Ebook

The Ultimate Guide to Running Your Business Through Uncertainty and Disruption

A Playbook on How to Overcome Business Continuity Challenges

tierpoint

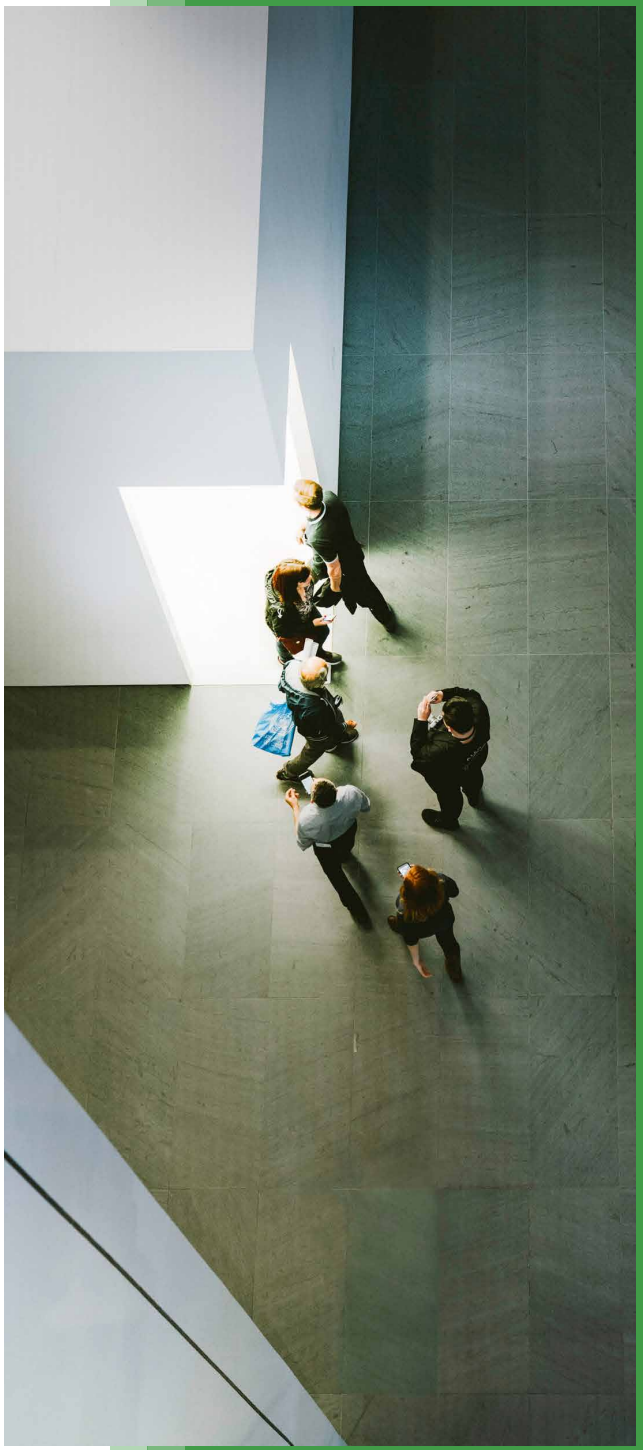
What is Business Continuity?

It's much easier to plan for the best-case scenario business outcomes than it is to prepare for turbulence. However, considering what business continuity means for you is not something you can afford to ignore. You need to have a plan in place for any difficult situations that may arise. How can you get back to "business as usual" under any circumstances with as little disruption as possible?

Your business continuity plan examines the realm of adverse conditions that may occur and is designed to answer the question of how your organization will continue to operate and perform critical business functions despite challenges.

When thinking about an IT business continuity plan, you need to be able to answer questions about how much downtime your business can handle, what data and applications are necessary to keep your operations functional, and how fresh the data in applications need to be in order to be relevant and helpful.

To make business continuity a top priority, you first need to identify what makes it particularly important for your business, what challenges may impact your day-to-day functions, and what you can do to overcome them and get back to work.



Why is Business Continuity Important?

