ITGlue

BUSINESS CONTINUITY PLANNING FOR MSPs

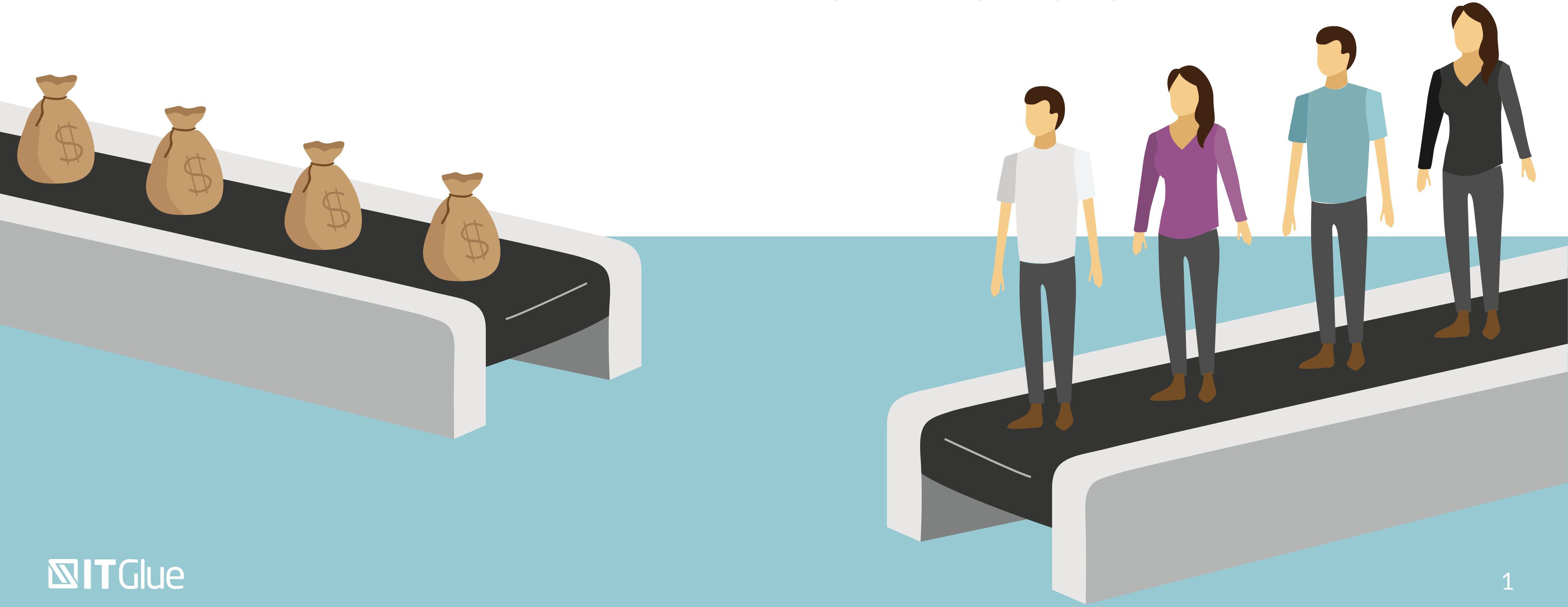
What You Need to Consider

CONTENTS

What is Business Continuity?

