PagerDuty

Best practices in communicating internally during an incident

Table of contents

PagerDuty

Introduction

Drive proactive communication between business stakeholders and your incident response team.

When a major customer-impacting incident happens, you need to get the impacted teams together to talk about it quickly and effectively. It might seem like communication is just something that should happen naturally, but for the modern enterprise, this is harder than it sounds.

Think about how much communication has changed over the last few years. Instead of leaning over to ask your deskmate a question or booking a conference room for group work, now you and your teammates might be spread across the globe. In-person white-boarding and incident response still happens, but perhaps not as often as it used to. With teams distributed across geographies and time zones, getting the right people to discuss and solve for the problem at hand can be a big challenge.

Compound this with all the channels teams use to communicate and how much data can get lost along the way. Consider all the different groups that need to be looped into the conversation and what different pieces of information each of those groups need. What tools are you going to use to keep track of decisions the responders make? What do your internal stakeholders need to know?

Not so easy, is it?

Luckily, there are tools you can use and best practices you can follow to streamline this process. You don't want to be figuring out the answers to these questions in the middle of the incident, so we recommend putting a process in place for communication during an outage in advance. We put together this guide to share some of the best practices we've seen for internal communication during incident response.

Incident response team

Good communication starts with your incident response team members, since they're the people closest to the incident. We've seen our customers work most effectively when they have a codified way to coordinate incident response across subject matter experts and front-line responders. It's important that you have an efficient way to sound the alarm, and make sure that your conversations facilitate a coordinated response.

To be successful, you'll need to do three things: get the right people involved, pick the right communication channels, and make sure you document everything.

Get the right people involved

Before all else, consider appointing an Incident Commander. This is a single person with final decision-making authority. This person might be the person who acknowledges an incident. However, for higher priority incidents, many teams like to add a dedicated Incident Commander who has gone through role-specific training.

It's important that an Incident Commander knows what their role entails. They have to assume all responsibilities that haven't otherwise been assigned and delegate what they cannot do to others. They track the incident, coordinate response between different groups, and loop in subject matter experts (SMEs) where needed.

In addition to the Incident Commander, you may want to consider other roles such as a:

- **Deputy:** A Deputy is a direct support role for the Incident Commander.
- **Scribe:** A Scribe documents the time-line of an incident as it progresses and makes sure all important decisions and data are captured for later review.
- **Customer Liaison:** A person responsible for interacting with customers, either directly, or via our public communication channels.
- **Internal Liaison:** A person responsible for interacting with internal stakeholders.

Together, with dedicated SMEs, this builds a full response team. This isn't necessary for all incidents. You may only use this format for Sev1 or Sev0. But everyone should be aware of their roles and responsibilities.

Pick your communication channel

Communication within your incident response team can take place across multiple channels. The right channel depends not only on the severity and scope of the incident, but also on your team culture and work location. Whichever channel you choose, make sure you clearly define what will be used and how participants can get involved. With today's emphasis on hybrid and remote work, it's important to ensure that there is always a virtual backup channel, even if you usually work in-office. Additionally, if you're responding off-hours, you want a place to work that doesn't require you to go into office.

There are several possible communication channels, and your team may use all within a single incident. The two most common communication channels are chat and video conferencing. Chat is perfect for sharing screenshots, communicating asynchronously, and documenting the incident as you go. Video conferencing works best for live collaboration and troubleshooting.

In PagerDuty, you can configure Incident Workflows to automatically spin up an incident-specific channel or conference bridge for each incident. Automating this ensures that you always have a place to speak with your team without the manual effort of creating a channel and adding all incident participants to it.

Document everything

Whatever communication channel you prefer, it's important that key moments and discoveries, as well as communications, are recorded to refer back to later during a postmortem. This is one of the scribe's responsibilities, but all responders can save information to include later when reviewing the incident.

When documenting, here are some things you should remember to save:

- Pertinent logging, monitoring, and alerting information, including screenshots
- Major decision points, what those decisions were, and when they were made
- Outgoing communications, both to other line of business stakeholders and to customers
- Attempted (and successful) remediation efforts

If you don't have a scribe to take notes, the Deputy or Incident Commander should record as much as possible. There are some ways you can make this easier. You can record your conference bridge during response and use it to pull notes from after the incident is resolved. You can also record everything in your incident-specific chat channel so you can refer to it later. This method is particularly useful as it's already timestamped and transcribed correctly.

Business stakeholders

Customer-impacting outages naturally also affect people outside of your technical team. After all, customer support is often the first line of defense when things go wrong, and leaders from across the organization may start to ask questions as their teams start sounding alarms. Proactively keeping relevant, internal stakeholders in the loop for large scale incidents helps the entire organization collectively coordinate and solve for any cascading problems throughout the company. Planning ahead of time will go a long way towards ensuring successful internal communication. Have an idea of what to share, set up a place where colleagues can get information, and determine who will get updates and how often. Last but not least, templatize communications when you can so they're reusable the next time you need them.

