Proactive Observability

Internet Outage Prevention Checklist

If your organization provides any type of service via the Internet, then you have likely suffered a service outage at some point. If you haven't, it's probably just a matter of time.

Modern online services are extremely complex. There are myriad components involved in delivering your services to your customers, any of which could fail and cause an outage. Some of these systems are under your control, but many are not. It's essential to anticipate and plan for a wide range of outage scenarios, so you aren't caught flat-footed when something goes wrong.

You need to take proactive steps to reduce the risk of an outage, have a plan to quickly diagnose the cause of an outage and restore your services, and be prepared to communicate effectively with your customers throughout. This checklist is intended to serve as a guide as you develop your outage prevention and mitigation strategy.

catchpoint

Prevention and Preparation

You can't avoid all outages, but these best practices reduce the chances that a change to your systems will lead to unexpected downtime and prepare you to respond effectively when something goes wrong.

- **Establish and consistently apply a rigorous change-management process** across all systems, whether manual or automated. Include:
  - Thorough testing of all changes in a pre-production environment.
  - Documentation and tracking of all changes.
  - Clear policies/procedures around how, when, and by whom changes will be implemented.
  - Documented procedures for rolling back every change.
- **Be familiar with underlying protocols and infrastructure that your application depends on.** When evaluating your internal systems, don't just focus on your application's code. Include:
  - DNS
  - BGP Routing
  - TCP Configuration
  - SSL
  - Operating systems
  - Virtualization platforms
  - Physical servers and networks
- **Don't overlook your automation scripts!** Apply the same level of planning, testing, and tracking to automation as you do to application code.
- **Identify every part of the delivery chain between your system and your end-customers** and establish a plan of action in case of a failure at any point. Consider all relevant third-party systems, such as:
  - ISPs
  - Cloud compute platforms
  - Cloud services
  - Content distribution networks
  - Managed DNS
  - Page optimization
  - Advertising and marketing
- **Identify edge-cases that may cause issues,** and make sure your team is aware of them. An extremely unlikely scenario has only to occur once to cause a major problem.
- **Establish a monitoring and observability plan** that covers all internal system components and the rest of the delivery chain. Monitoring whether your service appears to be up or down is not enough.
  - Monitor each potential point of failure independently to identify the root cause.
  - Establish performance baselines to use for comparison, to identify behavior changes after outages.

- **Create a crisis call process**.
  - Answer these questions: If something fails, who will be on the call, and what will they do?
  - Create templates and runbooks and make sure your teams are familiar with them in advance.
- **Create a communications/PR plan.** Work with your marketing and PR team in advance to:
  - Decide what channels of communication you will use during an outage.
  - Agree on who will be responsible for messaging and what the messaging cadence will be.
  - Create communication templates and have them ready.
- **Don't just make these plans — test them!**
  - Practice your outage response regularly.
  - Ensure team members are familiar with their roles and can handle problems confidently.

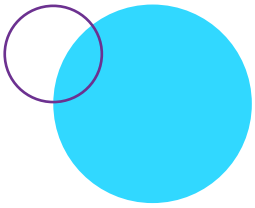
During an Outage

Despite best efforts, outages will still occur. Follow these steps to minimize the duration of an outage and its impact on your customers.

- **Confirm the outage and proactively acknowledge the situation to your customers.**
  - Let people know that you are aware of the problem and working on a solution.
- **Execute your crisis call process.**
  - Establish communication among your internal teams.
  - Make sure the right people are actively working on diagnosing and resolving the issue.
- **Determine whether the technical problem is internal or external to your systems.**
  - Use your monitoring/observability system to troubleshoot each component of the service delivery chain.
  - Identify the root cause as quickly as possible.
- **Identify recent changes to your systems if the problem is internal.**
  - Follow your roll-back procedures to restore the system to a working state.
- **Communicate with your vendors if the issue appears to be external.**
  - If appropriate, provide data from your monitoring/observability platform to help them confirm the cause of the issue.
- **Follow your planned communication cadence.**
  - Even if you don't have new information to share with your customers in each update, make sure they know the general nature of the problem.
  - Reassure customers that you are working toward a solution.
  - Be honest and transparent throughout the process.

Postmortem

After technical issues are resolved and the "fire" is out, learn as much as you can from the experience, and let your customers know what happened and what you are doing to avoid similar problems in the future.



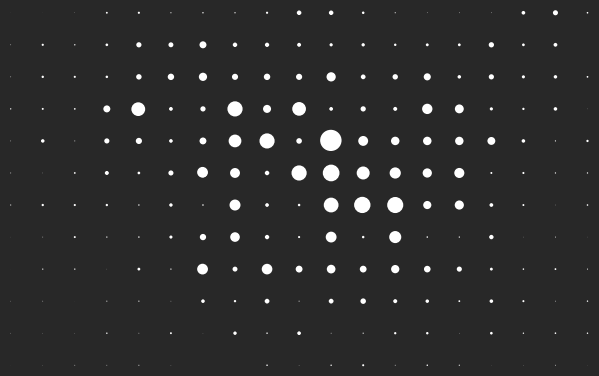
- **Perform a thorough root cause analysis.** Ask the following questions:
  - Was the outage due to something you could have prevented with different procedures or preventative measures?
  - If so, what policies might you put in place that would reduce the risk of a similar problem reoccurring?
- **Communicate a summary of the Root Cause Analysis (RCA) to your customers.**
  - Let customers know what happened.
  - Let customers know what actions you are taking.
- **Ensure the problem is fixed.** The steps your crisis-response team took to end the outage won't necessarily have addressed its root cause.
  - If the outage was due to something fundamental to your system's design, be sure that your Product Management and Engineering teams properly vet, prioritize, and permanently resolve the issue.
- **Evaluate your third-party vendor relationships.**
  - If the problem was due to an issue at a third-party, make sure they have taken proper action to prevent similar problems in the future.
  - Consider whether you should switch vendors or use multiple vendors to reduce your exposure.
- **Evaluate your response plan.** Ask the following questions:
  - What aspects of your outage response plan worked well?
  - What didn't work well?
  - Is there anything you could have done better in response to the outage?
- **Evaluate your communications plan.** Ask the following questions:
  - How effective were your communications during the outage?
  - Did you find yourself reacting to customers and media outlets?
  - Were you proactively communicating and controlling the message?
- **Evaluate your observability and monitoring strategy.** Ask the following questions:
  - Did you have observability of every part of the delivery chain so that you could diagnose the issue quickly?
  - Do you have historical data that you can use to compare system performance before and after any configuration changes?
  - Do you have the right monitoring tools and strategy in place going forward?

Conclusion

There were numerous major Internet outages last year involving some of the most prominent tech companies in the world. The stories behind these outages contain valuable lessons, not just about what can go wrong, but about how important an organization's response to a crisis can be.

To learn more about the causes and outcomes of these outages, check out Catchpoint's eBook:

Preventing Outages in 2023: What We Learned from Recent Failures



Catchpoint is the Internet Resilience Company™. The top online retailers, Global2000, CDNs, cloud service providers, and xSPs in the world rely on Catchpoint to increase their resilience by catching any issues in the Internet Stack before they impact their business. Catchpoint's Internet Performance Monitoring (IPM) suite offers synthetics, RUM, performance optimization, high fidelity data and flexible visualizations with advanced analytics. It leverages thousands of global vantage points (including inside wireless networks, BGP, backbone, last mile, endpoint, enterprise, ISPs and more) to provide unparalleled observability into anything that impacts your customers, workforce, networks, website performance, applications and APIs.

Learn more at **www.catchpoint.com**

catchpoint