There's never a good time for business operations to grind to a halt. While there may be slower days at your company, what would an average hour of downtime cost you? For large enterprise businesses, an hour of downtime can cost $400,000. On a monthly basis, 35% of businesses at the large enterprise level experience at least one outage. If you want to calculate the average labor cost of your downtime, take the average hourly wage of your staff and multiply it by the number of employees you have. If that sounds like a strain for just one hour of downtime, imagine how that might set you back if you are unable to access your data for hours or days.

Now think about what might happen if your systems go down on a make-or-break day. You've had a huge influx of traffic due to a particularly successful promotion. You just landed that whale of a client. There's seasonal demand for your product or service, and you're trying to stand apart from your competitors. Business continuity can be the difference between success and failure in those moments. You need to understand the potential risks that may impact your business.

tierpoint

What Kinds of Disasters are Causing Disruptions?

Every year, the World Economic Forum publishes a report of top global risks that are affecting the economy. In 2022, some of the global risks that made the list included extreme weather, economic divergence, infectious diseases, and natural resource crises.

Extreme Weather

Extreme weather, the second most severe global risk listed, has increased in recent years. It will continue to increase if the number one global risk, climate action failure, continues. More extreme weather conditions mean your data can be at risk whenever there is a major weather event that can cause damage to data centers or worksites. If your data center is in a particularly vulnerable geographic area, or you don't have redundancy and failover resources, you are putting your business at risk any time extreme weather occurs.

Economic Divergence

The World Economic Forum attributes greater economic divergence to the COVID-19 pandemic, which launched a global recession and continued to widen economic divergence. Countries with lower vaccination rates have also experienced reduced worker productivity and availability, causing a ripple effect on the supply chain and consumption. We are likely to see the continued impact of this divergence for years to come, if not decades. Businesses are starting to look at resilience as an important factor in minimizing costs in an attempt to reduce disruptions to the supply chain. However, any change in business strategy can take a while to fully transition.