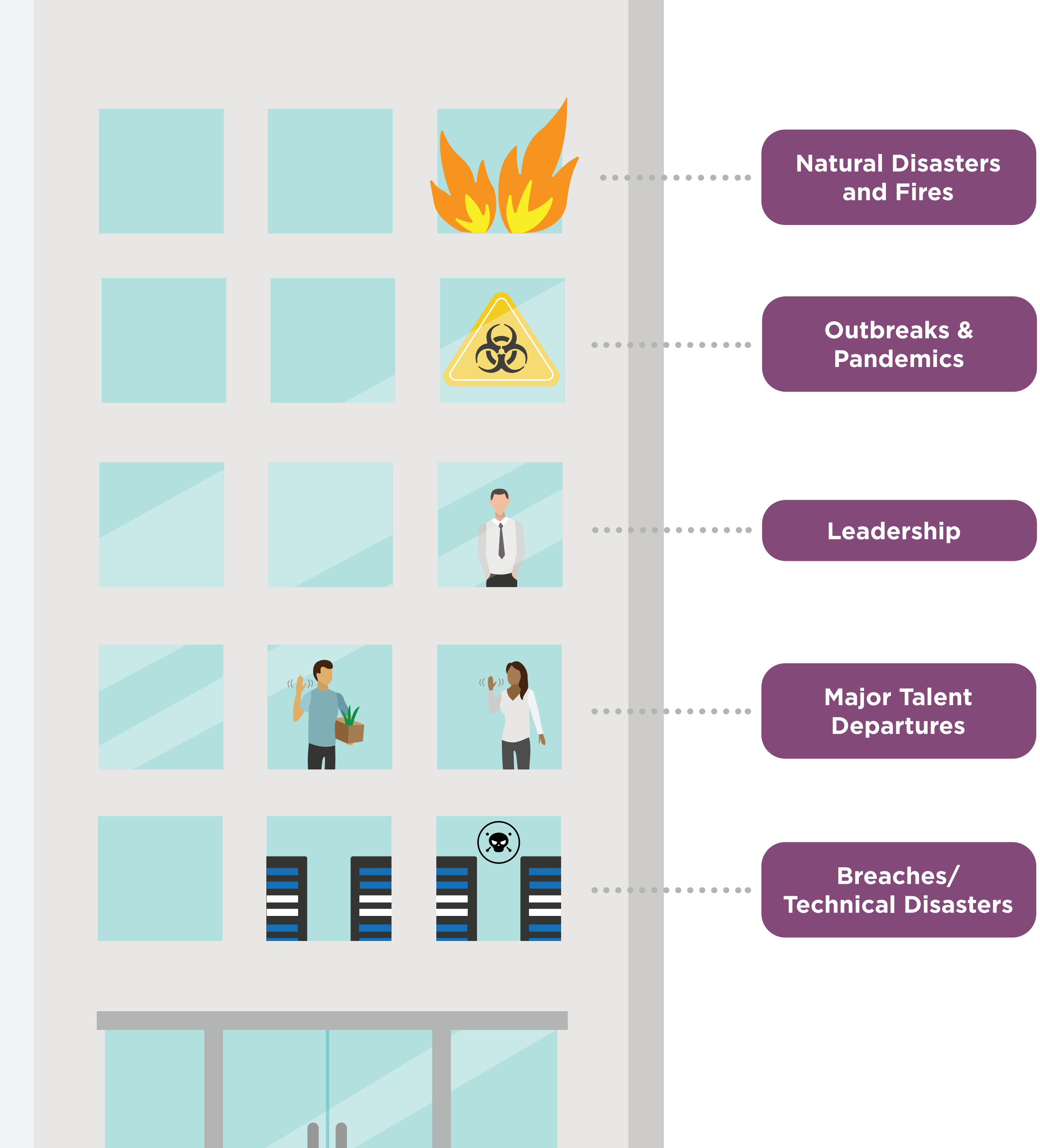
Sometimes it takes a crisis to get people thinking about business continuity. Well, here we are. There's a lot of different things to talk about, but they all come back to the same one or two main challenges: cash flow and people. If you don't have money to keep the lights on, or make payroll, your business is unlikely to continue. Business continuity planning involves thinking ahead to possible scenarios that may hurt your business and creating action plans to help you mitigate challenges before or as they arise.

If you fail to plan, you plan to fail.



There's no such thing as an MSP that's too big to fail, so you'd better avoid failing in the first place. To do this, you need to understand where the critical points of failure are, and address them proactively.

What are the critical points of failure?



Natural Disasters and Fires

Outbreaks & Pandemics

Leadership

Major Talent Departures

Breaches/ Technical Disasters

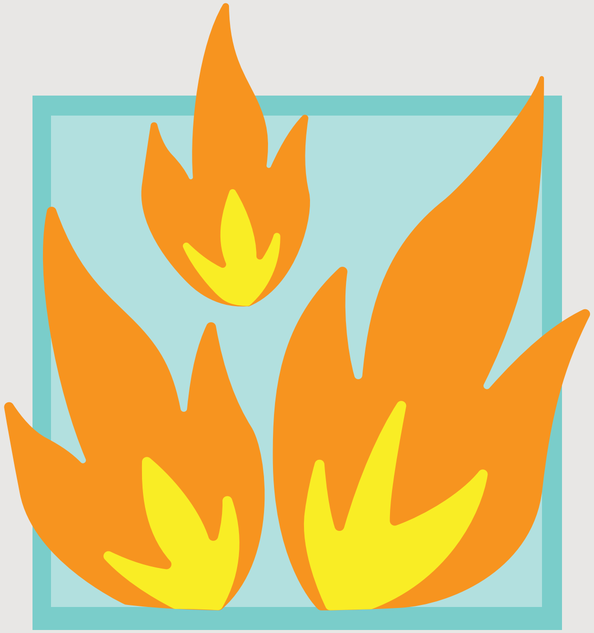
Scenario 1

Natural Disasters and Fires

Whether the existential threat in your area is earthquake, hurricane, tornado, flood or fire, destruction of your premises is definitely a business continuity issue. Insurance is always recommended as a component of business continuity, but a payout isn't the same thing as actually keeping your business running.

