

Axcient

White Paper:  
Calculating the Cost of Downtime  
In Your Business

[axcient.com](http://axcient.com)

## Introduction to Calculating Downtime

With so many potential problems that could cause IT downtime within small to medium-sized businesses, it makes financial sense for SMBs to understand how much outages could cost them. Many SMBs don't realize it, but the average small enterprise loses more than \$55,000 in revenue due to IT failures each year.<sup>1</sup> But these costs are unique to every business.

Knowing specifically how much downtime will cost an organization is critical for understanding what kind of investment in backup and disaster recovery makes sense for its business. Having a solid ballpark number allows these organizations to use cold, hard facts to weigh their economic tolerance for how much data and downtime they can afford to suffer, and to compare it against the investment they'll choose to make in backup and disaster recovery systems.

### 1 | Causes of Downtime

Before delving into costs, it helps to understand what can cause downtime within a typical SMB's IT holdings. Most downtime events fall into two categories: everyday disasters and catastrophic site-wide disasters.

Everyday disasters usually account for 95% to 98% of downtime events at SMBs.<sup>2</sup> As common as these incidents may be, these disasters are far from mundane, so don't let the everyday designation offer you a false sense of security. Sometimes, something as simple as a server crash could cause six hours of downtime for an email system—so while something may be an everyday disaster, that doesn't mean it isn't costly.

These kinds of issues can manifest themselves in a lot of different ways. For example, hardware issues such as fried motherboards, hard drive failures and bad fans and power supplies can all knock out systems for some time. These are typically the most common sources of downtime, accounting for about 55% of resiliency issues within SMBs. Further exacerbating these issues is the fact that even when these systems are covered by warranties, that may not be a guarantee that the manufacturer can actually get a replacement shipped and installed in a timely manner.

Issues such as software or database corruptions or deleted items can also pose hazards. Similarly, connectivity problems from misconfigured networking gear, interruption of Internet access and fiber cuts can also cause meaningful outages. And, finally, lack of redundancy in systems such as firewalls, switches, Wi-Fi components, routers and servers can all contribute to downtime.

In many cases, these problems are triggered by a user error of some sort. User errors are the top causes of downtime for SMBs, causing about a quarter of incidents.

Meanwhile, site-wide disasters happen less frequently—but when they do occur, they have the potential to be ruinous for an SMB that's dependent on its IT resources. These are the types of events that most people immediately associate with the word disaster—catastrophic incidents like fires or floods, or natural disasters such as tornados, hurricanes and earthquakes. When these disasters occur, their effects are rarely isolated to certain systems or servers.

The ultimate lesson is that it is almost inevitable that an SMB will at some point or another face some form of downtime. The question is, how much will these events hit their bottom line? And what kind of investment in business continuity makes sense to offset these potential losses? In order to answer these questions, organizations need to understand how much downtime will cost them when it affects certain systems and hits the organization site-wide. This can then be used to weigh against the likelihood of the downtime and the cost of the preventative disaster recovery measures needed to offset the potential costs.

## 2 | Understanding the Cost of Downtime

Downtime tends to cost organizations most when it hits mission-critical systems or other systems that employees need to do their daily work. So the basic utilities like Internet access, phones and email will all obviously take a toll on the business when they're down. But even when these systems are up, when line-of-business applications, cloud applications or any other system that's needed to book revenue or perform services goes down, a business feels a financial impact.

Those dollars-and-cents consequences tend to be felt both as tangible hard costs and less-quantifiable soft costs. Hard costs include things like lost revenue and customer churn. Soft costs include damage to brand reputation and customer satisfaction due to service-quality degradation.

## 3 | Calculating Downtime Costs

Obviously, soft costs can be extremely tricky to calculate. So in order to come to a reliable estimate of your cost of downtime, it makes sense to focus primarily on hard costs. One simple but effective calculation to be made is the following:

$$(Revenue/workdays\ per\ year) / open\ work\ hours = Revenue\ per\ hour$$

As you make the calculation, be sure to factor in whether downtime would be complete or isolated based on concentration of offices or workplace. So, say you had a healthy midsized company that was pulling in \$20 million per year. The company is open an average of 23 days per month, with about 12 operating hours per day. And about 50% of the firm's mission-critical employees work at company headquarters. To understand the cost of downtime for critical systems at company HQ, you'd start with that simple calculation:

$$(\$20\ million/276\ workdays)/12\ hours\ per\ day = \$6,000\ Revenue\ lost\ per\ hour\ of\ downtime\ company-wide$$

Then you'd account for site specific city:

$$(\$6,000\ per\ hour\ lost\ company-wide)*.50 = \$3,000\ per\ hour\ of\ downtime\ at\ corporate\ headquarters$$

While soft costs are more difficult to calculate, SMBs should still keep these in mind when weighing the risks—when communicating these numbers to decision makers, it helps to verbally explain that these are minimum baseline costs.

Once a downtime hard cost has been estimated, organizations can start to think about their tolerance for downtime or outages. The basic gist of these tolerances is to understand just how much financial impact the organization can absorb without too much business disruption.

An approach with a core offering, plus many customization options, is meant to counter the all-or-nothing dilemma faced with a comprehensive MSP bundle approach.

“We see too many MSPs leaving money on the table,” explains Erik Thorsell, president and founder of Success Computer Consulting, which uses an a la carte approach. “Too many providers overcommit in their pricing bundles and get creamed on their labor costs down the road, when they are forced to perform all sorts of unanticipated but labor-intensive work for clients facing downtime or a disaster.”

A customized model depends on the bundling of additional fee-based services on top of the basic BDR service offering. The idea is to have a core base offering and an extensive a la carte menu that the client and MSP can use to tailor each deployment based on the client’s tolerance for downtime. This approach depends on truly listening to the needs of clients, and tailoring services.

## ABOUT AXCIENT:

- The Axcient Business Availability suite is the proven business continuity and cloud migration solution for Managed Service Providers (MSPs). The Axcient Business Availability suite includes Replifit, BRC, CloudFinder, Anchor, Fusion, and the Axcient Cloud. MSPs and their clients depend on us to protect their data and ensure business continuity in the event of security breaches, human error, and natural disasters. Our focus on partner experience has resulted in more than 3,000 MSP customers throughout the world.

## CONTACT:

Axcient, 707 17th Street, Suite 3900, Denver, CO, 80202 | Phone: 720-204-4500

## FOLLOW US:

