BackupAssist™

IT Outage Best Practice Guide

A step-by-step on dealing with planned and unplanned outages.

Introduction

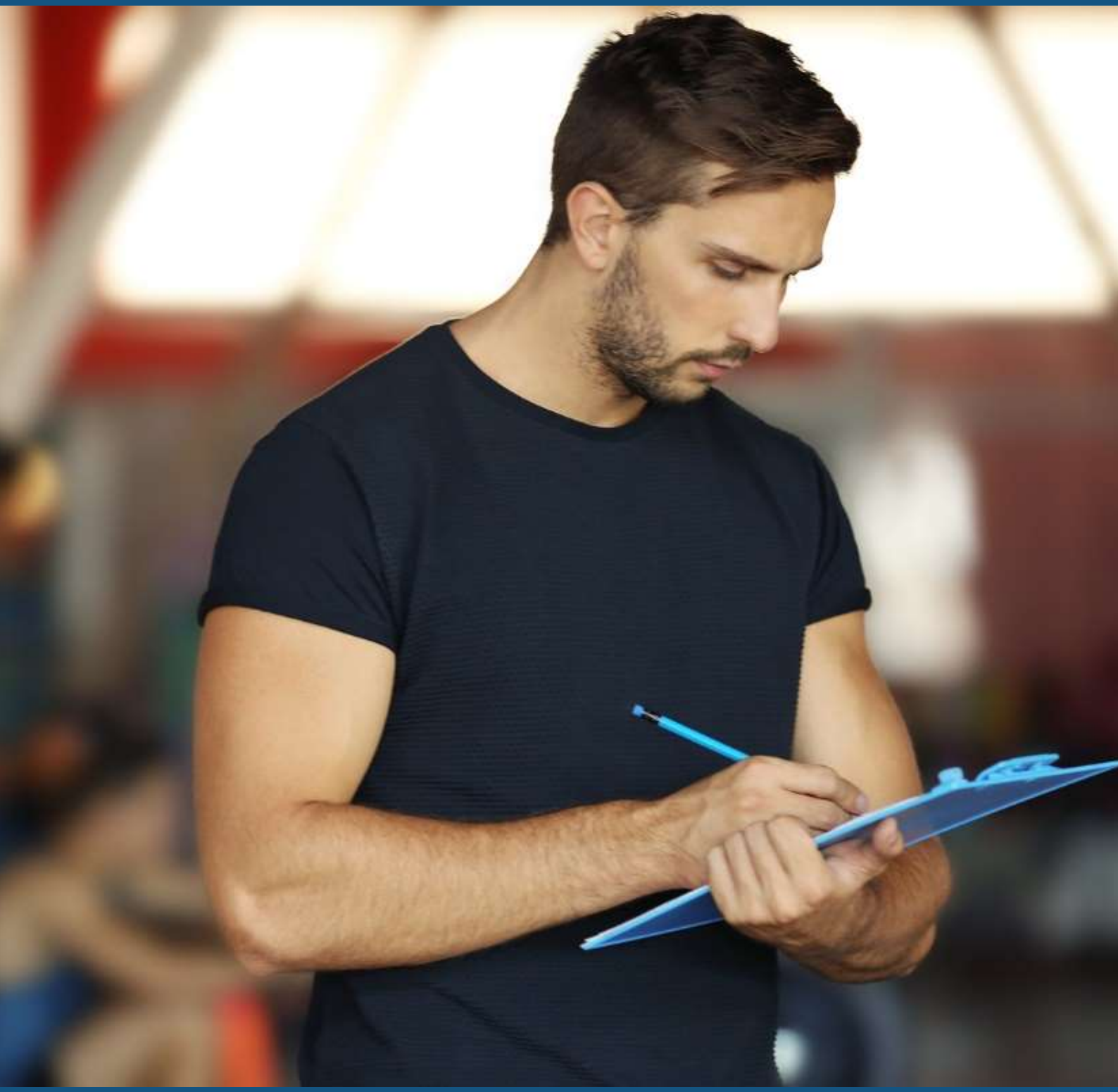
Outages happen. Whether you're providing or receiving an IT-based service, it's a cardinal truth. And from management to employees, outages are a horrible pain.

When they do happen, it's your best practices that will see you through the other side. Because in the heat of the moment, things can quickly get out of hand.

This guide is a simple step-by-step primer on what to do for both planned and unplanned outages, and how to get your business back on its feet.

Table of Contents

Making an Emergency Plan



You're probably not surprised to hear this, but your best strategy is to prepare well ahead of an outage. An emergency plan brings order to the chaos, clearly identifies who should do what, and gives you all the details you need to deal with a crisis.

If you're reading this guide and you're not in the middle of an outage right now, this should be your first step. Doing the work now will save you time during an Outage.

If you *are* in the middle of an outage, skip this section and go right to 'Dealing with an Unplanned Outage' on Page 7. As a side note, add 'Making an Emergency Plan' to your post-mortem for when the outage is resolved.

