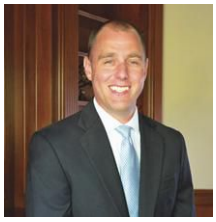
What Happens if Your Colo Fails?

How to protect against disaster.



Tim Kittila is Parallel Technologies' director of data center strategy. In this role, Kittila oversees the company's data center consulting and services to help companies with their data center, whether it is a privately-owned data center, colocation facility, or a combination of the two. Kittila earned his bachelor of science in mechanical engineering from Virginia Tech and holds a master's degree in business from the University of Delaware's Lerner School of Business.

Although a data center network is designed not to fail, it does happen. Sometimes the unexpected and unanticipated does happen. And if it does, it puts "data owners" in a precarious situation — especially when it is a colo that goes down.

As recent situations have illustrated, the ramifications of a colo outage can be devastating. Case in point: two outages in data centers in the UK in July 2016 operated by one of the world's largest communication and colo providers reportedly took down 10% of voice and data traffic in and around London for more than four hours. Unfortunately for the businesses that operated out of those data centers their assumption that they had secured their data in a stable environment unwittingly felt the consequences.

Despite going to great lengths to design and operate data centers to avoid outages, colocation facilities are not immune to problems. Unplanned outages are costly failures for colos in both the short-term and long-term. Many may face one-time financial penalties for not meeting their SLAs, yet also the long-term damage to reputation and recurring revenues if a customer chooses to leave or use the incident as leverage to stay but at a lower rate.

From a colo's perspective, it's a pretty straight-forward discussion on what should (or shouldn't) have been done to prevent these outages. However, it is a different discussion if you are the data owner and your colo solution goes down.

If you've made the strategic decision to colocate your data off-site you've gone through the risk analysis and justified the decision. But have you prepared yourself for the unthinkable? The question is, what to do if you find yourself in this situation?

Preparation doesn't begin and end with the colo selection process. In fact, the best way to prepare for a "worst case scenario" colo failure is to continually address the "possibility." In the event of a colo failure, your diligent preparedness and awareness of the processes will provide you with resources and tools to mitigate the situation. If you haven't already or haven't thought about it recently, I recommend evaluating your situation in the following areas:

Spread it out. First and foremost, when you are developing a data center strategy, we recommend that you do not put everything in one place. Having everything in one place multiplies what I call the "risk factor." It may seem like an obvious statement but it is just as important to not put all the critical applications in the same location. Consider putting production in one location and your back up in another. Then walk through each scenario and identify how a failure of any level will impact production and operations. Repeat this process on an annual basis.

Trust but verify. It may seem basic and obvious but it doesn't happen nearly as much as it should. Get their audit records and more importantly review it. In many cases, colos are audited to be compliant with regulations like HIPAA, SOX, and PCI. However, sometimes boxes are simply checked by people who don't fully understand IT or how data centers must operate. Have an audit done by industry professionals who understand how a reliable data center should operate. These third-party audits are typically minimal in cost when compared to the amount of risk they identify and the wealth of info they can provide. In most cases, mitigating these risks is often minimal in CAPEX and OPEX when compared to overall opportunity cost when an outage is suffered.

Get it in writing. You need to be able to know what they are going to do in order to fix the situation. When developing the contract with a colocation provider, be sure to have written agreements in place that acknowledge what the parties have agreed to in terms of what constitutes an outage. Having a common understanding of the language and what it means is critical. I've heard more than one story of how after the fact the data owner found out that language didn't encompass what they thought it did. Additionally, have in writing the services they provide during a failure and their commitment to rectifying the situation within an acceptable timeframe.

