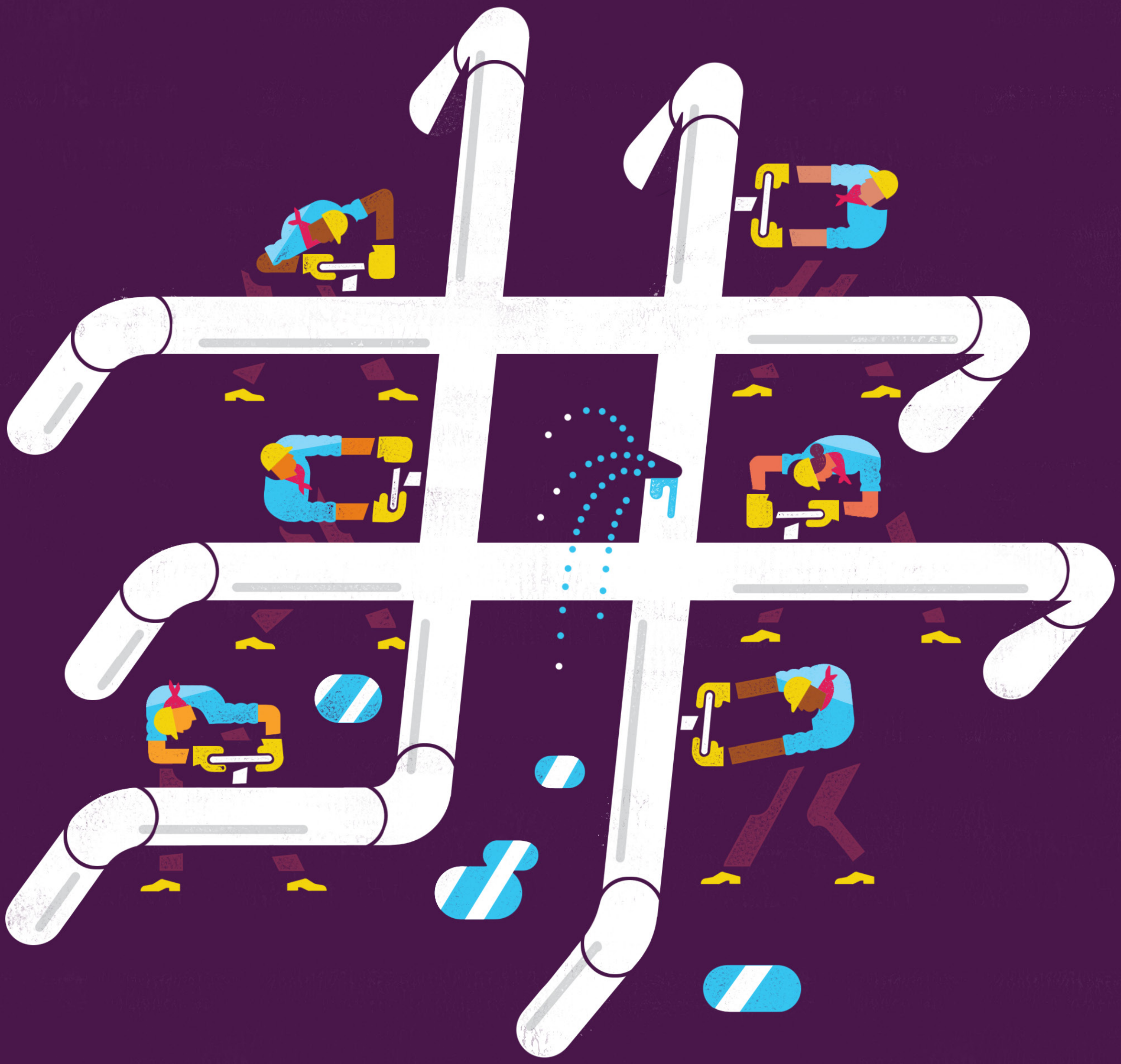
slack



Modern incident response

How our customers use Slack for faster resolution, less stress and fewer repeat incidents

Modern incident response

What's inside?

