I will be discussing a number of upsetting topics in theory, because I am drawing an analogy to emergency response situations in the physical world. There will be no details and no actual scenarios. I won't be going into any of this until slide 8, so if you need to step out, you have time to do so. Please do what you need to do to take care of yourself.
What would you do if you
hypothetically
woke up, checked slack while you were still in bed
(I know you wouldn’t do this)
and saw
for anyone who may not be able to read this, it's a slack message from our AWS TAM which says "Can you please look into this case # blah, your AWS account number blah is compromised"

and since you don't have your AWS account IDs memorized (if you do, please don't tell me) your mostly-asleep brain assumes it's the BIG account
“i’m gonna need some coffee”

this is what my brain did
but seriously

@hashoctothorpe

if this happened at your company, do you know what you would do? Is there someone you could call? do you know how you would reach them? do you know the answer to that now, or would you need to look it up?
Hi, I’m Courtney. I’m an SRE and incident response specialist, and I’m here to talk about what to do when everything goes wrong.
this talk is about emergencies

fundamentally, what we are talking about here is an emergency
the most common definition of emergency is “a situation that poses an immediate risk to health, life, property, or environment”
depending on your business, any of those could apply to you, but property (or business reputation) is probably the most common
this is something lots of coworkers and conference friends have said to me- “nobody’s gonna die”. But do you KNOW that, though? Let’s say, for the sake of argument, that you actually do know who alllllll of your customers are (which you definitely don't, but let’s pretend). Do you know who THEIR customers are? And do you know alllll the workloads alllll of those people are doing? Do you know that allllll of them are only using your system in the expected ways?

There’s no way to know the fourth or fifth order impacts of an outage of your system, so saying that no one will die as a result of your outage is making an assumption which may be unwarranted. I don’t say this because I want you to freeze, but because I want you and everyone you work with to take incidents seriously . It doesn't make things better to have a loose and poorly-specified incident response protocol, even for very small incidents that are easily corrected or that only a few customers notice.

AND if you work electronic medical records, you DEFINITELY cannot say this.
possibly you’ve heard productivity people talk about urgent vs. important
Urgent is about *timeline*. If something is urgent, it must be handled quickly (do you want to order lunch with your office friends?)
Important is about *needs or consequences*. (Making sure you have your medication refilled or that you know where your children or pets are). Important can be about *danger*. 
So an emergency is both urgent (time-sensitive) and important (about danger or consequences). A fire would be about both danger and consequences, a broken bone from a bad fall would be about consequences. How do we KNOW it’s an emergency, though?
well, someone has to know about it, assess the urgency and importance, and decide it is
that means someone has to find out about it
in the physical world, maybe you see something happen or come across someone in distress
in our industry, that probably means you get paged- hopefully by a monitoring service, or maybe by your support staff and then they have to decide how to respond - physical world, 911 or an alarm company? in our industry, page more people?
“I didn’t have time to think”

How many times have you said this, or heard someone say it to you? thinking takes time also if you don’t know what the options are, you’ll freeze or panic So we need to eliminate the need to think for as many people involved in the emergency as possible that’s why calling 911 connects you to a dispatcher who can reach all the common response teams directly- so you don’t have to take a moment to decide who to call and figure out how to reach them
This is a picture of the sign on the back of my hotel room door in Toronto, where I first gave this talk. Hotels across North America (and probably in other places too) have signs like this in every room, just in case you should need to call for help or evacuate the building.

Both the US and Canada use 911 as an emergency number. 911 creates a framework for response - it represents years of planning and communication, including these signs the dispatcher knows:

- who they can call
- how to reach them
- how to get information from you about the situation you’re reporting
- to remind you to keep yourself safe - critical

This framework enables you to respond when you encounter an emergency if you don’t know what the options for help are, you don’t know what to do.
calling 911 also triggers the response framework used by the dispatcher and emergency response specialists
fire personnel, EMTs, and police have plans for
  ● how to reach the emergency (assemble)
  ● how to stay in contact with the dispatcher while they do
  ● how to assess the emergency when they arrive
  ● how to communicate within their group and across groups (at a fire, fire personnel have to coordinate with medical personnel).
  ● how to escalate (summon more fire trucks)
The details vary by country- Canada’s is called An Emergency Management Framework for Canada, the US uses the National Incident Management System
what have we learned?

- Frameworks enable people to respond quickly and effectively
- They define emergencies and how to get help (call 911)
- They tell responders how to answer a request for help
  - how to assemble (ambulance, fire truck)
  - how to communicate (radio, phone)
  - how to assess the situation (what’s happening? is there danger?)
  - how to delegate
  - how to disperse (how do we decide the situation is handled?)

there’s a lot of text here, don’t worry about reading it all- we’ll revisit each part
Frameworks are about organization and planning
If you discover something that might be an emergency and your mind goes blank, that means you haven’t been *enabled to respond* - you don’t know what you need to know in order to react
responding to a friend confessing suicidal thoughts
responding to a security issue
let’s apply this

now that we’ve talked over all that, we can talk about creating an incident response system for your organization. the best way to do this is take a national system and adapt it to your needs and tools. the rest of my talk will give you guidance for doing that.
what’s an emergency?

you need a way to know there’s something wrong, so you need monitoring and alerting that you have some confidence in
then you need to decide what constitutes an emergency for you. in a commercial context, this will usually mean that people either can’t use what they’re paying you for, or they can’t pay you in order to start using it
examples: not being able to buy things on Amazon
not being able to launch a new app on Heroku
how do I get help?

like 911, if you make people decide who to engage or look up how to engage them, you’ll waste precious time
make sure you have a single point of contact, that it’s easy to use/remember, and publicize it widely (some companies use chatops commands in slack)
the people it reaches should be able to fill the role of the dispatcher- figuring out what the issue is, who else to engage, and how to reach them (probably want some technology to help with that, this one of our pain points)
those people are probably going to be the same people trained as incident commanders, and unlike the 911 dispatcher, they will probably continue to manage the incident response as it progresses

