

# Cloud Contingencies: Lessons For Small And Medium-Sized Businesses

September 24, 2024 | Forbes | Kevin Beasley

July's outage involving CrowdStrike provided a poignant reminder of just how dependent companies of all sizes are on their IT systems. For example, some hospitals were unable to move forward with scheduled surgeries, while many flights were canceled, and travelers were stranded across the globe.

For many of us, it would be easy to chalk up the global meltdown of several airlines' systems to a "big business" problem. After all, for an issue to have a far-reaching impact, it needs to affect far-reaching systems.

But now that the dust has settled, I think it's clear that there are plenty of lessons for small and medium-sized businesses (SMBs) to learn about the benefits of contingency planning and the importance of due diligence when selecting cloud providers. This includes asking questions such as if there are outside dependencies that might impact that cloud provider, whether that cloud provider has complete control over all aspects of their cloud and what operating systems and software are used in deployment.

## Planning For Downtime

The aforementioned outage occurred due to a content update.

Though the issue was diagnosed quickly, it could not be pushed out automatically because the affected systems could not boot and required manual intervention.

Here are some tips for dealing with downtime and planning ahead for it:

### 1. Understand your cloud dependencies.

The software ecosystem is filled with interdependencies that can impact software, servers, platforms and, most importantly, your daily business operations. In the case above, some Microsoft Azure users were dependent on CrowdStrike. Users should have had some understanding of the risk. If you understand these dependencies, you can better understand risks and prepare accordingly.

### 2. Build cloud redundancies.

The fact of the matter is that outages can happen. We don't know about it because it might only impact a few users here or there. Eventually, your environment could face one. That's why it's so important to have a backup and, if you rely on a cloud provider, to have in-depth discussions about their

redundancies and backups. Redundancies ensure business continuity during outages.

### 3. Know your update policies.

The companies affected by CrowdStrike's update were those that relied on automatic updates, which can introduce vulnerabilities if not managed properly. SMBs should have policies in place to control how and when updates are applied, ensuring they can test updates before rolling them out to all systems to prevent widespread issues.

### 4. Invest in business continuity planning.

A solid business continuity plan can be exhaustive, expensive and take a lot of time to develop and maintain. They can also have a huge return on investment. If your business cycle is seasonal, for example, think about how much it would cost if your system went down for three hours. Some businesses might do 80% of their business in just one month out of the year. Losing three hours of availability could result in a significant hit to the bottom line.

There are lots of services that can help you do this. Some



cloud providers may also assist with it since cloud adoption is often done to ensure continuity planning. Having a documented plan, however, isn't enough. It's important to run drills and stress-test the system. Doing this will provide you with peace of mind and prove to insurers that your organization has done its due diligence in the event of an outage.

### **Balancing Risk Versus Expense**

A lot of companies may procrastinate or put off preparing for an outage. They might even think it can't happen to them, that it's too expensive or that a few hours or days of downtime is no big deal.

But IT and digital operations have grown to become the heart of business. Contingency planning can't be ignored. Fortunately, a modern IT environment is more robust than it was just a few years ago. Businesses have several options and strategies that can maintain availability: cloud backups for on-premises companies, hybrid clouds and a services ecosystem that includes insurers and disaster recovery consultants.

These processes don't have to be a drain on company finances. Businesses can evaluate their risks, their risk tolerance and the

potential impacts of downtime. But the worst thing that can happen is that an organization doesn't address these issues. While news stories focused on large global businesses during this July's outage, lots of smaller businesses were impacted, and the recovery process for many of them was not easy.

Immediately taking the steps to safeguard your company's operational health is one of the most important investments for the longevity of your company.

As the saying goes, it's better to be safe than sorry.

The Forbes logo is displayed in white serif font on a black rectangular background.