If your premises were destroyed, how long would it take to get you back up and running?

The backup and recovery business is huge for a reason, but don't forget to take care of yourself, too. On prem solutions are great if they survive, but do they store everything? Also, on prem solutions don't cover all disaster scenarios — sinkholes, nuclear war, Godzilla attacks or, oh yeah, virus pandemics that make it impossible for your employees to come into the office. Consider supplementing on prem backup with cloud solutions for an extra layer of failover.



Scenario 2

Outbreaks & Pandemics

What we're learning from COVID-19 is that we have to be prepared to institute work from home policies on short notice. This means having it all set up ahead of time, and it also means you can't be dependent on on-premises solutions.

Get everybody on 2FA and SSO as a matter of daily practice.

Have all your procedures, checklists and passwords logged in IT Glue so your team can access them from wherever they are. And make sure to do all this for your clients, too. That means hooking them up with MyGlue so you can share with them what you need, in an instant.

Virus outbreaks also require that you take care of your staff, especially if they are visiting remote work sites. Minimize site visits where possible, and ensure you have stockpiles of masks, sanitizer and other supplies to help keep your people safe.

Proactively map and document any potential workstation environments ahead of time. This will give you a sense of what you're dealing with if you need to swiftly roll out remote work environments.

Scenario 3

Leaders Matter

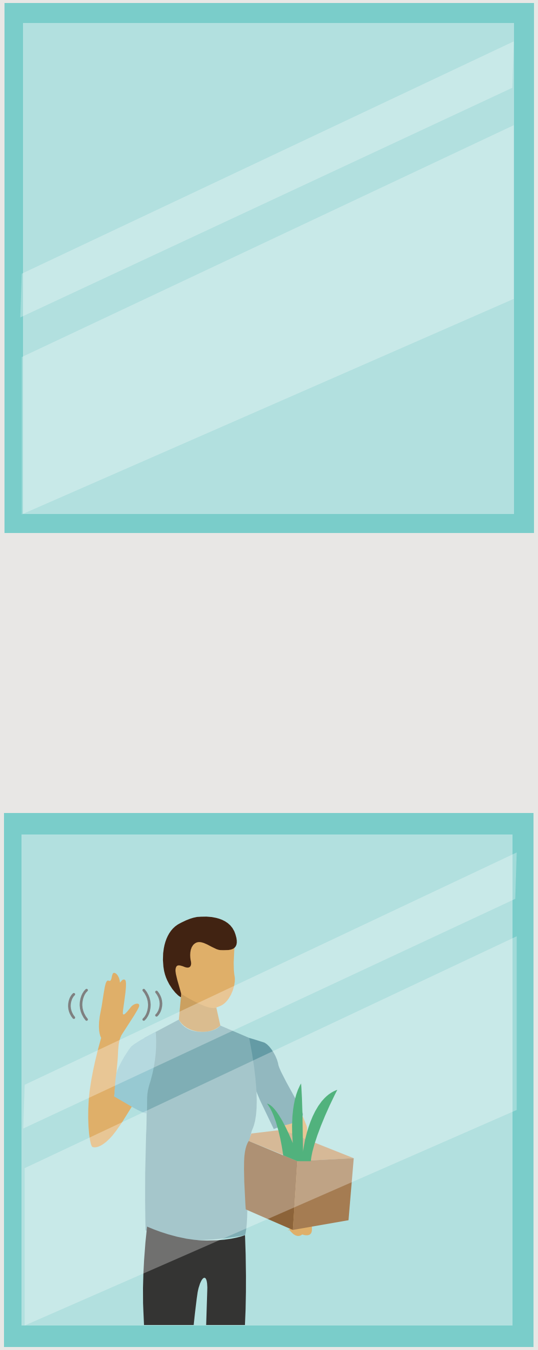
A lot of small businesses have a high level of dependence on their leaders. Some organizations have key person insurance, while others won't let multiple execs fly on the same airplane. For your MSP, there's two things to think about here: succession planning and ownership transition planning. If your exit strategy is to sell, these are the same thing. But that's not always the case. In fact, only 20% of MSPs are able to be sold*.

There's an entire cottage industry of consultants who work with MSPs to make them strong enough to be sold. Many companies in the channel also give away a lot of advice for free on building a better MSP — we do it, too.

