Howie: The Post-Incident Guide

DR. LAURA MAGUIRE, NORA JONES, AND VANESSA HUERTA GRANDA

jeli

Howie: The Post-Incident Guide

Welcome to the Howie guide to post-incident investigations!

The guide you're about to read will provide you with an explanation of how to get the most out of your incidents. This process has been developed by a number of leading experts in the field and shows the steps to conduct an in-depth investigation.

We affectionately call this process the "how we got here process" (or "Howie process" for short), and it is applicable to companies of different sizes and stages of maturity with investigation programs.

Why a focus on learning from incidents?

Recent events have shown how critical digital services are to individuals, organizations, and society as a whole. As software gets more entangled with all spheres of society, now more than ever, investigating and learning from incidents is crucial to maintain service reliability requirements so companies can continue delivering on their commitments to customers, keep employees connected and productive, and in many cases, preserve public safety.

As Nora Jones notes:

> *We're at an age in software when learning from incidents is pivotal to our companies' continued successes. There is a massive opportunity for software engineers to learn more about the applications of resilience engineering, human factors, and systems safety to their everyday work with the goal of learning how we can extract value and build expertise from incidents and surprises.*[1]

[1] Nora Jones, "Introduction," Learning from Incidents (blog), November 25, 2019, https://www.learningfromincidents.io/blog/learning-from-incidents-in-software.

When we think about learning from our incidents, we often don't have a good framework for what we can get out of this work. As noted cognitive psychologist and researcher Gary Klein explains in his book on human performance in everyday work conditions.[2]

Performance Improvement = Error reduction + Insight generation

So far, the industry has over-indexed in the "error reduction" part of the equation by emphasizing incident metrics like mean time to respond and not much on generating insights. By investing in learning and in generating quality insights from each individual incident, you will be able to provide context around your incident metrics and show a more complete picture of performance improvements.[3]

This guide provides some concrete strategies to help you begin to develop skills in generating insights and to help your company in developing an incident analysis program. It will start by walking you through the stages of an investigation: how to assign and accept an investigation, identify your incident data for analysis, prepare for interviews, and write a calibration document. As you wrap up your investigation, you will also learn how to lead a learning review meeting, complete an incident report, and integrate any additional findings and action items before you finalize and distribute your learnings within your organization.

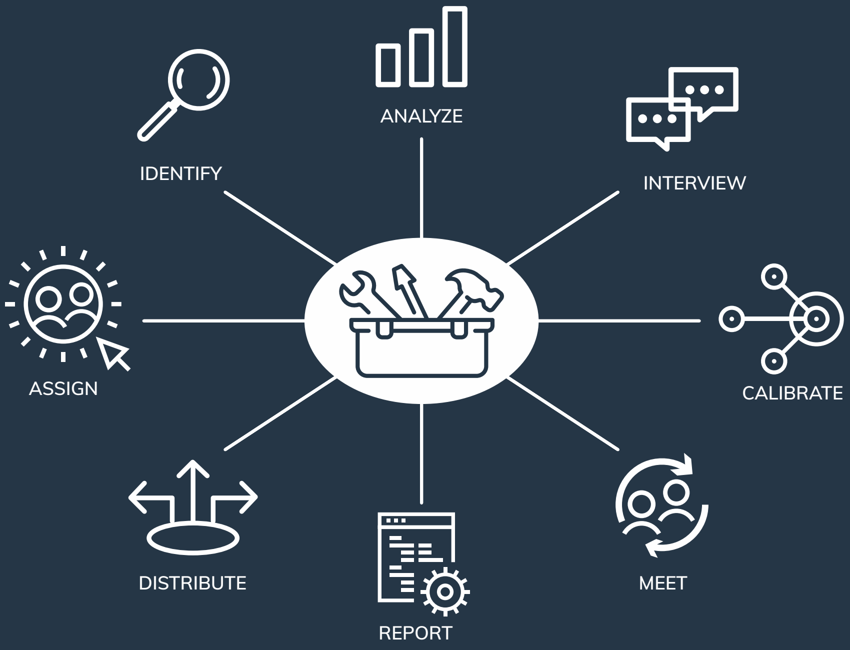
[2] Gary Klein, Seeing What Others Don't: The Remarkable Ways We Gain Insights (New York: Public Affairs, 2015).

[3] Vanessa Huerta Granda, "Making Sense out of Incident Metrics." Learning From Incidents, May 28, 2021. https://www.learningfromincidents.io/blog/looking-beyond-the-metrics.

While the steps outlined here represent a well-rounded way to review an investigation, our research shows that:

1. Every organization has different needs, strengths, limitations, and goals for their incident investigation process, so some of the steps may not be applicable to every organization.
2. Many investigators have constraints on how much time they can spend on an investigation, and some investigators are currently the only ones doing investigations, so it has to be efficient.
3. Incidents have differing levels of value for investigating incidents. Fundamentally, we believe you can learn from every incident but, realistically, we know that organizations are balancing tradeoffs between time spent in development or operations versus time spent in learning.

This means that an investigation process needs to be flexible and adaptable to the goals, interests and needs of the team or organization. We built Howie to be customizable for different sizes of organizations, skills of investigators, or levels of severity of incidents.



In this way, an investigator should think about this process as a set of tools in a toolbox. As you progress as an investigator and your company progresses with its incident investigation program, we encourage you to seek more tools to add! This will help you increase the number of insights gained in your investigations.

At the start of each investigation, you'll consider how much time you have, the availability of participants, and how much value the findings from the investigation will have for the company. High severity, very public events, or substantial near misses would use more of the tools provided here. We encourage you to take the parts that make sense to you at this specific time.

What we hope you take away from this is how to structure your post-incident processes and train others on them. We believe our guide will set you up for success in helping your workplace become a learning organization, one investigation at a time.

—Your friends at Jeli

A brief word about language in incident investigations

We introduce a number of terms in this guide that may be different from what is used in your organization. Generally speaking, we believe that getting the process right is more important than arguing over language. At the same time, many of the legacy terms used in the industry (such as “post-mortem,” “root-cause analysis,” etc.) come with a history of negativity. Using positive, specific language (such as “learning review” or “blame-aware”) is an important piece of building a culture of learning where folks are excited to be part of this transformation. We believe that language will always be evolving; in this guide we use a number of terms interchangeably (“incident investigation” and “incident analysis”) to reflect the way we use different terminology in our day-to-day work. We expect future iterations of this guide to present new terms and retire some of the ones we see here.

Glossary

Blame-aware – An evolution from "blameless," we recognize that everyone works with constraints and sometimes those don't appear until after an incident; we acknowledge our tendency to blame and name names and move past it in order to be productive.

Investigator – The person who will own the responsibility for the investigation all the way through the process (from initial analysis through distribution of findings); we outline a number of recommendations for what makes someone a good candidate for this role.

Knowledge elicitation – The process of gathering an expert's tacit knowledge (expertise and experience) underlying their performance. This is a sub-process of knowledge acquisition.

Calibration document – A document of initial findings put together by the investigator that will be shared prior to a review meeting to ensure proper alignment with interviewees and participants. This document should prevent any surprises from coming up during the review meeting. A calibration document can also be a draft to the final incident report.

Incident report/ how we got here report – A document sent out following the review meeting to all participants. This should be a learning document different from a post-mortem report in that its goal is learning. It is focused on the story of what happened and how events came to be.

Review meeting – A facilitated meeting where the investigator guides participants through the incident in order to uncover and share insights.

Action items meeting – A facilitated meeting or section of a meeting to focus on follow-up items uncovered during the investigation and where you can generate and assign any next steps.

ASSIGN

Assign the investigation

When your team or organization has had an incident it's ideal to mobilize your investigation process as quickly as possible to extract as much learning as you can from this unplanned event.[4]

Investigations need to be assigned to someone in particular. Though they can be collaborative, it's important that one person be responsible for moving the investigation forward. Assigning someone upfront also ensures that you're picking someone who has the capacity to take on an investigation and is in a good position to do so.

