MegaPath®

WHITEPAPER

HOW DOWNTIME CAN AFFECT YOUR BUSINESS

AND HOW TO AVOID IT

OVERVIEW

Think server downtime is no big deal? Think again. According to research from Forrester only 55% of surveyed companies claimed to have calculated the cost of downtime, and only 18% of those companies actually knew that calculated figure. The average reported total cost of downtime is steeper than you might think. Read on to learn that figure, and more reasons why it is imperative to have a solid solution to avoid server downtime.

Businesses suffering from server downtime are subject not only to potential lost profits, but to lost sales and productivity.

WHAT YOU STAND TO LOSE

The first and most obvious concern for most businesses experiencing server downtime is the potential loss of profits. Small businesses, on average, stand to lose $12,500 per hour of downtime. Their average loss of profit for all businesses per hour is a staggering $212,000. Suppose a business has their server down for an entire 8-hour business day. That represents an average potential loss of $1,696,000 or $100,000 for a small business. That's not the kind of money anyone wants to see go out the window.

Businesses suffering from server downtime are subject not only to potential lost profits, but to lost sales and productivity. Sales employees without access can't make sales, and moreover any employee in a paperless, or largely paperless, workforce cannot get anything done

with success. Server downtime can also bring about the loss of customer satisfaction. Any business that has customers relying on access for purchases, support, services or information, which in the present day is most businesses, also stands to disappoint their customers. Customer dissatisfaction breeds complaints and can lead to loss of business. The final, and perhaps most threatening, potential ramification of server downtime is loss of data. Of all businesses that endure severe data loss, only 6% survive.

So what costs do all these factors tally up to? According to a report from the Uptime Institute Symposium, the average cost of unplanned IT downtime across all industries is about $5,600 per minute. That clocks in at a whopping $336,000 an hour. According to The Huffington Post, the research that informed the paper, "identified costs across 41 data centers in varying industry segments; the data centers studied were a minimum of 2,500 square feet, so as to identify the true bottom-line costs of data center downtime." The same report, entitled "Understanding the Cost of Data Center Downtime: An Analysis of the Financial Impact of Infrastructure Vulnerability," found that the average incident resulted in 90 minutes of downtime, or, a cost of roughly $505,500.

Still, Forrester reports that, of the vast majority of businesses they surveyed, an overwhelming 90% don't know or can't calculate the cost of their most recent disruption. As explained by Forrester, "Infrastructure and operations groups have improved planning, maintenance, testing and actual response, but the overwhelming majority still can't actually measure the cost of a declared disaster." The 10% of the businesses Forrester spoke to that did have a figure for the total cost of their "last disaster or disruption" reported an average total cost of some $10.8 million.

THE BEST OFFENSE IS A GOOD DEFENSE

A 6% survival rate following severe data loss and average total cost of $10.8 million are undeniably ominous numbers. Fortunately, you can protect against, and reduce, disasters, which more often than not are the result of everyday issues and not extreme occurrences.

Of all businesses that endure severe data loss, only 6% survive.

According to the Forrester research, "Most disasters are still caused by mundane events. That headlining disaster that you're watching out for most likely won't be what causes your downtime — instead, it'll be a backhoe operator at the construction site next door who accidentally severs your power or network lines." According to their research, 40% of downtime is related to power station issues, while another 25% is the result of hardware failure, 19% is due to network failure and still another 15% is the result of simple human error. The following practices can be considered a source of basic preventative actions that should be taken by all businesses.

- **File backup:** Backup all of your files regularly. Use both virtual and physical backups so that you have safeguards in place for any situation that might arise. Think of it as the opposite of putting all your eggs in one basket.
- **Avoid power outages:** Logic tells us that we can't defy nature, and that's true. Some power outages are the result of storms and other natural disasters; however, power can fail for other reasons, including insufficient supply. Ensure that you have a reliable power source and follow all proper precautions so as not to overload the circuits. Use power strips to prevent surges and make sure that all your devices and generators don't overheat. If you employ cooling sources, make sure they are just as reliable as your power sources.
- **Have a high-quality, high-speed internet connection:** In a business world that is increasingly, and exclusively in some cases, dependent on internet connectivity, having a reliable and secure connection is essential. Make sure you have a reliable provider. The best providers will offer high speeds, security and guarantees against downtime.
- **Have a resilient, redundant failover solution:** Even the most reliable internet connections will experience downtime. Service level agreements typically reimburse a portion of monthly recurring costs, not the cost of downtime. If your business can't live without your internet connection, implement a failover solution that monitors your primary connection and automatically fails over to a backup connection for high availability.

- **Maintain patch management:** Put simply, patches are security updates designed to fix vulnerabilities. Patch management is how businesses refer to the policies that inform which patches should be downloaded and applied. Following best practices with patch management to boost security and reduce vulnerabilities. Some patch management software solutions are available to assist with patch management.
- **Monitor usage:** The best way to know your power and bandwidth needs is to monitor them constantly. Monitoring usage also allows you to avoid circuit overloads and to truly know that your setup meets your usage needs.
- **Have reliable protection against security breaches:** Make sure you have up-to-date, effective firewalls and anti-malware software in place to protect your system from potential security breaches.
- **Have data loss and intrusion prevention measures in place:** The idea here is to focus not on recovering data, but on protecting your system to a degree that you never have to lose it at all. Discuss the options for protection with your provider or a security consultant
- **Train and encourage staff members to follow all the above methods.**

A reliable provider can help with all of the above considerations and ultimately save businesses money. How? They prevent the loss of money and productivity from downtime, while faster speeds and reliable connectivity result in increased productivity. Equally important is the fact that your in-house IT staff can focus specifically on internal concerns while your provider keeps things running smoothly. According to Boundary, the Uptime Institute has a methodology designed specifically to aid with making important business evaluations and decisions. The methodology, referred to as FORCSS, measures six key factors in business decisions to ensure an effective investment evaluation for any business. The six considerations are: Financial, or the cost requirements involved; Opportunity, or the ability of what is being considered to fulfill demand over time; Risk, or the potential for negative business impact; Compliance, or verification that what is being considered upholds government and industry standards; Sustainability, or a look at how the service being

A reliable provider prevents the loss of money and productivity. When looking for a provider, you should seek one that offers guaranteed uptime, fast connections, and security.

considered affects the environment; and Service Quality, or how the service being offered is able to meet your needs and requirements. Chances are, any provider that passes these considerations is going to merit consideration to service your business.

While all of the above are extremely valid and important considerations, when selecting a network provider, there are a few additional, specific considerations. When looking for a provider you should seek one that offers guaranteed uptime, fast connections, and security.

As a provider of nationwide business voice, data, network, security and cloud services, MegaPath delivers the technology, resources, and expertise businesses need to compete in today's technology-driven landscape and respond to evolving standards and new security processes.

Take stock of your current data network, server and security setup and ask yourself what vulnerabilities your business has, and how much risk you are comfortable with.

NEXT STEPS

Visit www.megapath.com/security to learn more, or contact a MegaPath Business Consultant today at 877-611-6342.