



fusionconnect.com | 888-301-1721

How Downtime Impacts Your Business

AND HOW TO AVOID IT



OVERVIEW

Think IT downtime is no big deal? Think again.

Forty percent of enterprise organizations indicate that a single hour of [downtime can cost](#) their firms from \$1 million to over \$5 million, exclusive of any legal fees, fines or penalties.¹

But IT Infrastructure clearly isn't a business' only concern, with technology infrastructure now spread out far beyond the traditional office location. Today's connected enterprise encompasses SaaS applications, access and traffic across data centers, branch offices, and hybrid- and multi-cloud environments, as well as [a hybrid workforce](#)² that is partly—if not mostly—remote. So while downtime continues to be a very real and potentially expensive, today, IT and business leaders must think about and plan resiliency and recovery for a technology infrastructure that is much broader, far-reaching, diverse, and extensive than even a decade ago.

While large businesses typically have some “cushion” to help them weather a temporary loss of connectivity, power, SaaS vendor downtime, or other type of disaster, the stakes of downtime are high, as the world's largest social media company discovered. Continue reading to learn how much this company lost in a single outage, and why a solid plan and solution to avoid downtime is so important.

WHAT YOU STAND TO LOSE FROM DOWNTIME

The first and most obvious concern for businesses experiencing downtime is the potential loss of profits.

Based on industry surveys, [Gartner](#) cites the cost of network downtime as \$5,600 per minute, over \$300,000 per hour.³ And, according to 2019 survey by [Information Technology Intelligence Consulting \(ITIC\)](#), “a single hour of downtime now costs 98% of firms at least \$100,000. And 86% of businesses say that the cost for one hour of downtime is \$300,000 or higher.”⁴

Downtime may cause lost profits, productivity, sales, and good will.

Company size is just one factor in calculating loss from downtime. Industry vertical also plays a role. A [survey](#) by ITIC showed that the verticals with the highest downtime price tag—\$5 Million for a 60-minute outage—included banking/finance, food, energy, government, healthcare, manufacturing, media and communications, retail, transportation and utilities.⁵

Finally, business model factors into actual downtime cost. Obviously, the more a business depends on uptime, the more it is affected by downtime. Ecommerce and social media are two familiar examples of business models highly dependent

on uptime. A 14-hour outage in 2019 is estimated to have [cost Facebook](#) \$90 million.⁶

That's obviously not the kind of money anyone wants to see go out the window. Businesses suffering from 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.

System downtime can also bring about the loss of customer satisfaction, and erosion of trust. 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 downtime is loss of data.

Of all businesses that endure severe data loss, [only 6% survive](#).⁷

WHAT COSTS DO ALL THESE FACTORS TALLY UP TO?

According to a report from an [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 per hour.⁸

[Another study](#) offers a similar downtime cost. ITIC showed that 86% of firms reported the cost of one hour of downtime as \$300,000, or \$5,000 per minute.⁹

The number can be higher—\$16,700 to \$83,000 per minute—for larger companies according to a 2020 study by the same organization. In this survey, 40% of enterprise respondents said that a single hour of downtime can now cost their firms from \$1 million to over \$5 million – exclusive of any legal fees, fines or penalties.

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.¹⁰ 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.¹¹



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 are often the result of everyday issues, not extreme occurrences. 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.¹²

The Uptime Institute offers a similar statistic for power failures, stating that power outages “accounted for 36% of the biggest, global public service outages tracked by [Uptime Institute](#) since January 2016.”¹³

Other causes Forrester cites include hardware failure (25%), network failure (19%) and simple human error (15%).¹⁴

THE CONNECTED ENTERPRISE AND THE HYBRID WORKFORCE

Technology infrastructure and the workforce have moved beyond and outside the traditional office space. Growing numbers of individuals and teams are flexing where and when they do their jobs.

This new reality requires enterprise IT to deploy, support, and secure a connected enterprise infrastructure that provides technology tools that delivers seamless communications with employees, customers, and trading partners, inside or outside the organization.

Seamless connections rely on uptime.

Increasingly, IT leaders are paying attention to the performance and security of applications, networks, and connections. Here are a few important considerations for IT leaders managing network infrastructure and computing resources in today’s work environment:

- The cost of technology downtime and IT issues could be a larger factor in the hybrid workplace economy. According to one study, [employees report only half of the IT issues](#) they experience.¹⁵ Depending on the severity of the issue, remote workers in today’s hybrid

workplace, unable to walk down the hall for help, might be less likely than office-bound counterparts to reach out to IT to report an IT issue or get help resolving it. This could mean losses in productivity.

- Failures at third-party cloud, colocation, and hosting providers, when aggregated, are now the [second most commonly cited reason](#) for IT service failure.¹⁶
- A study by [Vanson Bourne](#) of Help Net Security revealed that IT challenges and poor digital work experiences actually cost businesses tens of millions of dollars in lost work time.¹⁷

STEPS TO RESILIENCY

What steps can businesses take? Below are several basic preventative actions.