[4] DD Woods, "Report from the SNAFUcatchers Workshop on Coping with Complexity." Snafu Catchers (Columbus: The Ohio State University, 2017), https://snafucatchers.github.io/.

First, assign an investigator who will own the responsibility for the investigation all the way through the process (from initial analysis through distribution of findings). While this step may seem straightforward, not everyone will be a good match for every investigation.

This person:

Should	Shouldn't be...
Have a foundational level of knowledge of the components involved in the system	Someone directly involved in the response and mitigation of the incident
Be trained on investigation techniques, interviewing, and facilitating post-incident learning reviews (this guide may be a good first step in that direction)	Untrained, inexperienced or completely new to the organization In a position of authority over participants or the interviewees.
Be committed to establishing or reinforcing a post-incident process where participants feel safe	
Be able to dedicate time and attention to driving the investigation through to completion	

Why these things?

Someone with a foundational level of knowledge will be able to understand the technical issues involved. That person also being trained in investigation techniques, including knowledge elicitation[5] allows them to better surface information and ask better questions. Without someone who is committed to helping people feel safe, it will be difficult to get their perspective.

It's not recommended that someone who was directly involved in the incident investigate it because that can unintentionally bias them. Being directly involved can also prevent an investigator from being seen as a neutral third party. Similarly, the facilitator shouldn't be someone with authority over the interviewees in order to not create a fear of reprimand, concerns about looking unsure in front of management, or doubts around admitting to doing "the wrong thing," all of which can limit the learning that takes place.

We understand that every organization is different, and they may not be able to find investigators who meet all these requirements (some companies may only have one team doing incident reviews,[6] or a smaller startup may have everyone involved in every incident). If this applies to you, make sure to remind your team to take a third-party perspective.

[5] Nancy Cooke, "Knowledge Elicitation," (New Mexico State University), https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.457.339&rep=rep1&type=pdf.

[6] A dedicated Learning from Incident team carries pros and cons; they may hold some perceived authority, while being removed from a traditional chain of command allows them to investigate controversial topics without fear.

Accepting an investigation

If you've been asked to lead an investigation, awesome! We're here for you. A few things to consider when accepting an investigation are:

Do you have the time to handle your colleagues' potentially challenging experiences with care and attention?

A clumsily executed investigation can make things worse in terms of people's difficult emotions in the aftermath of an incident. In order to determine if you have the bandwidth necessary, think of the length of the incident and the conversation surrounding it because you will need to become acquainted with the whole thing prior to starting the incident investigation.

It's also important to consider the impact. Incidents with higher impact (e.g., it made the news, led to a large monetary loss) may be emotionally and politically charged, which can have an impact on participants and you as the investigator.[7] It's important that you're able to be impartial and empathetic to the situation.

Can you meet the deadline being set, or are you able to manage your workload to finish the investigation in a timely manner?

Some incidents will take a long time to give due diligence, you will have to balance thoroughness with prompt interviews (while the incident is fresh on people's minds).

[7] Incidents can trigger personal or organization trauma. They may bring up distrust and highlight power dynamics; if you suspect you are entering such a situation, your organization/teams may need to do more pre-work before starting the investigation.

IDENTIFY

Identify incident data

The first step is to collect incident data. Think of what data sources will give you contextual information to help you get started with your incident: chat transcripts, organizational charts, information about those individuals involved in the incident. Contextual information is the relevant background needed to make sense of the event. Things like: what teams are participants on? How long have they been at the organization? Who do they typically work with? What systems do they typically work on? How long have they been on-call for these systems?

You may already be collecting this information in a document, pasting it into a Jira ticket, or keeping old school printouts.

It's common for incident data to be spread across multiple communication chat channels. Take a look at the main incident channel and keep track of key players and their roles. Scan any potentially relevant channels (shared user or on-call channels, general company channels or specific component channels) to see if the incident is mentioned or search based on keywords/ticket numbers. If you find something, make a note of the channel and capture relevant messages.

ANALYZE

Analyze incident data

Incident analysis is iterative. You move from a general awareness of the incident to having deep knowledge of the event as you work your way through incident-specific data and other artifacts. As you progress in your investigation, it will inform your understanding of the technology, participants, and progression. At times it may be necessary to circle back to data or people you've spoken with to confirm or clarify new details as they emerge.

As you prepare for conducting the initial analysis, the first step is to get yourself familiar with the event. Sometimes, this step is easy because you were already aware of the event, so you know what happened and who was involved. Other times you may just get a verbal report from someone who was either in the event or tracked it in some way along with the request that you investigate. Other times you may be asked to investigate the incident without any context. Regardless of how you become the investigator, our recommended approach to conducting the analysis includes:

1. Orienting yourself around the initial data you have aggregated (transcripts, people data, alert logs, on-call schedules, dashboards, etc.) by tagging to organize your analysis
2. Creating a narrative and timelines of the event

3. Making note of the emerging themes and key questions remaining to be answered
4. Identifying any additional data you need in order to answer the questions
5. (Optional) Identifying and preparing for interviewees (if conducting interviews)
6. Compiling the data collected and themes
7. Consolidating your analysis, supporting data, and themes into a calibration document for review and/or to guide your facilitation
8. Your analysis should be refined and deepened following discussions in post-mortems or after a review from participants.

Let's look at each of these steps in more detail.

Tagging

A useful way to orient yourself to the event is to read over the data you've collected. This helps orient you to the event itself and helps you begin to make sense of different parts of the incident. For example, how did the event get detected? Who was brought in to help? How did they react to what was going on? Most investigators will immediately begin looking for information to assess the nature and severity of the incident and any key moments in time to help develop a timeline.

To begin to deepen this process, we suggest flagging events of interest and we refer to this as tagging. We suggest tagging with a defined set of words that group similar parts of the data around important aspects of the incident and how it was handled. To prepare for tagging, we see investigators cut and paste ChatOps transcript data into a text editor or print out hard copies of the data. Find a method that works best for you and that is flexible enough to let you work with the data all the way through to the report or meeting facilitation.

To start, the investigator reads through the transcript, tags key events, and begins building the narrative of the event. We recommend having a standard set of tags for your organization that everyone involved in an investigation can reference. What tags you use, their definitions, and how many you have will depend on how deep of an analysis you conduct. We've seen teams that just use a few tags to help them build the timeline and identify key moments in time (for example: detection, diagnosing, repair completed) and other teams that tag extensively, identifying things like when hypotheses about the contributing factors are raised and proved/disproved, when updates are provided to external stakeholders, sudden changes in system behavior, or actions that were taken to minimize impacts.

Tagging is often an iterative process. The goal is not to be comprehensive in your tagging at the start; that's a lot of pressure to take on and may not be necessary. Instead, think of tagging as a way to organize and hone your investigation. As we've mentioned before, the extent of your tagging and annotating will depend on how much time you have, how many people are involved in the investigation, and how deeply you want to explore the event.

You may only have time for the first pass; if you're able to spend more time tagging, you may be able to gather additional insights into your incident. There is no right or wrong—tagging is a process to help you see more in an incident. As you hone your skills as an investigator, you will improve your ability to draw out deeper insights from the data you collect.

Two basic tags that help support moving quickly to your next steps are marking any messages or events relating to how you'll tell the story of what happened with "narrative" and tagging anywhere you have a question for someone who was a part of the event as "participant follow-up."

What is the narrative?
A deeper analysis goes beyond simply recounting what happened in a basic chronological timeline. Instead, try to recreate the event as it happened, walking through the progression of the event and identifying what made it challenging or easy to diagnose and resolve.[8] Investigators who recreate the timeline by creating a narrative about what happened tell a story that allows for complexities and confusions to become apparent. This allows readers of a post-incident report (or participants in a learning review meeting) to get more actively engaged with the investigation since it tells a richer, more compelling account. Readers can imagine the situation the way it happened, not in hindsight when the outcome was known and it is easily understood what should have happened. Learning becomes clearer when you go beyond a simple timeline.

Here are some examples of things you as the investigator can ask yourself to focus your tagging and lay out the narrative to take an analysis deeper.