CHAPTER 1

Introduction

The digital world is open 24/7. So it follows that digital consumers expect IT and customer service to keep the same hours. These exceedingly high expectations mean that no issue is too small or common to frustrate customers, from broken code to site-wide outages. The data analytics company Splunk reports that many companies experience incidents like these about five times a month, with each offense costing more than $100,000—and annual IT downtime costing enterprises $700 billion in lost productivity.*

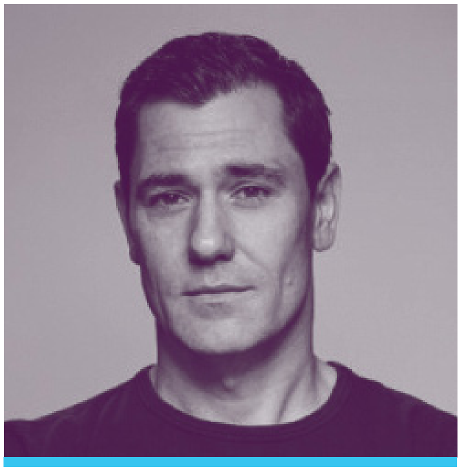
E-book author:
Jessica Dawson

*Source: The Cost of Server, Application, and Network Downtime: North American Enterprise Survey and Calculator, IHS Inc.

Most companies don't have a dedicated incident response team. Instead, whenever an incident occurs, they rush to assemble an ad hoc team composed of whoever is on call and has relevant knowledge, skills and capabilities—much like a volunteer fire department. When fire departments respond to a five-alarm blaze, their ability to save lives and property depends on how quickly they establish roles, communicate about the nature and extent of the fire, and agree on the best path forward.

Technical glitches and bugs aren't life-or-death, but the way we can remedy them using Slack isn't all that different from the best practices used by first responders around the world.

With Slack, anyone in the company can "pull the fire alarm," which auto-



"The goal of incident management is speed: speed of response and speed of resolution. Slack has been critical for that."

Timothy Kersten, IT Operations Manager, Tyro

The most recent industry surveys have shown that the average enterprise **estimates that there is an impact of approximately $8,851 for every minute of unplanned downtime** in their primary computing environment.

Source: Gartner "Ensure Cost Balances With Risk in High-Availability Data Centers," David Cappuccio, 1 April 2019

matically alerts on-call engineers and incident commanders, and get a response any time of day, seven days a week. By using automation and creating a central location where all stakeholders can quickly view relevant context around the issue at hand, we can not only shorten the incident but reduce its impact.

When the cloud-based accounting software company Xero's office printers went down globally on a busy weekday in 2019, there was no scramble to find resources. Instead, engineers leveraged an intuitive Slack workflow built around dedicated channels, custom Slack tools, integrations, threads and emoji to identify and triage the issue without sending anyone into a panic or losing a huge chunk of time.

Slack streamlines incident management right out of the box, acting as a single command center for detection, containment and post-incident analysis. Instead of a stressful, reactive and siloed atmosphere, employees are equipped to take a proactive approach and collaborate in real time with an evolving, intelligent tool.

Modern incident response with Slack

ACTION	Create dedicated Slack channel	Set channel topic, pin info, start threads	Automate processes and existing tools	Integrate slash commands	Collect post-incident Slack findings
	↓	↓	↓	↓	↓
RESULT	One source of truth for stakeholders	Increase productivity	Accelerate agility	Simplify and speed up response	Learn, iterate and prevent future incidents

CHAPTER 2

Centralize your command center

The Australia-based software company Iress previously relied on email and phone calls for urgent issues, tracking people down one by one. Messages were missed, emails bounced around, and time was lost. Using Slack as part of a broader support strategy helped Iress cut the average response time for complex customer issues from eight days to two, and led to a 64% decrease in its customer support ticket backlog.