Infectious Disease

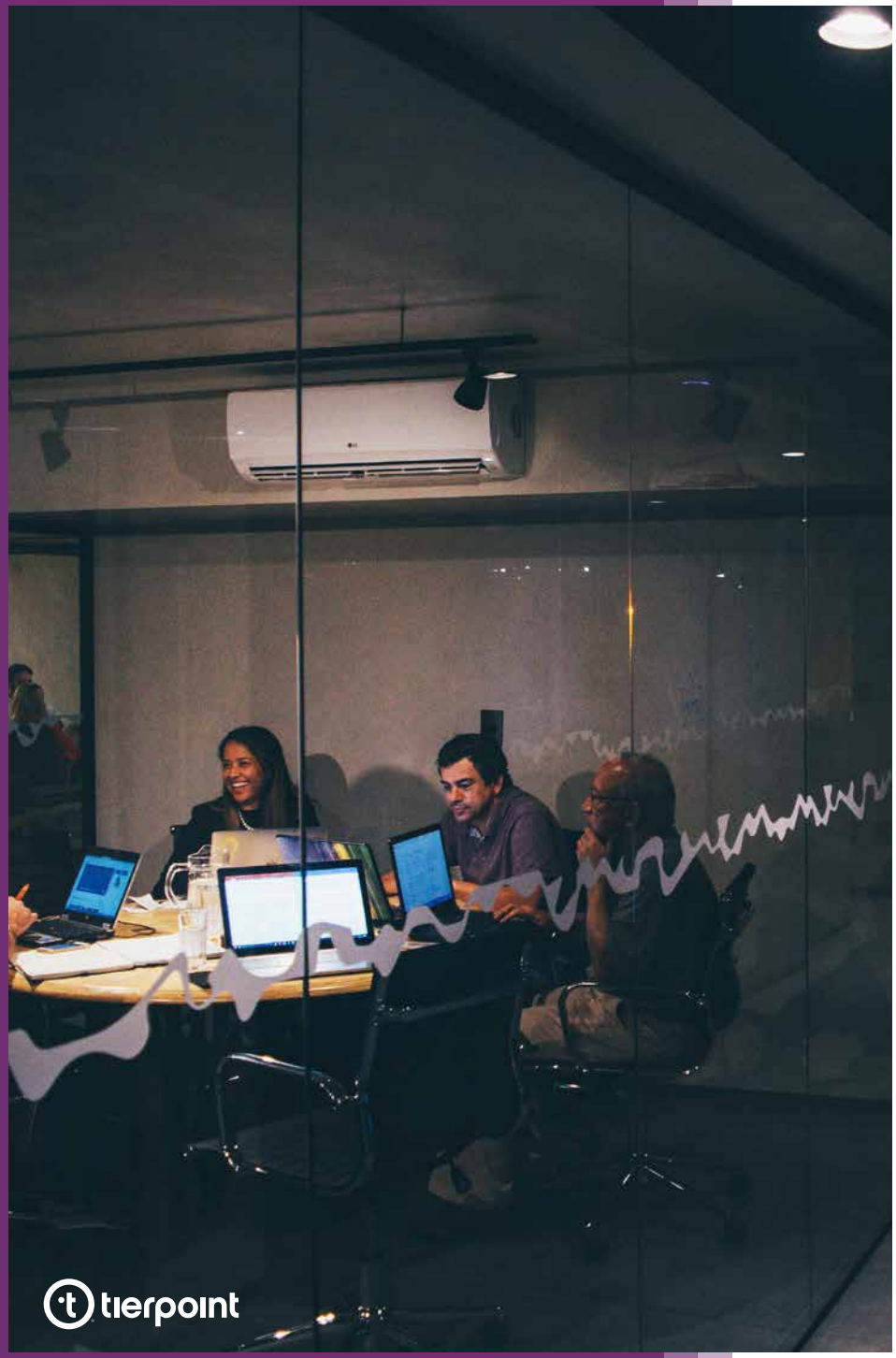
Most recent business interruptions can be attributed to infectious disease, climate risks, or a combination of both scenarios simultaneously. As we continue to navigate our way through an uncertain business landscape, we will see more interruptions to business as usual. Some additional consequences of the COVID-19 pandemic include:

The Great Resignation

The Bureau of Labor Statistics reported that 4.5 million people left their jobs in November, which has been a record high thus far since the start of the pandemic. Approximately 3% of workers voluntarily quit their jobs, topping the previous record set in September 2021. In addition, 1.4 million people were either fired or laid off from jobs, and 377,000 more had some other kind of separation from their jobs during November 2021. While the job numbers are discouraging, not all sectors are experiencing the dip equally. Accommodation and food services jobs had a much larger quit rate (6.9%) compared to finance (1.7%). The information sector was a bit higher than finance, with a quit rate of around 2%.

While the cybersecurity workforce has actually increased in recent years from 3.5 million globally in 2020 to 4.2 million in 2021, the new worker numbers are still not enough to fill the cybersecurity workforce gap, which was at 2.7 million unfilled jobs in 2021. While the gap has improved from 3.1 million in 2020, there is still a significant gap to close. If the Great Resignation picks up further steam, and the information sector experiences higher quit rates, this will continue to be an uphill battle.

"The Bureau of Labor Statistics reported that 4.5 million people left their jobs in November, which has been a record high thus far since the start of the pandemic."



Supply Chain Shortages

Economic divergence has been one cause of supply chain shortages, made worse by the global pandemic. With everyone at home, relying more on their devices, semiconductor demand increased by almost 30% in the period between August 2020 and 2021, with backlogs moving into 2023. Chances are, you've experienced supply chain issues in both your work and personal life. Has it taken 4 months to get the couch you ordered? Are you finding it exorbitantly expensive to purchase new hardware? If you're in the market for new infrastructure and hardware, you may be in for a long wait or may have to pay much more than what the equipment is worth.

Increased Coverage Needs

The workforce is also being affected by an increased need for sick time or time needed out of the office to care for family members or quarantined at home due to exposure at schools or their partner's workplace. While all employers have to think about how to retain current employees, they also have to have a plan for adequate coverage when staff is out, especially if operations depend on physical presence.