But what if you can't sell when you want to exit? You need a Plan B. If you want to retain ownership but turn over the day-to-day operations to someone else, then you need to identify and groom somebody to take over that role. In fact, two somebodies is probably best in case one decides to leave. Overstuff your talent pipeline, and don't be afraid to make your people better throughout the organization.

Succession planning is something you need to do years ahead of time. If you're looking to exit in the coming 24 months and do not have a succession plan in place, this should be a top priority for your business.

** IT Glue 2019 Global MSP Benchmark Report*



Scenario 4

Major Talent Departures

The smaller you are, the more likely you are to be dependent on a handful of people. The barriers to starting your own shop are pretty low, so your best tech could not only leave, but take clients with them. Not cool, but it happens. Not only will this reduce your productive capacity but if they poach clients, your revenue will also take a hit.

Defending against major talent departures and client pillaging starts with making sure your entire team feels valued, can provide amazing service, and has access to the information they need to do so.

It definitely helps if you're able to withstand losing top talent by shrinking the gap between your best people and the rest of your team.

Scenario 5

Ransomware, Breaches & Other Technical Disasters

When MSPs get ransomed, it's not pretty. The demand can be six or seven figures, and they might target your clients instead. Even if you resort to "pay to make it go away", your reputation is going to take a huge hit.

Protect your systems with extensive security training for your workforce.

Lock down systems with multi-factor authentication. There's really no excuse for an MSP to be an attack vector, so ensure that you're 100% up to speed on best security practices and implement them immediately. Have some cyber insurance as well, in case the worst happens and you do need to pay to have your systems unlocked.

There are a number of ransomware simulators available to help you test your action plan. Make sure your action plan takes into account communications with clients, in order to mitigate the impact to them as well.

Resource Management

In a time of crisis, two problems arise with respect to resource management. One is that companies experience a shift in resource deployment priorities. The coronavirus crisis, for example, triggered a rush to set up multiple clients for remote work, then track and secure those environments. But in no crisis is it business as usual. Because of that, you'll probably run into the second problem of resource management, which is shortages of needed resources.

During normal times, you may be motivated to maintain as little inventory as possible, both to free up cash flow and to avoid being stuck with unnecessary hardware. But during a crisis extra inventory allows you to avoid any supply shortages in the market, so investing in a little buffer inventory can more than pay for itself when faced with the unexpected.

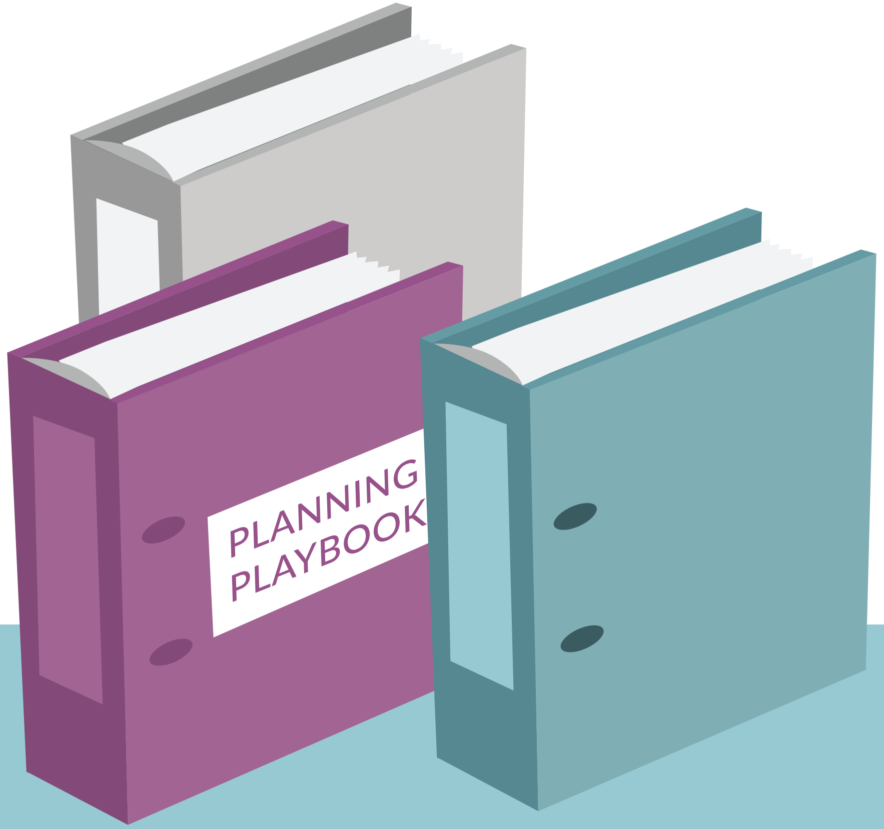
Have Scenario Planning Playbooks

Best practice is that your organization has a handful of playbooks in place, one for each major contingency. These playbooks will help to guide you through that particular scenario, and get you started. Moreover, they provide reference for your entire team, which helps keep people calm and focused.