64%

decrease in Iress' customer support ticket backlog while using Slack as part of support strategy

Decrease in Iress' average customer support response time:

8 days

↘

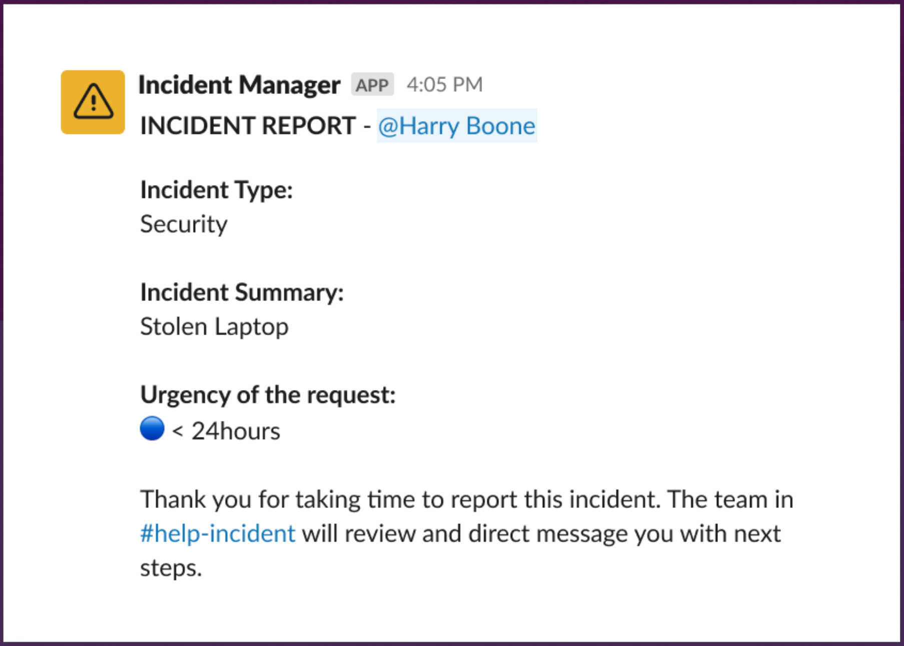
2 days

Whether it's a fast-growing 2,000-person company like Iress or a Fortune 50 company like Target, Slack offers employees a central source of truth to easily navigate high-pressure scenarios. Employees have one tool for everything, removing the burden of redundant email chains, endless games of phone tag, and isolated applications that don't speak to each other. "The highest value is that people know exactly what's going on without having to ask and can see everything in a very centralized place: Slack," says Andrew Cunningham, a delivery lead at Australia's rapidly expanding business bank Tyro.

SLACK TIP

Meet the Slack Workflow Builder

Moving information through rapidly growing organizations can lead to unintentional silos that cause confusion around priorities and harm productivity. With Workflow Builder, anyone can quickly submit a form to report incident information. The details are then automatically shared with the designated team channel to take action.



Incident Manager APP 4:05 PM

INCIDENT REPORT - @Harry Boone

Incident Type:
Security

Incident Summary:
Stolen Laptop

Urgency of the request:
🔵 < 24hours

Thank you for taking time to report this incident. The team in #help-incident will review and direct message you with next steps.

Some other handy ways to use Workflow Builder for incident management:

Security:	Data security or privacy incident reporting
Operations:	Frontline worker incident management
Facilities:	Office workspace issue notification
Product:	Incident triaging and post-incident reviews
Customers:	Issue reporting in channel with Slack Connect

When everyone knows exactly where to look, teams can effectively collaborate asynchronously, even if they're not in the same office or country. At business consultancy R/GA, CTO Nick Coronges says, "people work across multiple time zones and geographies, and we depend heavily on real-time communication in Slack to work collaboratively without slowing down the pace of decision-making. On a given project, we may have three to five offices working together, and email doesn't cut it as a communication medium."

"We're working as a team across 4 different locations right now in 3 different time zones. Slack is what has kept everyone up to speed."

Katrina Bekessy, Senior Technology Director, R/GA

For every incident, a Slack channel

The software company Autodesk standardizes its channel naming to let employees know a channel's purpose from the get-go, increase discoverability and encourage cross-team collaboration. "With so many people on Slack, they are led in the right direction in a timely fashion. It's the difference between days and minutes," says Guy Martin, Autodesk's former director of open source.