ONCE YOU HAVE AN EMERGENCY, IT CAN’T BE SOLVED BY ONE PERSON. Emergency responders in the physical world are almost always sent out in pairs or larger groups, because when you have something both urgent and important, you need the resources of multiple people and skillsets to turn it around. Incident response is a team sport.
how to assemble

- (ambulance, fire truck)
- (conference call, Slack)

how to communicate

- (radio, phone)
- (conference call, Slack)

in physical space, “where to go” is sometimes ambiguous (for instance, natural disasters won’t necessarily have a single street address), but usually, responders will congregate in person and use radios (or occasionally phones) to communicate. You will likely need to decide on a digital “site” for your responders to join, and that “site” will be the same as your communications infrastructure - conference call, Slack etc.

The specialists who join your incident response will also need to assemble at this site, and they should not leave it without designating a replacement or being released by the incident commander.

Make sure this site is likely to still work if your own infrastructure is down, and have a contingency plan if your site isn’t working.
how to assess the situation

in our industry, you’ll probably be looking for impacted systems and customer experience.

identifying impacted systems means you can get the right people to join your incident response.
identifying the customer experience means you can tell customers what issues you are aware of, so they know you’re working on it (and so they will still open support cases for *other* issues).
this is an ongoing task for the incident commander—depending on the issue, the answers to these questions could change during the course of your response, based on the environment or your actions.
the essence of successful incident response is cooperation and delegation
no one can handle this solo, and that means dividing up the work
considerations for dividing it up include avoiding duplication of effort and parallelization
it also means that all the people handling this work need to report back to the incident commander on a regular basis

how to delegate

@hashoctothorpe
For the duration of the incident, the incident commander is the start of authority for the company.
The incident commander is the only one with a view of the whole problem and all of the people working on it.
even if everyone’s in the same slack channel, the ic’s only job is to pay attention to this.
that means it’s critical that no one argue with or countermand the incident commander- not other responders, not managers or execs.
doing so means that everyone helping with the incident has to decide whose side to take- the incident commander or the person arguing with them.
that wastes time and is ultimately unproductive.
it also means no one leaves until they are released by the the IC or replaced.
you need some criteria for when you decide things are done! sometimes that's clear-no more impact, we rolled it back, etc but what if it's:

- we mitigated it, but we won't have the fix from the vendor for three weeks?
- what if it's: we can’t mitigate it, and we won’t have the fix from the vendor for three weeks?
- what if it's a security incident and now everyone in the company has to patch their Redises and it’s going to take three weeks?

start by coming up with a few high-level plans for cases like this when they happen, you can use those plans as a starting point
a special case of assembly and dispersal: shifts

Operational incidents can be very quick, but they can also last hours or days, and security incidents sometimes last weeks. You need an idea of what a shift is and what the process for a shift change should look like. I strongly recommend 4 hours—this is what we found people could handle as incident commander, empirically. It was also what I learned in classes with fire personnel.
MVP

- Is this an emergency?
- People who know the relevant subject areas (EMTs, API team members)
- Someone who knows how to organize them (incident commander)
- Place to assemble
- Way to communicate
- Shifts
- How do you tell when it’s over?

those of you who like to take pictures of slides, get out your phones
here’s the summary- here’s your minimum viable incident response plan
there’s a lot more to it than this! but here’s how to get started
if you cover this stuff, you’re on your way
and then you need TRAINING

at the barest minimum, you need training and documentation for your incident commanders
you will get much better results if all of your engineers are trained as if they were incident commanders themselves! they’ll know what the incident commander needs and more importantly why
reduces grumpiness
next steps

- how do you communicate with the customers while all this is happening
- how do you engage the lawyers
- how do you engage the PR people
- how do you engage the executives
- how do you engage your vendors
- how do your vendors engage you
- PROFIT

there are lots of places to go from here! this is just the very beginning steps-something to get you going, to help you understand the problem and its parts
so what actually happened?

for those of you still wondering about the story I started this talk off with
the account in question was a brand new dev account that had its creds checked in to
GH by accident first thing
BUT several other people also heard that we had an account compromise and came
to find me about it over the course of the day, so that was fun
Further resources

- Wikipedia: Incident Response System
  https://en.wikipedia.org/wiki/Incident_Command_System
- Incident Management for Operations by Rob Schnepp, Ron Vidal, Chris Hawley:
  http://shop.oreilly.com/product/0636920036159.do
- Emergency Management from Public Safety Canada:

- Wikipedia: Incident Response System
- Incident Management for Operations by Rob Schnepp, Ron Vidal, Chris Hawley
- Emergency Management from Public Safety Canada
Things I want to read

- A Paradise Built in Hell: The Extraordinary Communities That Arise in Disaster by Rebecca Solnit
- The Survivors Club: The Secrets and Science that Could Save Your Life by Ben Sherwood

- A Paradise Built in Hell: The Extraordinary Communities That Arise in Disaster by Rebecca Solnit
- The Survivors Club: The Secrets and Science that Could Save Your Life by Ben Sherwood
Acknowledgements

● Marlena Compton, for reading over a draft of this presentation and providing encouragement
● Mental Health First Aid Canada, for helping me take care of other people better and for showing me what it feels like when you know what to do (https://www.mhfa.ca/)

● Marlena Compton, for reading over a draft of this presentation and providing encouragement
● Mental Health First Aid Canada, for helping me take care of other people better and for showing me what it feels like when you know what to do (https://www.mhfa.ca/)
Thanks

Courtney Eckhardt (@hashoctothorpe, she/her)