What Your Plan(s) Should Include

Contact details: Your emergency plan should have contact details for management, IT, and other involved parties. This should also include private contact details.

Even though some people may hate being on call, it's essential to have a strategy to deal with incidents no matter what time they occur. It's highly recommended to let people go off-call after dealing with an incident (Usually 24 hours).

This will lessen resentment for being on call, act as a positive reward for having successfully dealt with the outage, and let them deal with their fatigue (Minimizing social and/or health issues).

Types of Outage: You want to write a plan for every sort of unplanned or planned outage that can occur, because they will require different steps to resolve them.

Spend a LOT of time thinking about the sort of outages that can occur with any IT-based service. E.g. Are you hosted on Google Cloud? What happens if the Gmail goes out during a Google Cloud Outage? What happens if there's a weather event and your phone service is knocked out? What happens if Slack is unavailable?

This is a plan for the worst, so think of the worst!

Steps to Resolution: The steps or checklist for how to resolve the outage. You can use this guide as a framework for writing this.

You want to also include any special procedures your IT-based service or infrastructure requires to work with. E.g. Server / program shutdown order, how to bring a single one offline, who and where to obtain passwords from, etc.)

Assign Clear Responsibility: Detail exactly who is responsible for carrying out the steps above, so there's no confusion or doubt. All anyone needs to do is check the plan to see who needs to be contacted, or who should be doing what.

You can use some simple monitoring platforms to inform the people responsible when an issue occurs.

Make sure there is one clear person in charge called the 'Incident Commander'. This means you won't end up with a scenario in which there's 'too many cooks' or people in charge.

Also, make sure the people involved have the authorization to fix the outage quickly. E.g. If power goes down in the building, it's not an IT problem—who has the authority to get it fixed quickly?

SLAs: Make sure to include which outages are covered by a Service Level Agreement (SLA)! This way, you're not rushing around during an emergency demanding your Service Provider fix the problem, only to find out your SLA doesn't cover it and you wasted valuable time.

Remember to keep your SLAs in a known, safe spot for when this time comes.

Escalations: Detail in your plan the additional steps you need to take if things are getting held up. E.g. If the problem cannot be easily fixed, if the SLA provider exceeds the time limit, if a large data loss has occurred or will occur, etc.

This way, your plan will cover both minor and major incidents, especially if they become progressively worse. You can also use a monitoring program to provide automatic escalation if the issue is not resolved, sending a message to the next person in the chain.

Internal Communications: Before an outage even occurs, there should be a means of conference set up. This should ideally be something that leaves a record, like a

Slack room named #outage. Think of it as a war room for when things go wrong. You also might want to use a issue and project tracking software like JIRA.

Phone calls and verbal conversations have no accountability, so these should be your last resort method. If you must go with this, have a situation room set aside and take notes during the whole process.

External Communications: Identify if your customers are going to be impacted by an outage, and how you're going to keep them in the loop. You'll want more than one medium for this. E.g. E-mail, social media, website, etc.

Hardware and Network Description: A list of the hardware and network information that is relevant to a particular outage. All this information will be relevant to the person(s) trying to resolve the situation.

Emergency Laptop: Make sure IT has at least one laptop available for an outage that is kept updated.

Automate What You Can: Human error is the top cause of most disasters, so you want to minimize the human factor as much as possible (E.g. Automated backup schedules). This should also reduce the workload during an outage. Identify anything that would chew up time or effort, and see if it can be automated.

Multiple Plan Copies: Once you're done with your plan, make sure you have hard copies in certain, predefined places around your company, and a digital one on your company's intranet.

Dealing with an Unplanned Outage

Disaster has struck. You're experiencing an unplanned outage! Here are the steps you need to take to get through to the other side intact.

Confirm that it is, in fact, an outage

Before you break the emergency glass and assemble the A-team, make sure you're not dealing with something else (Lag, internet being down, etc.). You don't want to tell your manager there's an outage when it's something mundane.

Determine the Cause

In a time-effective manner, determine the cause. Is it a programming error? DNS problem? Expired domain? Hardware failure?

Just find out generally what you're dealing with. You don't want to exhaustively investigate the issue at the expense of not resolving it.

Stay clear of blame through this entire process. Save it for the postmortem after the outage is fixed!

Get Out Your Emergency Plan (If Applicable)

If you followed our guide on page 3, 'Making an Emergency Plan', you should already have a plan in place that you can pull out for this scenario.

If not, skip this step, and you're going to have to figure out everything as you go along.

Designate an Incident Commander

There should be one person in charge of dealing with the outage. If you've written up an Emergency Plan, this person should already be designated. If not, you're going to have to choose someone now.

The Incident Commander is the person who has the final decision-making authority, and is usually the first person to respond to an incident. They're running the show, and any task that isn't already assigned to someone falls to them.

They will need to bring people in the loop that need to be involved, such as subject experts. Your Incident Commander is vital to resolving the outage.

The Incident Commander will either need the authority to fix the outage quickly or be in contact with people who can.