It can be helpful to designate an incident commander, or IC, who builds the team structure and brings in the right people at the right time to solve the incident. At the edge cloud platform Fastly, executives and specialists come together in an internal cross-functional channel to develop solutions for support situations. Even if it's a Saturday, key participants will join calls or respond via Slack's `mobile app` to keep resolutions moving. "Because of Slack, we're able to see activity almost instantly, triage events if needed, determine the severity, and pull other people in," says Kim Ogletree, Fastly's senior vice president, client services. "Then we diagnose exactly what we need to do in near real time."

Everything in its place

Once there's a designated incident channel, the IC starts pulling in subject-matter experts who will create, test and deploy technical fixes. Much like you `@mention` any other member of your workspace, you can @mention a `user group` to pull an entire team into a channel at once—and then collaborate with whoever's available.

The IC might also pull in a customer-experience-team liaison to bridge engineers with any impacted customers, and an executive-team liaison for high-profile or urgent incidents. From there, a `channel topic`, which is visible at the top of the incident channel, helps keep new responders up to speed and can serve to identify both severity and status. The IC can also take advantage of a `pinned message` to provide the team with a quick snapshot of the most essential information or pressing needs.

Comprising various specialists, Xero's customer experience (CX) team previously relied on emails to share guidance and documentation. Matt Simpson, a lead workflow coordinator, says those emails always got lost: "They were just here, there and everywhere." Today, CX has 30 to 40 Slack channels dedicated to each specialist group, and the customer support flow is smooth and streamlined. When an agent needs guidance, he or she simply mentions the designated user group in their dedicated channel, which notifies every senior member who's online. Whoever picks up the issue reacts with an emoji to indicate that they're on it. Then they'll start a thread to provide a resolution. "Agents can move on to the next customer," Simpson says. "That means our customers are actually getting quicker answers. That's huge."

With a specialized team at hand, the IC can assign clear actions, and new responders get up to speed by scanning channel topics and scrolling up to see previous investigative paths and decisions. Everyone has a holistic view of all communication, even during off-hours.

As we all know, emergencies rarely wait for the 9-to-5 window. At the movie ticketing company Fandango, CTO Paul Zimny says, "the ability to jump into Slack to work an incident with a team and get a timeline view of all the communication that's preceded is extremely helpful. Especially if you're responding to a middle-of-the-night incident."

In addition to helping responders get caught up as they join the incident response, other stakeholders can follow along in the channel and see what fixes are being implemented and when, without slowing down the process. The channel also provides a transcript of the event for future reference. With the full context, teams can explain issues during customer meetings and postmortem discussions—and share the knowledge with their colleagues to prevent similar situations in the future (see chapter 5 for more details).

Shift focus to where your company needs it most

To avoid cluttering the main channel, `threads` are a powerful way to provide a quick and easy place to focus on a particular subject. At Target, Slack is the central hub for engineering com-

"For most of the engineers, the biggest thing was both threading and the ability to integrate in with their applications, like GitHub Enterprise and Jira."

Jay Kline, Director of Technology–Engineering Enablement, Target munications, which is especially helpful when the team needs to exchange information that isn't easy to convey verbally, such as URLs and IP addresses. Jay Kline, Target's director of technology–engineering enablement, says, "For most of the engineers, the biggest thing was both threading and the ability to integrate in with their applications, like GitHub Enterprise and Jira." Now Target's engineers can keep conversations organized and easy to follow, as opposed to sifting through long email chains that only some people read and even fewer respond to.

For large-scale or complex incidents, or those that might contain sensitive data—say, a health organiza-

👋 **SLACK TIP**

To move around channels, direct messages and workspaces even faster, you can use Slack's `Quick Switcher` with command+K or control+K.

tion working with patients—companies can create additional public or private channels that follow the same naming convention as the main channel. With the “share message” feature, employees can copy key messages from the main incident channel to these auxiliary channels as needed. For added security, Slack Enterprise Grid has the option for multiple workspaces, and each workspace can have different access controls (i.e., different people who are allowed to access it). So everyone at the company might be allowed in your Main workspace, but only a subset of people would have access to the Security workspace.