Decide what to share

Your internal stakeholders are, for the most part, not interested in the long story of how your system went down and what methods you're using to fight the fire. They are mainly interested in a couple of key pieces of information:

- **Severity.** How severe is the outage, and what is its likely duration?
- **Impact radius.** How many customers are affected and is it a total outage, or a degradation?
- **Action plan.** A What's being done, and when can the team expect the next update?

Example:

Hello, we are contacting you to inform you that a P0 outage is occurring on the shopping cart business service. At this point, we estimate 50% of our customers are affected by this incident. We are working to resolve this matter and are currently in the diagnosis stage. You can expect an update one hour from now on our progress.

Making sure this information is clear will help your colleagues on other teams continue doing their own jobs. Additionally, it prevents the "executive swoop and poop." This phrase is a funny way to describe a very frustrating situation. You're working to resolve an incident, but keep getting interrupted by stakeholders. While having an Internal Liaison to field these asks is helpful, the best way to ward off pings is to proactively communicate with those who rely on you.

Automate wherever you can

Wherever possible, it should be easy for internal stakeholders to get information without reaching out directly to your Incident Commander or Internal Liaison.

It's important to make incident information available internally to whoever wants it, whenever they want it. One way to do this is with an internal status page. This is similar to an external status page, though here you may add more information to help the business respond better jointly.

Within PagerDuty, you can leverage Stakeholder Subscriptions. You can provide updates for the customer-facing services your stakeholders care about. They'll be able to receive notifications when there's a problem with these services.

Another way to automate the communication process is to ensure that you don't need to write a new communication each time you need to inform stakeholders. With Status Update Notification Templates, you can create reusable rich text templates. Then, with a MadLibs-like approach, you can drop appropriate incident variables like the service it relates to, the incident state, and more. With less overhead, you can communicate quicker. This also reduces the likelihood of errors and miscommunications.

Coordinate follow-up

Even with automation, your colleagues might have further questions about the outage. It's important to find a balance here between keeping your priorities straight and not going radio silent. Directing questions to your Internal Liaison will unburden the rest of your team and keep them focused on the problem. Remember that your whole company is vested in solving the same issue, so your Internal Liaison should be quick to answer any queries that come up. Similar to communicating with customers, it can also be helpful to let stakeholders know at what interval to expect updates. If you set the expectation that you'll update them every hour on the hour, it should prevent them from reaching out every 15 or 30 minutes

Enable your support team

According to PWC, 1 in 3 customers would stop doing business with a brand they loved after one bad experience. One of the last lines of defense during an outage is your Support team. These are the people interacting with customers on a daily basis, and they'll be the ones who handle upset people during an outage. It's important that communication is a two-way street.

Your support team should be able to trigger an incident when they're getting reports of abnormal behavior. Ideally, you should catch issues before your customers become aware of them, but that's not always the case. If customers are feeling the impact before you are, your Support team should feel prepared to create an incident. This helps kick off the remediation process faster and reduces customer impact.

Additionally, if you find out about an issue before the customer does (which is ideal) but know you won't be able to resolve it before customers feel the impact, it's crucial to give Support a head's up. This helps them prepare communications and set expectations with the customer.

This is tricky to orchestrate on your own, however. That's why we recommend using PagerDuty Customer Service Operations to create bidirectional communications and allow both teams to talk despite working in different tools.

Wrap up

Grow + learn

Even though engineering teams are under colossal pressure to maintain a profitable, reliable product, they don't always take the time to learn from past failures.

Postmortems are a critical part of incident response. They allow you to look at a project's history, analyze what went wrong, and formulate a way to prevent it from going wrong again.

You should consider who you invite to collaborate and provide input for postmortems. While technical teams are consistently involved, other stakeholders may not be. Since communication goes both ways, it's important to think about how well your communication was perceived by your stakeholders. This helps you improve your business response, not just your incident response.

You should also circulate postmortems widely within the company. This helps your stakeholders feel like they're being included and that you're prioritizing improvements.

Key takeaways

Here are the top takeaways for communicating internally during incident response:

Within the incident response team:

- Be clear on roles and have a designated Internal Liaison when necessary to field communications..
- Know your channels and automate the process of adding all relevant parties to the conversation.
- Document as you go, as much as possible.
- Learn and grow from postmortems and take feedback from the stakeholders you involved.

With business stakeholders:

- Share an appropriate level of detail with internal business stakeholders and keep in mind your audience may not understand the technical nuances of the response efforts.
- Automate the internal communication process and create reusable templates where applicable to remove cognitive load and coordinate follow-up.
- Enable your Support team to have two-way communication with the response team.