1. Look at what was happening at the beginning of the incident by asking yourself:
   - What did the responders think was happening?
   - Who joined or was recruited to help?
   - What information is available? What's uncertain/ambiguous? Who is asking? Who is answering?

2. Examine how the group was diagnosing the problem they face by asking:
   - What were the hypotheses being put forward? During this time there will be multiple hypotheses put forward, some of which endure and some of which will be quickly discounted or ignored (these are all signals you want to pay attention to).

[8] Sidney Dekker, The Field Guide to Understanding "Human Error" (Farnham: Ashgate Publishing, 2016).

- Who is proposing hypotheses about the potential sources of the outage? Seeing who proposes a hypothesis can be useful to narrow in on formulating a potential interview question for that person.
- Who is helping to prove or disprove these hypotheses? Most hypotheses are supported or disproved by others who provide evidence in the form of dashboards, log files, or specialized knowledge about how a piece of software works.
- What action was taken? By whom? Some actions may be taken to safeguard the system from further deterioration, others can be to gather more information or try to prove or disprove a hypothesis.
- Was there any ambiguity or confusion about what was happening? This is very common and is often a signal about the difficulty or complexity of the failure, not about the knowledge or skills of the responders.

3. How was the team working together and with others during the incident?
   - Where are examples of successful coordination between different parties involved? Incidents test practices and procedures and can identify opportunities for improvement or revisions to workflows.
   - Does a team proactively anticipate who will be needed to help resolve the incident and are able to easily bring them in? Recruiting specialized skill sets is crucial for speedy resolution, especially in hard problems. A key factor to reducing mean time to respond is smoothing out this coordination.
   - Where are communication breakdowns occurring? Are the responders able to share information quickly and easily?

Creating timelines

Incident timelines provide a way to orient a reader or learning review participant to what happened during the incident. Going beyond a text-based timeline and creating a more visual representation of the timeline allows you to see your incident from different points of view, craft stories (based on said points of view), and enhance collaboration. We recommend developing multiple timelines when you have the time to do so. This can allow you to focus a timeline to see the false-starts, red herrings, and progression of the event that can move past the idea that the incidents display a clean, forward progression between "detect, diagnose, and repair."[9] Many find that creating a timeline also gives them an initial structure for organizing the multiple data sources that can sometimes get messy. You can create timeline visualizations of events, keywords, specific participants, and different data types.

Making notes

As you work through the initial review of the transcript, you will come up with questions. If the question is specific to a particular message, you should leave a note for yourself or co-analysts to come back to it later and note who you want to reach out to for follow-ups.

An example of this practice would be if you see a message from a responder saying, "I actually think $SOFTWARE is involved so rolling back those changes should help." You might want to tag this as part of the narrative (since it was a proposed hypothesis about what was causing the issue, along with a suggestion about what would help), as well as a participant follow-up tag and add a note to yourself to ask that person, "How did you know it was $SOFTWARE? What did you notice that made that a likely culprit? Why did you suggest the rollback?" This way you can compile your timeline from your

[9] John Allspaw, "Incidents as We Imagine Them versus How They Actually Happen," Adaptive Capacity Labs (blog), November 5, 2018, https://www.adaptivecapacitylabs.com/blog/2018/11/05/incidents-as-we-imagine-them-versus-how-they-actually-are/.

narrative tags and arrange the questions you'll answer in your next steps.

Some other examples of questions you may have are:

- How does this piece of technology work? What is the history behind it at this organization?
- Where did this work start?
- What was the business reason behind it?
- How did we know to reach out to this subject matter expert?
- How did we find this information?
- What sorts of pressures were responders under?
- What does this (acronym, reactji, etc) mean?
- Who else knows this?

Identifying interviewees during your initial analysis

Reviewing the available data serves as an orientation to the event and sets the investigator up for deeper analysis if time and resources allow. After orienting yourself to the event through your initial review and tagging, you will have a general sense of who might be good candidates to interview.

If holding individual interviews is not feasible, it is still beneficial to identify key participants you might want to call upon in a review meeting or to aid with reviewing any reports that are generated.

We've said it before, and we'll say it again: analysis is iterative! As you work through reconstructing what happened and talking to participants, new sources of information will become available. As you review this new information, it may drive more questions to be answered.

A great example of this comes from an incident review one of the authors was leading. In the review meeting the investigator asked a participant how they noticed the source of the problem. It turned out this engineer had dealt with the issue so many times before that they set up a dashboard to monitor it and ping them when there was trouble!

When this was shown to other engineers, it generated a detailed discussion about the piece of software and the variability of its performance, and it identified other "explody bits" that other engineers felt were unstable and monitored more closely. In this way, as new information becomes available you may need to return to previously interviewed participants to follow up.

INTERVIEW

Interview incident participants

So far you have consolidated the existing data from tools used in everyday software engineering work to make it quick and easy for you to understand who was involved and what responders did during the incident. However, that data only tells part of the story. A lot of incident response happens offline: in direct messages, in face-to-face conversations, and, importantly, within the heads of those involved as they reason about what is happening and why!

Interviewing the participants involved can help elicit more details about what was confusing and why, the event, the response efforts, and surface important knowledge about the system (which includes the technical architecture but also teams, company culture, and communication patterns). Talking to different people involved one-on-one will expose the differences between what they believe happened and why. Often these deltas are used to run the most productive incident review.

This section is built on methods from critical incident technique[10] and critical decision method[11] for investigating incidents. It covers deciding who to interview, conducting the interviews, and working with the data collected after the interview.

Deciding who to interview

We are rarely given unlimited time to conduct an investigation, as many organizations seek to complete their investigations within a given time window or require the findings from the investigation to inform immediate work. Therefore, you'll need to decide how to use your time to provide the optimal insights for your investigation.

Who you will interview and how many people you will interview depends on several factors like interviewees' availability, the time you have to complete the investigation, and the amount of relevant new information you get from each interview.

Your initial analysis will help you identify high-value interview subjects. As you work through chat or audio transcripts, you'll notice key players. This often includes people who are leading the response (formally as incident commander or informally), who bring key insights (like relevant hypotheses about the problem), add important context (to validate/invalidate a hypothesis or to bring a broader perspective to the problem), or manages stakeholder relations that could impact response efforts (such as providing updates to leadership or customers to keep them in the loop).

[10] John C. Flanagan, "The Critical Incident Technique," Psychological Bulletin 51, no. 4 (July 1954), https://www.apa.org/pubs/databases/psycinfo/cit-article.pdf.

[11] Robert R. Hoffman, Beth Crandall, and Nigel Shadbolt, "Use of the Critical Decision Method to Elicit Expert Knowledge: A Case Study in the Methodology of Cognitive Task Analysis," Human Factors 40, no. 2 (June 1, 1998): 254–276, https://doi.org/10.1518/001872098779480442.

Don't worry about compiling the most comprehensive list of participants right away. As you conduct the first batch of interviews, you will learn about additional participants that you'll find are important to interview. Some suggestions for who could be interviewed are:

- Key players in the event – did they have a leading role or were they heavily involved in the detection, diagnosis, or resolution of the incident?
- People that might feel blamed – interviewing these participants can help alleviate fear and make sure their perspectives are accurately represented in the investigation.
- People that weren't expected to be involved (people that weren't on-call) – these participants can be critical sources of expertise and their involvement evidence of resilience within the system.
- People that were "lone wolves" (taking action independent of the group efforts) or exist on "islands of knowledge" (they were the only one who knew what was needed to resolve the incident).
- Owners (or former owners) of the impacted system.
- People who hold subject-matter expertise on the systems or components involved in the incident.
- Person that wrote the work ticket that prompted the person to write changes related to the incident.
- Person that wrote said change.
- People that are new to the organization – these participants can help surface hidden assumptions or contradictions.

You will find that interviews reveal interesting details about the system of work in general. You'll gain context into organizational change efforts that may have contributed to the event, team dynamics that help or hinder coordination, or external forces that force tradeoff decisions in the moment. As an investigator, you will face important decisions about how to integrate these findings into your analysis. It's necessary to include some of these details to place the decisions and actions into the broader context of how work happens in your organization. Manage your time constraints by stopping your interviewing when the amount of relevant new information drops off noticeably.