While there are a variety of ways to scale incident channels as issues grow, channels are also helpful when they’re used only for a few minutes by a handful of people. Fandango’s engineering team, for example, creates one-off, incident-specific channels for relevant stakeholders. “These single-purpose channels help us keep the noise out and isolate that conversation so we can spin up and down very quickly as needed,” says Zimny.

CHAPTER 3

Accelerate agility with automations and integrations

Teams can leverage Slack's `automation capabilities` to quickly review context and shorten incident resolution time, reducing each event's impact on both customers and the company.

To accelerate agility, Slack integrates with 2,000 tools that teams use daily, from marketing and sales to HR, support, analytics and design. “Anytime I’ve seen a Slack integration, I’ve turned it on,” says Thomas Lawless, IBM’s executive IT specialist. “It provides so much value and helps us save so many extra steps in our process.”

Monitoring integrations like PagerDuty and Grafana ensure that even the smallest incidents don’t slip through the cracks by automatically piping critical alerts and notifications directly into Slack channels. This is especially helpful for engineers, who receive Slack alerts where they’re already coordinating code reviews and pull requests, empowering them to quickly gather content and escalate the incident to the right people. Companies can seamlessly manage and track a situation as it evolves, reassign or escalate as needed, and collaborate across teams to quickly resolve the incident.

After switching to Slack, the telecommunications company Vodafone dramatically reduced its mean time to resolution, in part due to Slack’s PagerDuty integration, which engineers use to monitor and escalate customer-facing events. When an incident occurs in a produc-

21%

Less time needed when using Slack to identify and resolve engineering-related bugs

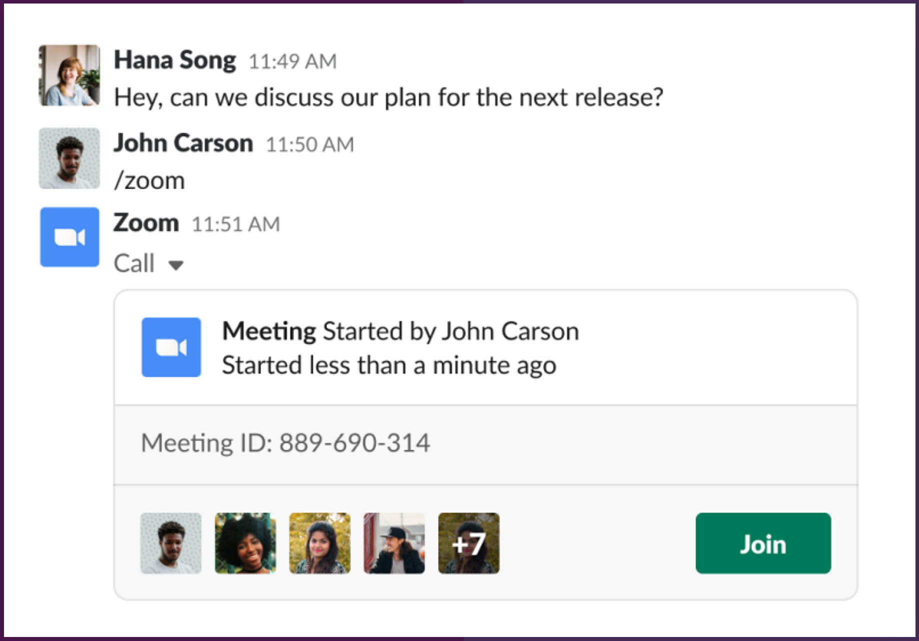
Source: "The Business Value of Slack, 2017," IDC research, sponsored by Slack

tion environment, the integration notifies the right team, down to the right individual, within milliseconds—and all within Slack. Paul Whyte, Vodafone's former head of systems engineering, says that before Slack it would have taken 15 to 20 minutes to find the root cause, "but we've reduced the mean time to resolution to under five minutes. It's been phenomenally successful in a very short period of time."