Find out if the Incident is covered by an SLA

There's a chance that your particular outage is covered by a Service Level Agreement (SLA), and you may be able to outsource part or all of dealing with it.

Find this out immediately and if you can get them to fix it. Escalate the problem if they don't complete it within an acceptable time limit, the problem can't be fixed by them, or you're at risk of large data loss.

Even if you can't outsource fixing your outage, you may also have access to technical support relevant to this sort of outage, which could help you resolve it sooner.

Get the Right People Involved

Assuming you can't push dealing with the outage off to a Service Provider, your Incident Commander is going to need to get to work.

The first thing they need to do is make sure the right people to be part of the process, particularly the Support Team. They're going to be fielding questions from your customers, so they need to know what's going on.

You'll also need a point person or persons to field incoming calls dealing with the outage. Make sure to enable the support team to do their job.

Communication is key. Ideally, you want it to be recorded, such as a Slack room. As mentioned in an earlier chapter, phone or verbal communication have no accountability, and you want a record for two reasons.

1. So people can go back over what the Incident Commander told them to reaffirm what they're meant to be doing.

2. For post-mortem analysis after the incident is over.

The Checklist

The Incident Commander will need to make a checklist of all the things that will need to be done to resolve the outage. This is best done with the input of the support team and any relevant parties.

Include details on how to escalate the situation if one of these tasks cannot be completed or isn't being completed in the right amount of time.

In Case of Hacking

If your outage is the result of hacking, there are a number of other time-sensitive tasks that will need to be done.

- You will need to isolate the targeted machine(s).
- Make sure you have uncompromised backups of your business data.
- Sift through any logs, do forensics, and try to find other compromised systems.
- Back up any evidence gathered.
- Find out if the attacker can be identified and reported to the proper authorities.
- Any damage repairs that need to be done.

Regular Sitreps for Internal Stakeholders

Internal Stakeholders (E.g. Employees) probably don't want to know the nitty-gritty about the outage or what you're doing. Usually, they want to know some very specific things:

- How severe is the outage?
- What's its likely duration?
- What's being done to fix it?
- Who's working on it?

Knowing this information isn't just a good way to keep them quiet, it also helps them do and plan their own jobs.

The Incident Commander should be doing hourly situation reports (SitReps) to the whole company. It should answer the above questions in a concise manner and avoid unnecessary detail.

You might even want to point them to a place where they can view these SitReps, such as an intranet page, or the discussions going on.

Automate Anything You Can

You don't have tons of time to spare, so automate anything you can. Not only does this remove the human element (one of the biggest reasons something can go wrong), it frees you to deal with other parts of the outage.

It should be easy for your internal stakeholders to get info without contacting the Incident Commander, who has enough on their plate.

Don't Go Radio Silent

When dealing with internal stakeholders, the immediate instinct will be to shut them out to deal with the outage.

Don't do this! While you should have avenues for people to find out about the incident, you want to be accessible, and nothing is more demoralizing than going radio silent.

People should be able to contact the Incident Commander to find out more about the outage. It's a balancing act between keeping yourself focused on solving the outage and cutting people out completely, but it's a tightrope that needs to be walked.

Keep Customers Informed

Decide in advance how much you want customers to know. You don't need to tell them everything, but it's wise to tell them something and keep them informed. Craft your message carefully.

An unplanned outage is a common way to lose customers, so you want to make sure you're as transparent as possible so they know you're dealing with the issue.

Make sure you're using the right tone. You'll need to be concise, authoritative, and serious. While you may be tempted, don't try to joke or be cute—remember, their business is being affected! Instead, you'll want to show humility, consideration, and don't be afraid to accept fault

Ideally, you'll want to keep them informed every 30 minutes, even if there's nothing to report. Don't expect users to go to the status page. If they go to e-mail user support, send them all a reply when the incident is solved.

The Post Mortem

After the outage is finished, it's time to win back trust. If you followed the steps above, you'll have a detailed record and information on what happened and what was done to resolve it.

Be accurate about what happened, what went wrong, and how you're going to prevent it from ever happening again. You can use this information to follow up with customers to regain their support. They want to know that there's no flaws anymore in your service, or you're in the process of fixing it.

In the future, make preventing outages a priority by having your teams spend a portion of their time making proactive steps to prevent it from ever happening. It's less glamorous than rushing in to save the day, but your shareholders and customers will love you more for a service that never fails as opposed to one that breaks often and is quickly fixed.

Dealing with a Planned Outage

A planned outage may be less stressful than an unplanned one, but only if properly handled. You're still effectively ending an IT service for a period of time.

Talk to Management

Planned outages usually happen as part of a project, one that you discuss with management beforehand. So first, you need to make sure they're in the loop.

Inform Your Users

If the outage is going to affect a number of users, you'll need to send out an e-mail ahead of time containing the following information:

- The time and date of the outage.
- The nature of the outage.
- Any possible effects of the outage.
- Any possible workarounds (Preferably with screenshots).