Sequencing

Knowing who to interview can help you as an investigator in managing your time. It is also important to consider how to schedule your interviews. Start with the "high-value interview" participants—the ones you think will give you the greatest context or the highest signal-to-noise ratio. That way if you run short of time you've targeted the key players.

Investigators often struggle with trying to schedule participants for follow-up conversations, so it's likely that availability of participants may drive your interview schedule, so be flexible and ready to ask your questions when a participant has time!

Some additional tips for sequencing interviews:

- If two interviewees are related in some way (for example, an engineer recruited a customer service agent into the event) start with the person who had the higher involvement or will have the most knowledge about the event.
- It's common to have to loop back to follow up with a participant after your interview if new information comes up in other interviews or during other parts of your data collection. You may wish to do this via direct message or email instead of a second interview to save time.

Length

How long you spend talking to a participant can vary depending on the interviewee's role in the event. We recommend a minimum of twenty minutes, but don't spend more than sixty minutes in a single session. In any case, you should respect your interviewee's other commitments, and plan the duration accordingly—it's better to finish early than run long.

Approaching interviewees

Incidents can be emotionally charged events in an organization—especially if there was substantial impact or the event was very public. Be conscious of the fear of being blamed when reaching out to participants for follow-up. Some people may be defensive or avoidant.

We recommend sending an informal email or direct message first to introduce yourself and the purpose of your outreach and to let them know you'll be sending an invite. Give them an opportunity to ask questions and, if you sense hesitation, reassure them the discussion will be confidential.

Send a calendar invite for a discussion or chat. Calling it an interview can be intimidating to some interviewees (it can come across as an interrogation or investigation). Include the details about the incident you are investigating and some information about how you are conducting the investigation (we've offered some guidance for what to say in the Appendix). Always give the option to opt out.

If the incident was contentious or difficult and you are not familiar with the interviewee, it can be useful to have someone who knows them (a colleague or manager) send an introductory message to help you build trust and rapport.

Preparing for the interview

Your preparation begins with analyzing the full scope of all the communication channels used to conduct the incident response (these may include chat transcripts, call recordings, etc.).

Review the participant's contributions in the channels, look at their team and tenure information, see who else from their team participated, and perhaps follow up on how they had participated in similar, previous incidents.

There are many different ways to conduct an interview. It may be informed by the nature of the event itself, personal preference, and the desired outcomes. As you develop more skills in interviewing, you will adjust your style. To start, consider the following:

- If you are new to interviewing, it helps to conduct interviews in pairs until you get more experience. It is cognitively demanding to be asking questions, listening for answers, capturing answers, and thinking of your follow-up questions simultaneously. Recording the interviews can help you revisit the answers, but shorthand notes will help you be more efficient in your analysis.
- Review your corporate policies about collecting and storing video and audio recordings of your colleagues.
- Pair with someone to scribe, who has also conducted interviews, to record the participants' answers. Having access to scribe notes can help you as an interviewer review earlier discussion points as the interview progresses.
- Encourage the scribe to aid the lead investigator with follow-up questions (over chat) or to jump in directly with questions.
- If conducting a virtual interview, have the scribe turn their camera off and mute their microphone so it's not distracting that they are taking notes. Conversely, the scribe can take notes by hand.
- If you do not have a scribe but are able to record the interview; make use of online transcription services to quickly and easily get a written record of the interview.
- Be mindful of time and your objectives with the interview. While open-ended questions give us broad context, they can run down your time, so if you have specific questions to ask make sure to leave enough time for them.
- Keep in mind that having a broad selection of threads to pull gives lots of places for insight during the learning review.

Kick off the interview right

As you start off your interview, you will want to make sure you are ready and bring any materials you have analyzed, including notes and charts.

Here's the pattern we always follow to get the conversation started smoothly:

1. When you start the discussion, introduce yourself and your scribe (if you have someone helping you take notes).
2. Explain what you are doing with the interview, that multiple perspectives help form a more coherent picture of what happened.
3. Say that you would like to record the interview so you can faithfully represent what they share with you.
4. Ask for the interviewee's consent to be recorded, but make it clear who will be reviewing the recording and how long you plan on retaining it.
5. Let them know if they want something off-the-record, you can stop the recording. In this case, none of the materials should be attributed to the interviewee but may be used as a jumping-off point for further investigation.
6. Explain to them the broader process of the investigation so they know how they fit into the bigger picture (that this interview will be part of the broader analysis that will get developed and distributed for feedback as well as shared with a larger audience).
7. Ask them if they remember the incident. The interviewee may not recall it well if it was a long time ago or they've been in multiple incidents since then. Ask if they need a refresh on the incident (you can either give a brief synopsis or have them review the channel).
8. Highlight the qualities of the incident that made it an attractive target for investigation.
9. Explain this is not about corrective actions
10. Ask if they have any questions before you begin.

Note: Productive interviews usually have a talking ratio of 5:1 (interviewee to interviewer). Your job as the interviewer is not to show knowledge of a situation (even if you do know about it), it is to extract what the responder knew about it.

To help interviewees feel comfortable with you and reorient themselves to the event, it is useful to start with general questions like:

- How did you first get brought into the event?
- What was your understanding of the situation as you were pulled in?
- From your perspective, can you explain what happened in the incident?

These questions can help get your interviewee talking in a natural way, allow you to find natural openings to ask about specific parts of the event, and can even provide you with a summarized point of view that is different from the one you arrived at during your initial analysis.

Getting more specific

Use details of the incident that you noted in your review of the transcripts to drive your questions. These are often things like:

- How did you get notified of this incident?
- What did you mean by $X?
- Tell me about the ordering of events?
- At one point you said: "$X"— what did you mean by this?
- At what point did you discover $POTENTIAL_MITIGATOR OR $POTENTIAL_ TRIGGER?
- What dashboards were you looking at? What were you searching for in $logs $dashboards? Can you show us?
- What was your comfortability with assessing the situation? How long have you been here? How have you seen things done?

- Are you frequently on-call or responding to things like $X? Is anyone on-call for $X? How did you feel it went?
- What surprised you in this incident?
- How did the shape of the incident response take place?
- Have some specific questions ready (the ones you tagged as "participant follow- up") but also allow the conversation to flow naturally.
- Ask for clarification as needed—better to have them over-explain something you know than to make an assumption.
- Ask for further clarification when interviewees share their opinions or counterfactuals.

After the interview

Go back through the interview notes and tidy up any sentence fragments, add context, and clean up typos. Spend a few minutes reflecting on the themes that emerged for you. You may want to identify ones that seem strong and ones that were weaker or would need further follow up. This should include any questions that remain unanswered or aspects of the event that are still unclear to you. This will help narrow your follow-ups. Identify anyone you'd want to interview next or if there are further questions to a previous interview. Begin your outreach immediately to keep the investigation moving forward. Link any supporting materials (including video recordings or transcripts) to your interview notes or documents you've begun compiling. Distribute the interview notes to co-investigators (as appropriate; you will want to be careful to not violate the privacy of your interviewee). Touch base with the interviewee later the same day or shortly after with a casual note like: "Thanks, I appreciate your insight, it is clear you have a lot of expertise in $X. If any additional thoughts come up, please send them my way." Continually provide updates to keep them in the loop and engaged in the process.

CALIBRATE

Calibrate on your analysis

After you've consolidated all your incident and interview data, you'll want to calibrate with your interviewees and incident participants to make sure you captured their input properly and there are no surprises during your meeting. You may do this by sharing your initial findings through sharing of notes or documents (including a draft of the incident report; we call this a "calibration document").

Doing this gives everyone a chance to clarify their mental models as well as make additions or corrections to your investigation.

The incident write-up or "calibration document"

We use a calibration document as a way of aligning with participants of the facilitated meeting about the event. This is not a final report; it is an interim findings document for interviewees to give the investigators feedback on the analysis and themes so far and comment on other topics that they'd like to include in the incident review meeting. This document can be used to start the final report.