Having all your tools and communication in the same place enables a faster response and eliminates the time and distraction costs of context switching. When people are able to use the tools they prefer, they're inspired to contribute more, increasing the likelihood of cross-team collaboration. “Slack is not only great at connecting people, it’s great at connecting the tools and the systems we already have,” says Coronges of R/GA, where engineers depend on Jira. This integration allows them to create and preview issues in Slack, and fetch key details to keep the team focused. Powerful filtering to selected channels, projects, issue types and priorities cuts out the clutter.

Zoom, the web conferencing tool, is another popular integration used by support teams to stay nimble and facilitate painless communication. “We have a ‘/zoom’ command that spins up meetings for our larger group needs,” says Cody Jones, the head of partnerships and alliances for Zapier, a popular web-based automation tool. Plus, “Slack automatically changes your status to alert others on the team that you are currently in a meeting.”

When employees need to interact more, they can use the `Slack call` feature to make a voice or video call to any member of their workspace: Once con-



Hana Song 11:49 AM
Hey, can we discuss our plan for the next release?

John Carson 11:50 AM
/zoom

Zoom 11:51 AM

Meeting Started by John Carson
Started less than a minute ago

Meeting ID: 889-690-314

Zoom app integration

nected, they can click, scroll, type and even mark up what's being shared from the presenter's screen. This is critical to operations at Zapier, where everyone, including the CEO, works directly with customers to answer tickets and debug issues. Working in pairs on one screen ensures that employees without a support background have a co-pilot when addressing customer questions. "We often find two minds work better than one," says Jones. "Slack's interactive screen sharing allows multiple members of our team to jump into a support ticket and work together to resolve it."

Put a bot on it

Anything a Slack app can do can be built into a `Bot User`. Often, incident teams build a bot with a face, name and personality to encourage users to talk and engage with it, just like they would a human colleague.

At Xero, it's Matt Simpson's job to make sure the customer experience team keeps to the response times promised in its service-level agreements. That often means being the liaison between a frontline agent and a specialist who can provide the insight needed to close a case. Before Slack, this could cause a huge bottleneck: If Simpson wasn't available, it wasn't always clear who should be calling the shots, and questions would pile up in an unproductive Yammer group chat.

Slack helped Simpson scale his operations in a way that didn't leave anyone—or any problem—behind, with a custom bot called Kevbot. To start, users open a direct message with Kevbot and ask, "Who's the current WFC?" Kevbot will list the workflow coordinator, saving users from a frustrating and time-consuming search. Similarly, the bot can recognize keywords and route reps to the right specialists. Kevbot gives Simpson peace of mind and ensures that workflows continue even when he's not around. "I don't have to go back three or four hours later and pick up any of the lost work," he says.

Simplify and speed up response time

`Slash commands` act as shortcuts for specific actions in Slack and simplify processes even further. At the e-commerce platform Shopify, employees can type "/spy" plus an action in Slack to run any of more than 100 custom commands, including tracking the duration of incidents and key events on the incident response timeline. Because Spy is so critical to their work, it's backed up across multiple data centers in case one fails. "An outage to our systems costs tens of thousands of dollars a minute. If it just saves one minute of confusion, it's worth it," says John Arthorne, a former production engineering lead.

A slash command also has the power to spin up a dedicated channel in Slack and post a message with rele-

👋 **SLACK TIP**

Don't see a shortcut that fits your workspace's needs? You can include custom slash commands as part of a Slack app created for your workspace.

vant documentation links. At Nine, one of Australia's largest national media companies, chief information and technology officer Damian Cronan and his team have automated several manual processes to help team members get the information they need, when they need it. Employees can report incidents, request transcripts, surface data dashboards, and more with simple slash commands and custom Slack integrations. "Historically what might have taken a couple of days to iron out is now generally something we can jump on within 30 minutes," says Cronan.

CHAPTER 4

Streamline communication and save time with emoji

When every second counts, emoji reactions make it easy to scan for status updates. Teams align on which emoji indicates what, and can even create their own incident-specific emoji to further customize the response.