Natural Resource Crises

Woven in between many of these disasters are global-scale crises with food, chemical, water, mineral, and other natural resources. These issues can come about because of human overexploitation, critical natural resource mismanagement, or a combination of both. Increased demand, extreme weather, climate action failure, and economic divergence all play into the global risks involving natural resources.

What are Major Challenges to Business Continuity?

With these global risks in mind, here are some of the challenges you may encounter that are the biggest impediments to IT business continuity:

Ransomware Attacks

Ransomware has become easier to administer in recent years. Ransomware as a Service (RaaS), coupled with more workers being at home on less-secure devices, means that your sensitive data is more susceptible than ever to attack.

Cybercriminals who target organizations via ransomware attacks find potential vulnerabilities through methods like spear phishing, infiltrating your system and then blocking the organization from accessing files with a pop-up demand for ransom (lock screen) or scrambling the data so that it cannot be read or accessed (encryption). The goal is to get you to pay the ransom to regain access to your data, a practice that encourages more ransomware attacks if it is successful. The average cost of a ransomware breach to organizations in 2021 was $4.62 million.

Increased cybersecurity risks

In addition to ransomware, the cybersecurity threat landscape will continue to evolve and change. Current and former IBM security experts predict that 2022 will bring attacks on supply chains, a high number of breaches early on, cloud-based malware, and increased triple extortion (which includes data encryption, theft, and DDoS attacks).

Primary and Backup Sites Too Close Together

When an extreme weather event occurs, if your primary and backup sites are too geographically close together, both could be wiped out at the same time, defeating the purpose for a backup site. This is especially risky if your sites are in an area particularly prone to extreme weather, like tornadoes, hurricanes, or earthquakes.

Nonexistent or Improper RTO/ RPO in Place

No business continuity plan is complete without a solid recovery time objective (RTO) and recovery point objective (RPO) in place. The RTO determines what an acceptable amount of time is between the failure of systems to their restoration after a disaster. The RPO defines how much data loss is acceptable to incur following a failure or disaster.

If you don't have both an RTO and RPO in place, or they aren't outlined in a way that helps your business continuity, you need to redefine what they mean and set new standards.

Frequent Outages

Another problem besides close proximity of primary and backup sites is the unpredictability that comes with on-premises data centers. Frequent outages in an on-premises set up, not to mention infrequent or insufficient backups, can cause significant data loss.

Infrastructure Costs

If you're trying to maintain your own equipment and infrastructure, the initial capital expenditure costs can prove to be a significant barrier in the way of having top-of-the-line technology at your on-premises data center. The cost is sure to be higher for at least the next year or two due to the semiconductor shortage.

Building a Business Continuity Plan

When creating a business continuity plan, you should include anything that will help restore normal business operations. This can include communications and operations plans, protocols for employees and clients, and IT protocols.