The calibration document contains some information about what data has been reviewed to date, who has been interviewed, and what themes have emerged from this effort.

It should be shared in advance of the facilitated learning review to participants to add their comments and questions, which can help focus the meeting.

As you go through the analysis process, you'll have lots of different pieces of raw data. You might have transcripts from chat, some interviews, or maybe some service logs. By itself, raw data doesn't tell the story of what happened. That's where an investigator comes in—to consolidate the data. This is typically something you do while you're also collecting data and interviewing. Ultimately, you'll consolidate data in a few different ways. First, you'll start by identifying key themes, then you'll use what you've found to help build a visualization, and finally, you'll be able to refine that into a written document that will contain your findings.

As you work through the initial review, you begin to form an idea of the event and important aspects of the technical or coordinative difficulties faced. You can begin consolidating key themes as soon as they emerge from the data.

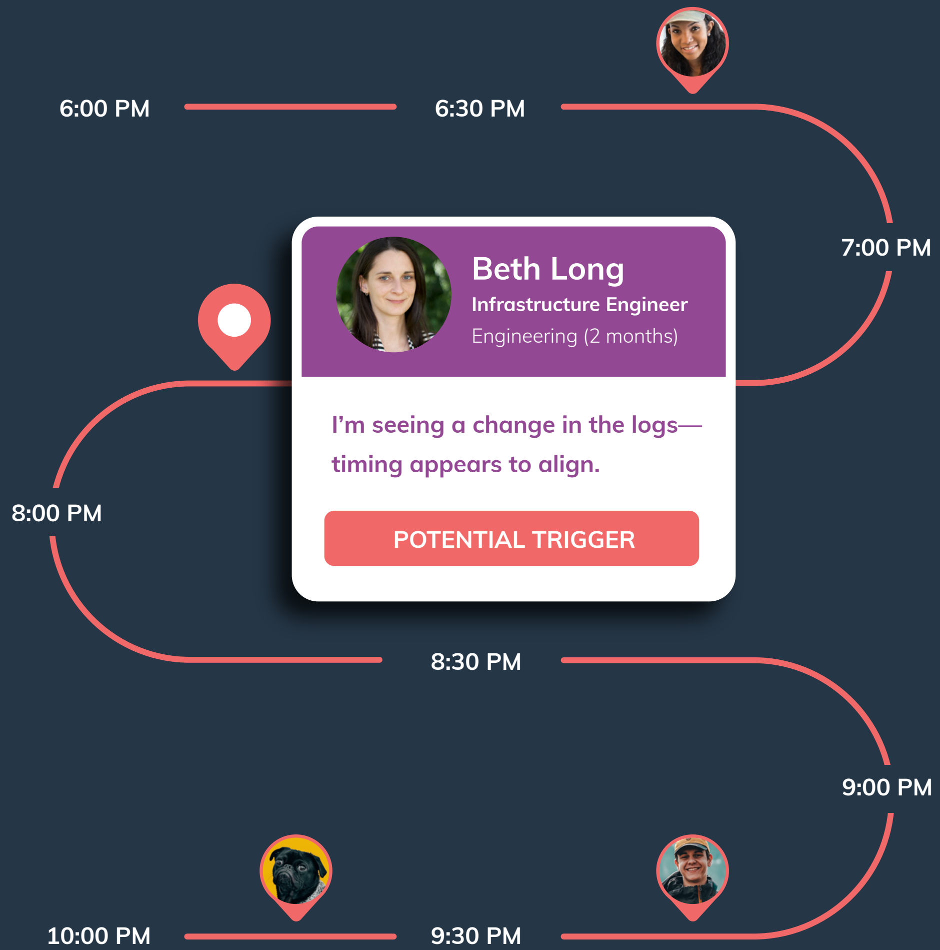
Consolidation of themes

Think of your themes as the topics of interest that surfaced throughout the investigation: what surprised you, what do you think others should know more about, what is shared among other incidents.

These can be aggregated in a collaboration document. You may find yourself with more themes than you will have time to review during the meeting; in this scenario, you can ask those involved in the incident ahead of time to help prioritize the top two to five themes to be discussed.

Consolidation of data as visual representations

There doesn't have to be just one timeline; in fact, you should create different timelines based on different points of view. For example, you might have different timelines that represent how different practitioners experienced the event.



I'm seeing a change in the logs—timing appears to align.

In addition to point-of-view timelines, you should also build a narrative timeline. This timeline will show key moments in the event, which you can use to facilitate your incident review meeting. This timeline can include things like when the first alert happened, when the issue was escalated as a major incident, when experts were recruited, when troubleshooting steps were taken, when hypotheses were developed or disproved, when impacts were noticed or changed, and anything else that you feel helps tell the story of the incident. This will allow you to walk through that story while asking for feedback from those individuals involved.

Consolidation of data in a write up document

Many organizations use some form of incident write-up to communicate the findings of the investigations. These may be in a document or take place within another kind of software system (like JIRA or OpsGenie).

We see this as a two-part process: First, producing a calibration document, followed by a more complete "how we got here" document. The first document will be used to ensure folks are on a similar page coming to the learning review meeting, while the second document adds to it with the findings from it.

Make sure you give others sufficient time to review and reflect on the document so there are no surprises during the meeting itself. It may help to ask specific questions when sending out this document in order to prompt feedback (and avoid folks only briefly glancing at it before the review meeting). You may ask:

- I want to make sure I captured this part properly; will you please review and let me know your thoughts?
- Are there any items that are missing from this document we should discuss?
- Is this technical detail correct?

You can find an example of a calibration document here.

MEET

Meet to review learnings

The incident review meeting is a facilitated opportunity to discuss, for the first time and as a group, how things happened, what unfolded, what was surprising, themes identified, and what is unclear.

This meeting itself is data that will be used for the incident review report. Everyone that participated or was impacted by the incident should have a calendar invite for this and anyone else should be able to request an invite.

Preparing for the meeting

To help the meeting go smoothly and to maximize learning in the time you'll have, you'll want to do a little bit of prep-work.

First, ensure any documents, screenshots, or materials you will use during the meeting have been reviewed by key participants and their feedback has been acknowledged and integrated.

Identify participants you'd like to speak with during the meeting. Remember that your role is to facilitate the sharing of knowledge and expertise among the group—use the experts themselves to describe what you learned. Reach out to them before the meeting and ask if you can call on them to explain something or describe their experience. Try not to catch people by surprise in the meeting, this can lead to defensiveness and limit learning.

Now you can lay out your agenda, circulate materials to all participants with sufficient time to review. This will allow everyone to come prepared, understanding how the meeting will flow and get a preview of what they'll see.

After the meeting, you can generate a brief three-to-four-question survey to circulate in order to capture the participants' experiences and suggestions for improvement.

Who should come to this meeting?

It's important for those who were involved in the incident to attend so they can share their perspective and recount their experiences where possible. Schedule the meeting to include as many key persons as you can.

That doesn't mean that those are the only people who should attend, though. You can also invite other participants; for example:

- Dependent service teams
- Engineers from related (but unimpacted) parts of the business
- Impacted users
- Customer success/advocate roles
- Management
- Key stakeholders

Ultimately, you should invite whoever is interested! Multiple diverse perspectives are crucial to making the learning review as comprehensive as possible.

Folks attending an incident review for the first time may be unsure of their role. As you will be the facilitator, you're in a unique position to be able to guide them! You should remind participants to be ready to:

- Communicate what happened from their point of view, how they experienced the incident, and how it impacted them.
- Listen to other parties; their experiences may be different from one another's. That's ok because it's how we all learn.
- Be open to discussion and collaboration. Don't assume any one answer or solution is the right one.
- Ask questions. If they don't know something, odds are somebody else in the call feels the same way.
- Think of how this incident can tie in with other events at the organization; feel free to share these insights.

Suggested agenda for the meeting

Here's a sample agenda you can use as a guide to circulate prior to the meeting.

