restored.

To avoid this issue, many enterprise IT professionals use active-active or active-passive clustering, but active-passive environments can still leave companies at risk. In fact, survey respondents who have active-passive clustering environments reported losing 34 percent more data and critical emails than those respondents who have active-active clustering environments.

Take Action: The High-Availability Checklist

No IT team can guarantee 100 percent availability. However, there are several steps that organizations can take to minimize downtime and ensure better availability of core systems:

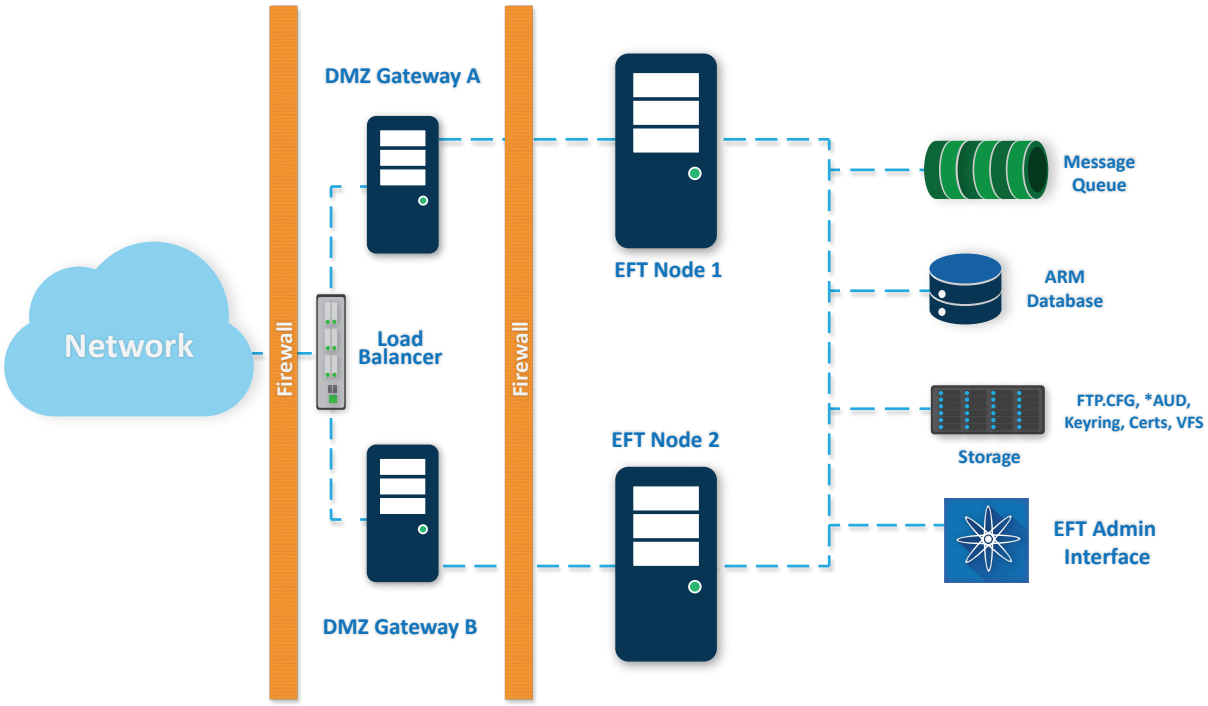
1. *Check the SLAs of all key vendors and partners.* Assess the level of availability promised in vendor contracts, and if it doesn't meet business needs, explore alternatives. If your systems consistently stop short of SLAs, consider implementing an active-active cluster.

2. *Use active-active clustering for all core IT systems.* Active-active clustering environments experience more uptime than active-passive clustering environments, with much less risk. When it comes to core IT systems, ensuring the highest level of availability is essential.

3. *Deploy load-balancing and highly-scalable infrastructures.* The ability to scale and balance workloads across multiple servers is critical to ensuring fast and efficient business transactions. That is, when one node is unavailable, such as when it is performing several actions on the same file, the other nodes can continue to process files.

4. *Rely on a single, managed file transfer vendor.* Using multiple file servers can create system-to-system integration vulnerabilities and issues, heightening a company's risk of downtime and system glitches. Using the same vendor ensures systems and processes are compatible, rather than competing.

Achieving "five nines" availability doesn't have to be a dream with an active-active, highly available cluster implementation.



About Globalscape

Globalscape ensures the reliability of mission-critical operations by securing sensitive data and intellectual property. Globalscape's suite of solutions features Enhanced File Transfer™, the industry-leading enterprise file transfer platform that delivers military-grade security and a customizable solution for achieving best-in-class control and visibility of data in motion or at rest, across multiple locations. Founded in 1996, Globalscape is a leading enterprise solution provider of secure information exchange software and services to thousands of customers, including global enterprises, governments, and small businesses.

4500 Lockhill-Selma Road, Suite 150; San Antonio TX 78249; 1-800-290-5054 (USA & Canada); 1-210-308-8267 (Worldwide)