Communications and Emergency Operations Plans

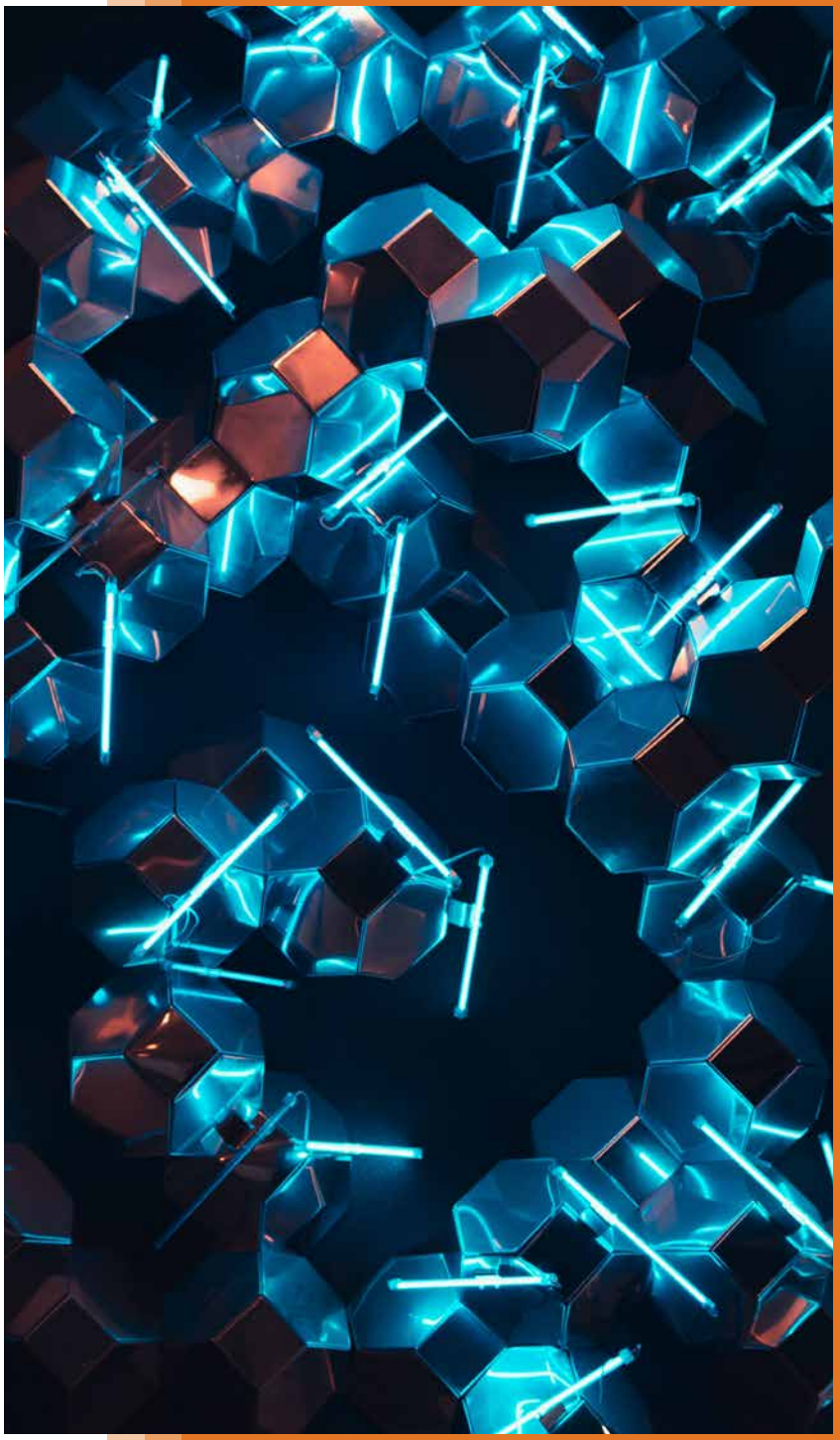
Some public relations firms specialize in crisis communication - planning for how to approach different adverse scenarios that can occur at a given business. Your business continuity plan should include guidelines for both internal and external communications, as well as action steps, for these scenarios. The goal of the communications plan is to set expectations, provide important contact information, and reduce the potential damage that may come from any downtime.

Your operations plan should include considerations for potential legal liability and emergency response protocols. Are there any legal ramifications that could come from a delay in recovery? What happens if you can't deliver as promised to your customers? Your emergency response plans should clearly outline different responses for different scenarios. For example, how you handle a fire will look very different from how you handle a ransomware attack.

Employee and Client Protocol

What should come next is a hit list of the things you need to do, and the order in which they need to be done, to keep running your business under an altered situation. Where will human resources shift their focus? What about IT? How are you going to handle setting up workspaces and virtual machines, and what's the expectation for staff? Is there anything you need to do manually while things are down?