- Intro/opening remarks to set context
- Structure of the process
- Narrative—this should be an interactive summary of what happened (calibrate)
- Themes from the interviews/questions we still have (keep these to two to five themes per incident, even if the calibration document goes through more)
- What's been done so far?
- Next steps—(or scheduling an action items meeting)

Running the meeting

We've talked so far about getting ready, you've figured out who to invite, and sent them an agenda with materials in time for them to review it. Now you're ready to actually facilitate the meeting.

We'll walk you through the process step by step, starting with the introduction and some ways you'll want to open the meeting.

Intro and opening remarks

You'll want to set expectations. If you're recording the meeting, make that clear and explain why. As part of those expectations, you'll want to explain the ground rules. Here are some we recommend, feel free to take or leave them as you see fit. We've included our recommendation as a script for you in order to make it easy; this way, if you need a reminder or are unsure, you can start by reading the following out loud:

"The meeting is intended to be blame-aware; we recognize that everyone works with constraints and sometimes those don't appear until after an incident, we acknowledge our tendency to blame and name names and move past it in order to be productive.[12] We will avoid counterfactuals[13] and remain respectful of each other's knowledge and experience.

The objective remains how to constructively help us get better at working together to solve the often-challenging problems we face.

One of the key discoveries in learning reviews is that different responders have different knowledge. A big part of this meeting is to have an open

[12] J. Paul Reed, "'Blameless' Postmortems Don't Work. Be Blame-Aware but Don't go Negative," TechBeacon, July 29, 2021, https://techbeacon.com/app-dev-testing/blameless-postmortems-dont-work-heres-what-does.

[13] Dekker, The Field Guide to Understanding "Human Error."

discussion that lets us share that knowledge and identify other potential knowledge gaps to increase learning.

We don't want to get too into the weeds. If a very specific technical conversation is better suited for another meeting or time, I'll gently take note of it and set it aside (also known as 'steer it to the parking lot').

This meeting is also not about corrective actions; again, these are important but will go to the parking lot for tracking to be dealt with in the action Items section.

Although this meeting is for sharing the findings, we will be asking different participants to recount their experiences or share the knowledge they contributed to the meeting. Because of this, the meeting may not follow the same structure you are used to."

You may wish to have participants write down the questions they have about the event and things they want addressed (and circle back to see if they got answered).

Start with an overview of artifacts studied (prior incident tickets, design review docs, meeting minutes) and methods (overview of the analysis process), number and scope of interviews, and how your analysis has been conducted.

Provide a narrative overview of the event. This is a short description of what happened and who was involved; include your interviewees in the narrative and have them explain from their perspective.

Next, you can address background knowledge gained during the investigation by having a subject matter expert provide some context on how the tech works so participants can learn about parts of the system they may be unfamiliar with and update their mental models.

After that, provide an overview of the themes, then ask for commentary from folks involved. Some themes may generate more commentary than others—that's perfectly fine! Once you've gotten some commentary, you can choose some of the themes to take a closer look at.

As you wrap up, ask what questions may still be unresolved. If there are none from the group, you may wish to share some from the investigation. Ask the "naive" questions; while we encourage participants to do so, they may not always feel comfortable doing so.

Next, to help everyone get on the same page, state what has been done so far.

Finally, discuss the next steps. This may include scheduling an action-items meeting or moving to that section of the meeting.

Priming the discussion

The aim in the meeting is to have participants talk more than facilitators. To do this you may need to prompt different participants (as noted previously, be sure they are aware in advance that you'll call on them!).

Some ways to generate discussion are:

- Ask some of the responders to describe the incident narrative; you may use the timeline you created to prompt discussion.
- Call on some of the subject-matter experts to explain how different parts of the system work.
- Have some of the impacted stakeholders talk about what went well and what was difficult for them (where constructive).

Closing remarks

- Get people excited about seeing the final write-up, let them know when to expect it and how they can help make it a living document!
- Invite participants who may not have previously seen the document to provide their input.
- Let them know what other events are being investigated with the Howie process.
- Solicit feedback to encourage participants to give their comments on the process. You may wish to reach out to individuals for feedback. Getting feedback from readers helps improve future write-ups, clarify any concerns, and engage participants. Some questions you may wish to ask are:
  - Was there something in this that strikes you as different from the "expected" way you've seen post-incident write-ups?
  - Is there any information we should add?
  - Will we get pushback on things in there?
  - Will we get pushback on things not in there?
  - Anything in there that you didn't know before about (team, component, business unit), and if so, what?
  - Is it easy enough to read that it keeps your interest after the summary bits at the top? (If not, what might make it more compelling?)
  - Does this writeup lead you to ask more/different questions about various bits that are involved? (If so, what are they?)
  - An alternative to a 1:1 follow-up is to circulate a brief two-to-three-question survey.

Action items/countermeasures meeting

Some guides recommend splitting out the action items meeting from the learning review. The purpose of this second meeting is to review any 'next steps' or follow up items raised during the incident review or during the investigation itself. This meeting is where you generate your work tickets, assign that work to responsible parties and track progression to help improve coordination of your teams and the components in your system. While we agree in theory this is a useful practice, we've found that many organizations struggle to hold even just one meeting. Therefore, we offer a compromise for those who will only have one review meeting and need to include them.

An effective approach we've seen is when teams make it the last section of their meeting. To avoid discussions of remediation creeping into your learning review, an important part of your role as a facilitator will be to keep each part of the meeting distinct by reminding participants the primary goal is learning. When an action item is raised, thank the speaker, quickly make a note of it and let them know you will refer back to it at the end of the meeting.

The key to quality action items is collaboration, ownership and reflection. Sharing the Calibration Document in advance allows participants to consider the right next steps and who would be the right group of people to work them. This approach allows time for greater forethought and more pertinent outcomes instead of shallow action items that will sit in a queue. Teams owning the work should be part of this meeting. We recommend inviting product owners, engineering managers, and project managers so that together you can all agree on the work required and the optimal time frame to achieve it.

Folks often think of action items as the "end" of an incident. However, your system is always changing and the action items of today can be contributing factors to the incidents of tomorrow. Therefore, refinements and learning are ongoing. This idea may be a "tough sell" for some organizations who just want closure from an incident. However, we believe a shift to continuous learning, along with integrating steps from this guide will better prepare you to adapt and handle future surprises.

Retro your retro!

Incident analysis is iterative, both you and your organization will get better with time and practice. Keep in mind that what works for other companies may not work for yours and that is ok!

We recommend you spend a few minutes reflecting on what went well, what could be improved, and how to handle next steps from the meeting, including follow-ups and integrating the feedback from the meeting.

If you circulated a survey, the responses can be a great starting point for this. Your own experience as a facilitator is important too! Was there a part of the meeting you felt went particularly well? Perhaps an area you felt could have gone better?

This is also when you'll want to go over any follow-up items that you may have generated and take care of those now.

REPORT

Report your findings

It’s time to generate a final report that will remain the organizational record of the event. If you’ve followed other processes before, like the “5 Whys” or the Google SRE model, you may feel like you’ve already done this, but there’s a difference. Here, you’ll be putting together a report that tells the story of how things unfolded, or “how we got here.”

When reports are one-dimensional, just a set of facts from a single point of view, they can be hard to learn from. We take a narrative approach to presenting the contributing factors to the event, background on the technology involved—including important historical context—and details about how the incident coordination was handled. It describes both the technical failures and the social and organizational processes involved.

Going beyond what broke and taking a broader view can make the investigation relevant to more people across different roles in the organization. For example, customer support can learn about what information is useful to provide during an incident or new engineers can get valuable background as part of their onboarding.

Generate your “how we got here” report

So far, you’ve gathered data from multiple sources, consolidated it by extracting themes, created a visualization, and possibly even done some interviews. You’ve created a calibration report that represents the story of how the event unfolded from multiple perspectives. Now is the time to finalize the findings from your investigations. Many organizations have a formal report they generate after an incident. We suggest creating a “how we got here” document that is sent out to all the participants.