Emoji can also delineate who is working on what; for example, the incident commander could mark themselves with a ⛑️ symbol, both in their status and in the channel description, so others can see at a glance who's running point. For teams with multiple incidents running simultaneously, an IC can name which one they're responsible for in their user status, which anyone can view by simply hovering over their status emoji.

👋 **SLACK TIP**

Some quick emoji responses

👀 → ✅ → 🚩

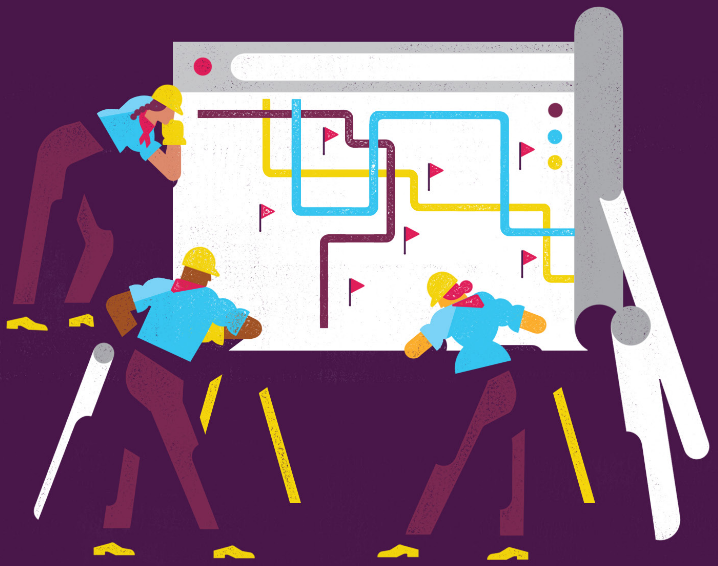
👀 "I'm looking into this"

✅ "This is done"

🚩 "Flag for post-incident-response follow-up"

With the Reacji Channeler app, users can leverage emoji to instantly route a message from one public channel to another. For example, let’s say someone shares a post-incident review doc in the incident channel: If they tag it with a particular reacji, this shares that message in a previously designated channel that anyone can follow. It’s an app you can install and use out of the box, no code required.

Emoji and Slack go hand in hand, but the meal-kit company HelloFresh found a way to make the experience even more human by using face emoji to recognize and celebrate great work. “So people start being looked at and respected for the things that they are really, really good at,” says CTO Nuno Simaria. “And that reinforces the team altogether.”



CHAPTER 5

Learn, iterate, prevent

Once companies solve an incident, an effective post-incident review ensures that it doesn't happen again. Luckily, you can organize your entire incident response to inform this review with little extra legwork. Using a specific emoji, like the ⛑️ mentioned in chapter 4, the response team can easily flag any message they'd like to include in a review: time-stamped discussions, screenshots, graphs, links to relevant systems and dashboards, and resulting decisions. Using Reacji Channeler, teams can instantly copy all of their flagged messages to a dedicated incident review channel.

The ability to archive channels means the historical record is preserved and can be referenced to identify patterns and onboard new engineers more effectively. When the incident review is complete, teams can share the final report back to the dedicated incident channel, where it's neatly stored alongside all the relevant context.

When a fire is allowed to burn unchecked, it gets hotter and larger. IT incidents work much the same way: When incidents take longer to resolve, the disruption grows exponentially. With a central platform where

"Slack has allowed us to really provide the experience we want to deliver. The satisfaction of the customer always goes up, and the overall resolution time goes down."

Jon Brummel, Senior Manager of Enterprise Support, Zendesk employees can take swift, efficient action and keep stakeholders informed, they're able to shorten the incident *and* reduce its impact, not only for your customers and your bottom line but for your hardworking engineering team (who might finally be able to sleep peacefully through the night). Zendesk's senior manager of enterprise support, Jon Brummel, sums it up nicely: "Slack has allowed us to really provide the experience we want to deliver. The satisfaction of the customer always goes up, and the overall resolution time goes down."

slack

Modern incident response

slack.com