- **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.
- **Avoid power outages.** 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 prevent devices and generators from overheating. 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 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.
- **Ensure secure connections.** Today's connected enterprise typically consists of a remote workforce, widespread adoption of software as a service and the broad dispersal of computing and network infrastructure across branch locations, data centers, and cloud providers like AWS, Azure, and Google. Remote workers are often connected to home or public networks, which can create security hazards for the enterprise. Besides the security risks, there are also network performance challenges. Today's IT professional needs to be sure there are secure connections to headquarters, data centers, SaaS, and multi-clouds. They also need to be sure that the network supports business priorities—gives priority to VoIP calls and SaaS applications, for example, and de-prioritizes less important traffic like streaming training videos.



- **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.**
- **Use a reliable provider.** 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.
- **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.
- **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.

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

HOW CAN A RELIABLE PROVIDER HELP?

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 and optimizing the products and services that help you, as a business, make money, while your provider keeps things running smoothly. 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.¹⁸

1. **Financial**, or the cost requirements involved
2. **Opportunity**, or the ability of what is being considered to fulfill demand over time
3. **Risk**, or the potential for negative business impact
4. **Compliance**, or verification that what is being considered upholds government and industry standards
5. **Sustainability**, or a look at how the service being considered affects the environment
6. **Service Quality**, or how the service being offered is able to meet your needs and requirements.

While these six factors are valid and important, when selecting a network provider, also consider if they offer guaranteed uptime, fast connections, and security. As a provider of nationwide business voice, data, network, security and cloud services, Fusion Connect 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, redundancy, and security setup and ask yourself what vulnerabilities your business has, and how much risk you are comfortable with.

SOURCES

¹ *Information Technology Intelligence Consulting* (Jun 2020). "Forty Percent of Enterprises Say Hourly Downtime Costs Top \$1Million"

² George Schoenstein, *Fusion Connect* (Jan 2021). "The Hybrid Model is the Future of the Connected Enterprise"

³ Andrew Lerner, *Gartner* (Jul 2014). "The Cost of Downtime"

⁴ *Information Technology Intelligence Consulting* (May 2019). "Hourly Downtime Costs Rise: 86% of Firms Say One Hour of Downtime Costs \$300,000+; 34% of Companies Say One Hour of Downtime Tops \$1Million"

⁵ *Information Technology Intelligence Consulting* (May 2019). "Hourly Downtime Costs Rise: 86% of Firms Say One Hour of Downtime Costs \$300,000+; 34% of Companies Say One Hour of Downtime Tops \$1Million"

⁶ *CCN* (Mar 2019). "Facebook's Catastrophic Blackout Could Cost \$90 Million in Lost Revenue"

⁷ *Homeland Security Newswire* (Feb 2010). "Gartner: only 6 percent of companies survive longer than two years after losing data" [Gartner Report]

⁸ *The Uptime Institute*, 2017 Symposium

⁹ *Information Technology Intelligence Consulting* (May 2019). "Hourly Downtime Costs Rise: 86% of Firms Say One Hour of Downtime Costs \$300,000+; 34% of Companies Say One Hour of Downtime Tops \$1Million"

¹⁰ Rachel Dines (May 2011). *State of Enterprise Disaster Recovery Preparedness* [White Paper]. Forrester Analyst.

¹¹ Rachel Dines (May 2011). *State of Enterprise Disaster Recovery Preparedness* [White Paper]. Forrester Analyst.

¹² Rachel Dines (May 2011). *State of Enterprise Disaster Recovery Preparedness* [White Paper]. Forrester Analyst.

¹³ *Uptime Institute* (2018). *Data Center Outages are Common, Costly, and Preventable*

¹⁴ Rachel Dines (May 2011). *State of Enterprise Disaster Recovery Preparedness* [White Paper]. Forrester Analyst.

¹⁵ *Help Net Security* (Apr 2020). "The true costs incurred by businesses for technology downtime"

¹⁶ *Help Net Security* (Apr 2020). "The true costs incurred by businesses for technology downtime"

¹⁷ *Help Net Security* (Apr 2020). "The true costs incurred by businesses for technology downtime"

¹⁸ Kevin Heslin, *Uptime Institute* (Jun 2014). "How FORCSS Works: Case Study 1"



THE FUSION CONNECT ADVANTAGE

ENABLING THE CONNECTED ENTERPRISE

Optimize your business communications, costs, and continued collaboration from any place or device, with crystal-clear quality. Securely connect your business locations and remote workers.

LEADING-EDGE TECHNOLOGY

Fusion Connect's optimized platforms leverage leading technologies, meaning seamless integration of solutions across your virtual and fixed technology platforms.

DEDICATED SUPPORT TEAM

Our 100% U.S.-based expert tech support is available 24/7 to keep your business online and available regardless of the situation.

Visit www.fusionconnect.com to learn more.

Or, contact a Fusion Connect Business Consultant today at **888-301-1721**.