A “how we got here” is different from a standard postmortem in that it is primarily focused on the story of what happened and how the events came to be. The goal with a “how we got here” report is to learn from the incident. This template was developed with our colleagues at Netflix, Slack, and Adaptive Capacity labs.

You may choose to start this document from your calibration document and add to it after your meeting.

You can find an example of the How we got here report here

Iterating on the report throughout the investigation

A key aspect of your role as an investigator and incident analyst is to ensure multiple perspectives are well represented in the finished product. This means integrating feedback from the calibration document and individual follow-ups so the comments are accounted for. Throughout your investigation you'll be collecting information to continuously update the document to include clarifications, feedback, new information, and important learnings from the review meeting.

Some organizations focus more heavily on the meeting and less on a written report. If this is your organization, you will still want to include a short overview in the document and link to a recording of the meeting, if available, to leave a record of your work and the subsequent discussions.

In addition, the action items should be added to this document to provide a consolidated view of what follow-ups are needed and help future readers to follow the full scope of the event and its outcome.

We recommend tracking analytics for the document. Seeing who is reading it and how often or how long after the event can provide lots of valuable insight into what is useful for the organization. You'll also be able to see where your distribution is working well and where it could be improved, which we'll tackle in the next section.

DISTRIBUTE

Distribute the findings

Your work shouldn't be completed to be filed. It should be completed so it can be read and shared across the business even after the learning review has taken place and the corrective actions have been taken.

The findings can be integrated into company newsletters, blog posts, or synopses presented at weekly or regularly scheduled team meetings. It's important that people in different roles get a chance to learn from the incident as well. While your incident may have primarily involved folks from engineering, everyone can benefit from the knowledge uncovered in an investigation. Also, having it available in different venues creates more opportunities for learning. Unless the report is read and utilized, learning can't occur; just writing doesn't guarantee learning across the organization.

Analytics or time-stamped commenting processes can be used to watch how and when the document is utilized long past the initial event. Knowing how (or if) people engage with the items you produce can help inform future reports. It can also give you insight into the things people are seeking to learn.

Investigation reports can become training documents, inform chaos experiments, serve as professional development and refresher training, and help enable meta-analysis across incidents.

Is it ever done?

As you can see, there is a lot that goes into incident analysis and infinite learnings to uncover from a single incident. So, how do you know when to end your investigation?

In 1996, Diane Vaughan released a book titled *The Challenger Launch Decision: Risk, Technology, and Culture.*[14] This book centers around the 1986 space shuttle Challenger disaster and the normalization of deviance that led to that fateful decision to launch. Vaughan spent almost nine years researching, writing, and editing what some would call a manifesto; the pinnacle of incident reviews. She realized that a great analysis of an incident can be iterated upon and researched thoroughly over many years. The work is never truly done.

As a practitioner of incident analysis within your organization, you probably won't have nine years to review your incident (even the one that took your entire web server down for hours!). At some point, you want to complete your investigation. The good news is that you can complete an investigation while letting others continue to contribute to it and learn from it. When closing your investigation and finishing your incident report, you want to ensure that it is read and, if needed, iterated upon in the future. As more people read the document, more information becomes available. Creating "living documents" that can continue to grow and represent new knowledge and experiences will maintain their relevance and value to your organization.

So go ahead, hit send, and watch your investigation take a life of its own!

[14] Diane Vaughan, *The Challenger Launch Decision: Risky Technology, Culture, and Deviance at NASA* (Chicago: The University of Chicago Press, 2016).

CLOSING THOUGHTS

At Jeli we believe in the power of taking a proactive approach to incident analysis to help you truly understand how you got here.

We believe that incident analysis can be your organization's secret weapon that will allow you to gain value from your incidents. We understand that good incident analysis is an investment, so we hope that this guide will help you push toward that change.

We also believe that the information laid out here will continue evolving. We will continue releasing additional materials to help you understand and apply the concepts in this guide as well as publishing revisions as the landscape changes.

Thank you for reading!

CONTINUED LEARNING FOR INVESTIGATORS

Developing skills as an investigator and analyst is an ongoing process. Below are some resources to help you level up your game.

www.learningfromincidents.io
A software engineering community based on resilience engineering, incident analysis and sharing of experiences. The blog posts are updated regularly.

Etsy's Debriefing Facilitation Guide
A comprehensive guide for facilitators developed by John Allspaw.

Two Views on Human Error
Dr. Johan Bergstrom from Lund University discusses two views about human performance and error common in safety sciences today.

The Three Traps in Accident Investigation
Dr. Johan Bergstrom from Lund University describes how investigators can misrepresent what really happened during an incident.

Resilience Engineering Repo
A well-curated repository of papers and talks associated with resilience engineering.

The introductory guide is a good place to start.

How Complex Systems Fail

The Error of Counting "Errors"

Laura Nolan's Incident Review Catalog

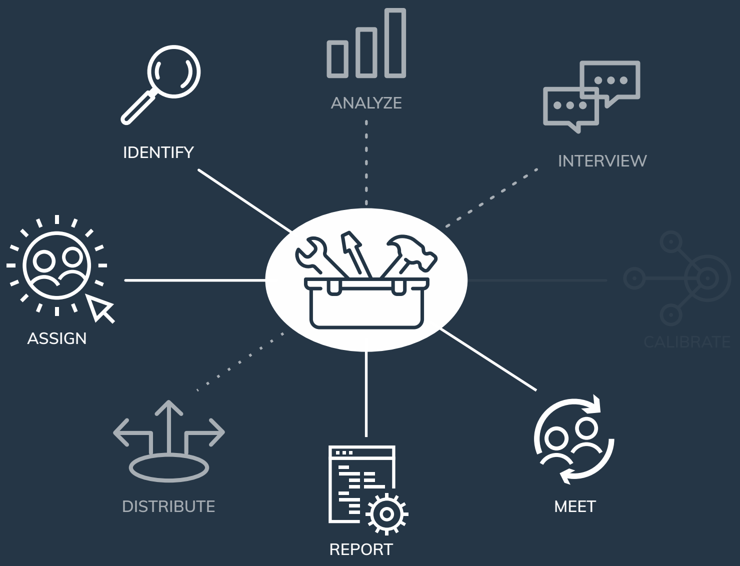
APPENDIX A

Using the Starter Guide to adjust the Howie process to fit your organization

As mentioned at the start of this guide, the Howie process can be adjusted depending on the specific context of your team, your organization and the goals for introducing or improving an incident analysis program. Here are two examples from companies that have adopted a Howie process:

Large company developing their first company standard

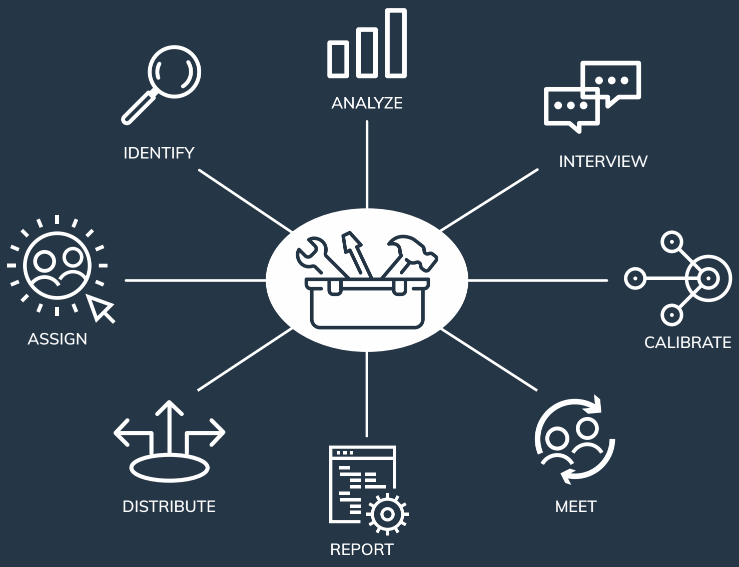
BoomBox, Inc. was a large multinational company with a centralized dev tools team that sets the standard for how to do incident analysis within the company. While some individual development teams were already doing a brief root-cause analysis after an outage, the core group wanted to introduce a standardized incident review process to maximize the time spent in reviews. To give their dev teams some guidelines without being too prescriptive, they adapted the full Howie process to help their dev teams get started. They rolled out this adapted process to begin building the muscles of doing consistent reviews in a lightweight way.