Everyone on staff should know what their marching orders are shortly after a disruption starts. If they are displaced, they should also know where they should be working - does your team move to an alternate workspace, or are they expected to work from home?



tierpoint

How to Overcome Business Continuity Challenges

Figuring out how to communicate a disruption internally and externally and taking the first steps towards operating under less-than-ideal conditions, is just one part of your business continuity plan. Handling the IT challenges that come with an emergency system should be happening alongside the actions listed above. Your business continuity plan should include these IT measures, among others:

Disaster Recovery as a Service (DRaaS)

One major component of your business continuity plan should be a disaster recovery plan. What happens if a natural disaster or cybersecurity attack hits your business? Your plan should cover how you will minimize losses, protect employees, and continue to serve your customers despite adverse conditions. Disaster Recovery as a Service (DRaaS) is designed to help you navigate any potential scenario while you are free to focus on other business matters.

Geographic Diversity

With extreme weather being one of the top risks to your business, having primary and backup sites geographically close together can mean all of your data goes out at the same time. Add geographic diversity to your data center locations. Keep in mind susceptibility to weather in different locations, the whereabouts of your staff and customers, and how failover resources will work between centers.

Tiering RTO/RPO Goals

Lay out your RTO and RPO goals using tiering, and then ensure you will reach your goals with DRaaS. Make decisions on what's most important by asking of each workload:

- **How mission-critical is this workload?**
- **How easily can the data be reconstructed?**
- **What compliance requirements govern this workload?**

Backups and Data Recovery

Having a specific backup plan is just as important as being mindful of the geography of your primary and backup sites. Your backup plan will build on your RTO and RPO goals with the objective of restoring data to a desirable point after a disaster or other data loss event. While your organization may choose to opt into backup as a service (BaaS), and backups do help prevent data loss, they aren't built for quick recovery or application recovery. That's where your DRaaS plan comes into play.

CAPEX to OPEX

Sometimes the only thing standing in between you and more secure infrastructure is the high cost to purchase and maintain new technology. You may want to wait until semiconductor prices go down, or until you feel like your company is in a better position to make a large investment, but your business continuity needs won't wait until a more convenient time. Moving from a capital expense (CAPEX) to operating expense (OPEX) model can help you save money by renting from data center providers who are dedicated to offering the best-in-class technology available in centers staffed by experts.

Testing Regularly

Of course, it isn't enough to build a plan. You also need to test your business continuity approach regularly to ensure you will reach your RTO and RPO goals in a critical time of need. Testing can include walking through the plan to identify gaps and areas for improvement, restoring backups in a test environment, all the way to a full simulation of a disaster. How often you evaluate, and what types of tests you run, will depend on what will help you have the most confidence in your business continuity.

tierpoint

Tools to Help You Stay Up and Running

Now that you're better equipped to handle what may come your way, here are a few more tips and tools to help your business stay up and running:

1. Ensure your employees can work from anywhere by enabling virtual desktop infrastructure. The switch can help with employee engagement, improve digital transformation and cloud adoption, and create an extra layer of security on devices. Perform regular tests to make sure that your virtual private network (VPN) can handle the influx of activity when needed.
2. Move your infrastructure to a data center provider instead of keeping it on-premises. Providers are already prepared to help you with business continuity and disaster recovery plans, and most offer 24/7 staffing for anything that may arise.
3. Use a cloud infrastructure to backup and protect key business data and applications. Backing up in the cloud is good for non-critical data and serves as an extra line of defense in times of crisis.
4. Set solid cybersecurity policies for your organization to prevent cybercrime risks before they disrupt your business. Include cybersecurity training in employee onboarding, regularly test compliance with spoof phishing emails, enroll employees in ongoing training so they can stay up-to-date on the latest threats. Your employees serve as a first line of defense, so make sure they feel prepared to identify suspicious activity.

About TierPoint

A leading national provider of hybrid IT solutions, TierPoint helps organizations drive performance and manage risk. No U.S. provider comes close to matching TierPoint's unique combination of thousands of clients; more than 40 edge-capable data centers and 8 multitenant cloud pods coast to coast; and a comprehensive portfolio of cloud solutions, colocation, disaster recovery, security and other managed IT services. With white-glove customer service, TierPoint professionals customize and manage agile solutions that address each client's unique needs.

tierpoint.com

tierpoint