Back up strategy. Be sure to know your business risk and plan for worst-case scenarios. Most colos have an alternate site that can be utilized for basic disaster

> **Despite going to great lengths to design and operate data centers to avoid outages, colocation facilities are not immune to problems. Unplanned outages are costly failures for colos in both the short-term and long-term. Many may face one-time financial penalties for not meeting their SLAs, yet also the long-term damage to reputation and recurring revenues if a customer chooses to leave or use the incident as leverage to stay but at a lower rate.**

recovery back up that will ensure their customers experience little to no impact to operations. Most companies are still chasing the elusive "active-active" database within data centers (colo, cloud, or on-prem). While some are close and claim successful "active-active" data centers, interruption to the production data center almost always will cause some pain while trying to leverage the disaster recovery back-up. Databases are not as complete as you would like and the chances of lost data or application impacts during transition are likely. I just recommend setting proper expectations in lieu of promising the [un-interrupted disaster recovery] world.

Understand (and document) the process. In a failure situation, everyone goes into crisis mode. It is important to understand (and document) how your colo provider handles events such as natural disasters or faulty components. What steps do they take and in what order? One of the key questions is to ask about access and who gets it in the event of a failure. Just like you, your server neighbors will be clamoring for access to their servers in a failure situation. Know precisely, if you'll get access, who has access, when you have access, and what you will be allowed to do if you gain access. Additionally, know exactly what extra security measures will be taken to protect your data during the period of repair.

A vital element of the process is the communication protocol. Open communication is vital to effectively managing the situation and providing your superiors with updates. Know who will be your main point of contact, who you call to get updates, and how often they will be providing you with updates. Additionally, verify the contact names and numbers regularly. Nothing is worse than having an outdated number or former employee on the call list when it matters the most.

Document everything. Documentation doesn't only apply to the colo side of the equation, but all data centers related to an organization's operations. We find time and time again that our customers don't have their processes and procedures for day-to-day operations documented. And if they do, it hasn't been updated as often as it should. Documentation is a critical element to being prepared in the event of a disaster — from knowing where applications are running to knowing what internal stakeholders are most impacted by outages and who needs to be informed of changes.

Ask about dirty laundry. During the evaluation process, most colos tell you about how the systems are put in place to prevent an interruption in service. They also provide you with testimonials and references from satisfied customers. What they don't often tell you about is their "dirty laundry" — specifically instances when there was a failure. As we all know, "oops" happen. First, let them know that their answers will not disqualify them. Then ask them directly if they had a failure in the last year and if so, the details of the failure, how it was rectified, and what steps have been taken to prevent this situation from happening again. You can learn a lot about a colo partner from their honesty as well as how they handled the situation. In situations of crisis, that's when good partners shine.

Know your escape clause. In the event that you lose confidence in your colo partner, it is important that you are aware of any "escape clauses" within your contract. It is important that there isn't any vague language that can be misinterpreted or construed in such a way that you are locked into the relationship.

Be aware of your options. Most colo contracts span several years during which the colo market will continue to expand and new players enter the market. While you might not be currently in the market for a new colo, it is in your best interest to continually evaluate other colos yourself, or use a consultant or broker to review your options with you. And in the event of a failure, you need to be aware of your options for moving to a new solution — should the situation warrant. In some cases, if the failure is significant or long enough, the ramifications could force the colo out of business and leave you scrambling.

Become a data center nerd. In the recent UK colo failure, the cause of the problem was a single faulty breaker. While one would think that critical facilities would not have a single point of failure, the evidence shows it did. Today, we are all in the data business and in your role you need to become a "data center nerd." You need to be on a continual quest for knowledge about not only your data center but also the trends in the market. Be a sponge at all levels.

Ask questions and read reports. Within you data center solution, you need to be intimately familiar with all aspects of the solution. Most importantly, you need to know the potential points of failure and understand what situations might trigger a failure.

Let's all hope that situation never arises. But if it does, you need to be prepared to address your stakeholders and direct your team. The best recommendation is to have a plan during those failure scenarios, and follow the plan. Communication is key to success of this plan. As impatient as people may be, they need to follow the plan. However, communication of how it works before the situation arises is the only way people will know what the protocol is during those situations. By regularly reviewing these key areas, you will have the knowledge necessary to effectively move through the failure. ■