Don't worry if your playbooks aren't precise — disaster scenarios never unfold the same in real life as on paper. But having a sense of what you need to do will help you move more quickly and make fewer mistakes.

Reviewing your playbooks regularly will also help ensure that they remain relevant to your current business needs and capabilities. The playbooks should always remain aligned with your internal and external environments.

Updating your scenario planning playbooks with lessons learned can also help put you two steps ahead should you be faced with a similar scenario down the road.



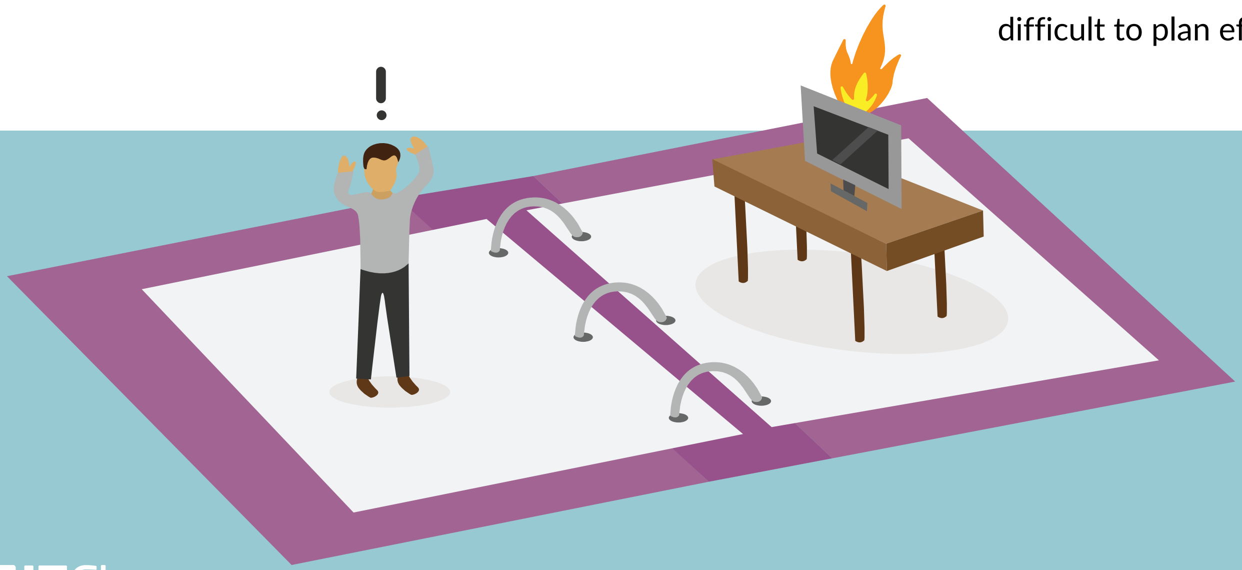
"A good plan today is better than a great plan tomorrow."

– Gen. George S. Patton

Have a Cadence for Evaluating Your Playbooks

While there's no way to practice for disaster that can fully prepare you for when you're in that moment, your playbook has to be more than an abstract concept document. To get there, it is recommended that you run through a simulation or dry run exercise every quarter to help your team understand the different issues that it might face.

Regular reviews of the playbooks and periodic dry runs provide an opportunity for your team to think about these types of challenges, raise issues and devise solutions. This process is absolutely essential, because otherwise when a crisis hits your team will default to the processes that they are already familiar with - processes built more for business as usual than business unusual. Not to mention the additional strain and distracted thinking that occurs during a crisis makes it difficult to plan effectively on the spot.



KEY TAKEAWAYS

- Business continuity strategies relate to the existential risks that can reasonably be predicted
- Business continuity planning should not be optional
- Identify and categorize risks
- Create playbooks for the most likely scenarios
- Conduct regular health checks on your business continuity playbooks
- Use simulations or dry runs to identify challenges, issues and opportunities
- Pre build checklists to help you get organized quickly

The crux of crisis management and mitigation is having structured, easily accessible documentation.

IT Glue's award-winning cloud-based documentation platform can get your MSP documentation in tip top form quickly.

Watch a Demo Now!