As they get more buy-in, they plan to introduce more steps (the dotted lines) to their analysis process to get deeper insights, involve more of the company by interviewing, and focus on sharing the findings more broadly outside of involved teams.

Mid-size company improving their existing practices

FastMover, Inc. is a growing company with a strong culture of continuous improvement among their many autonomous dev teams. The teams regularly hold post-incident reviews, but they wanted to get better at them by emphasizing collaboration and engagement. They adapted a Howie process to introduce analysis with Jeli, interviewing, and using the calibration document and training facilitator to make the most of their meetings.



APPENDIX B

Introducing a new investigation process

Organizational change management is a critical aspect of introducing a new investigation process. Give your new process the best chance of adoption by communicating its intent, how it will impact the company and how the reader can provide support or get their questions answered. This aspect of introducing new practices could be its own guidebook! We encourage you to learn more about how to understand the needs of individuals and teams within your company, develop the practices to best support them, influence change and create sustainable performance improvements at your organization.

At a minimum, as you introduce this new process for the first time, have some verbiage and documentation ready to share, as folks may be unfamiliar with this new approach to incident analysis. We often use the following:

We are improving the “after the incident” phase at $COMPANY and taking new approaches to the “after the incident” phase—specifically focusing on incident analysis (learning from incidents), and getting the most learnings we can out of incidents.

An important thing to remember is that we are at the beginning of how we handle the “after the incident” phase. What we’re doing with this phase now will help shed light on how we are doing as an organization and how we can improve.

As we roll out more comprehensive investigations, you'll notice they have the title "X" to specifically focus on how we got to this specific incident, including digging into historical incidents and decisions made at $COMPANY.

Q: What are the components of a strong incident analysis?

1. Incident occurs
2. Investigation assigned
3. Investigation accepted
4. Initial analysis by investigator to identify interviewees and insight generation
5. Investigator analysis of disparate sources
6. Individual interviews
7. Calibration document (align with participants on the event)
8. Facilitated post-incident meeting
9. Report/incident dissemination
10. Action items meeting or document

If you have any questions on what we're doing/what the plan is (in the meantime), please reach out to @$PERSON and we can chat.

APPENDIX C

Handling concerns & objections

These are some frequently asked questions you might get when sending out any communications on your investigation process changes. You can edit and adjust these to match your company's needs, then make this a pdf and attach it to an email or share it internally.

Q: This is a much more thorough and clearly interesting approach than what we have been doing, but how will this new approach to incident analysis scale? Doing this sort of investigation takes much more time than we're used to—we can't possibly spend this much time doing it for every incident we have!

A: Yes, doing a strong incident analysis for each and every incident that occurs at $COMPANY wouldn't be feasible! But there are two parts to this answer:

1. Taking this different approach to analyzing incidents will get easier and more efficient over time because doing this involves expertise. Doing this work effectively is the same as with software development—a more experienced engineer can write more valuable code in less time than a novice engineer.
2. Different incidents warrant different levels of analysis. Incidents are much more unique than they are typically understood to be. Therefore, the time/attention/effort to analyze them should be relative to their potential to reveal insights about $COMPANY's practices, systems, history, expertise, etc.

In other words, we don't want, nor need, to do the same level of analysis for every incident. The challenge we face is to develop the skills to recognize which incidents have a greater potential to reveal valuable insights and which ones don't. For those that do, we'll squeeze as much as we possibly can out of them. For those that don't, we won't.

Q: What are elements or qualities of an incident that signal high potential value and warrant a "stronger" investigation?

A: There is no prescriptive formula for this, and we will get better at recognizing these as we become more experienced, but here are some examples of incidents that might deserve more attention (this is not a complete list!):

- There were multiple (> 2) teams involved
- A new service or interaction took part in the event
- It involved misuse of something that seemed simple or uninteresting (hint: there's usually more to dig into here (e.g., expired certs)
- The event involved a use case that was never thought of—indication of a surprise
- The event was almost really bad
- It looks like a repeat incident
- There is a lot of discussion around the incident
- There was confusion in or around the event
- The incident took place during an important event (e.g., an earnings call)
- There is an interest in investigating it further (there is no prescriptive formula for this)

Q: Can I request that an incident I was involved in be investigated for deeper analysis?

A: Yes! For now, please reach out if you have an interesting incident you think could benefit from further analysis, and we will follow up. We are always interested and willing to engage with people that are interested in getting a "deeper look."

Q: What's the story with follow-up/action items in this new way of doing things?

A: All incidents produce an organizational drive for 'improvement' and our company is no exception to this. As Todd Conklin of The Pre-Accident Investigation podcast said, "The problems begin when the pressure to fix outweighs the pressure to learn."

Research has shown that when action items generated in a post mortem meeting they can distract from exploring and understanding the event in a more valuable way and are often rushed and not fully thought out. As a result, many action items are either dismissed, completed but not valuable, or forever remain on a backlog because, upon some further reflection ("soak time"), people who initially suggested them may realize that they were not likely to produce the effect they intended when they came up with them.

After separating the creation of action items from the learning part of the meeting itself, the postmortem meeting is then dedicated to developing a deeper and better understanding of the incident, and attendees commit to taking some (short!) time to consider what countermeasures or action items are likely to be genuinely valuable. The collection/collation of these ideas can even be done asynchronously in a day or two after the group meeting.

It's recommended to remind attendees at the beginning of meetings to keep a running list of notes about potential action items as the meeting unfolds and use these notes as fuel for dialogue with their teammates and consideration for formalizing them after the meeting.

Q: What happens if my team is involved in an incident that is chosen to be analyzed via this new way?

A: All of the people involved in the incident will be engaged in both the preparation for the post-incident meeting and the resulting document based on that meeting. The people involved in the incident will still be involved in this process and will be actively consulted to ensure that the artifacts the investigators produce are technically accurate and that people involved in the incident are being well-represented. Generally speaking, what you can expect might happen includes:

- 1:1 interviews between an investigator and an incident responder (or someone related to the incident). The investigator might ask you questions like: What happened from your perspective? How was it noticed? How was it handled?
- All of these questions will be asked with the goal of understanding what happened and how we got here.
- All people involved in the incident or experts in a system involved in the incident will be contacted after the initial analysis from the investigators. This contact will be done prior to the postmortem meeting to ensure that what the investigators are understanding is technically correct.
- All people involved in the incident will be invited to the postmortem meeting and are encouraged to participate and contribute to the discussion—this is not a presentation, but rather an opportunity to learn more about the incident and develop a deeper understanding of the events leading up to it and the themes that the event brings up.
- The postmortem meeting provides a forum to discuss some of these themes.
- The investigators will come up with a report. The report will be shared with folks involved in the incident prior to sharing it more broadly—the folks involved have the opportunity to engage with the report, shape the report, and use the report as a way to stimulate discussion about potential action items that they may want to add (even after the report is published).

ACKNOWLEDGEMENTS

Thank you to all the Jeli Beans that helped support the launch of this guide, with long days put into section rewrites, editing, and re-reading for continuity, especially Daniela Hurtado, Emily Ruppe, MacKenzie Wardwell, Thai Wood, and Will Gallego.

Finally, we appreciate the support of all those who worked on this guide for review and feedback, this Guide would not have been possible without you:

- Danesh Abeyratne
- John Allspaw
- Morgan Collins
- Jessica DeVita
- Alex Elman
- Dara Garvin
- Fred Hebert
- Lorin Hochstein
- Ryan Kitchens
- Duck Lawn
- Yanet Leon
- Chris Mitchell
- Courtney Nash
- Tim Nicholas
- Laura Nolan
- Paul Osman
- Nick Stenning
- Noah Sussman
- Chad Todd

jeli

LFI Learning From Incidents

REVISED 12/02/21