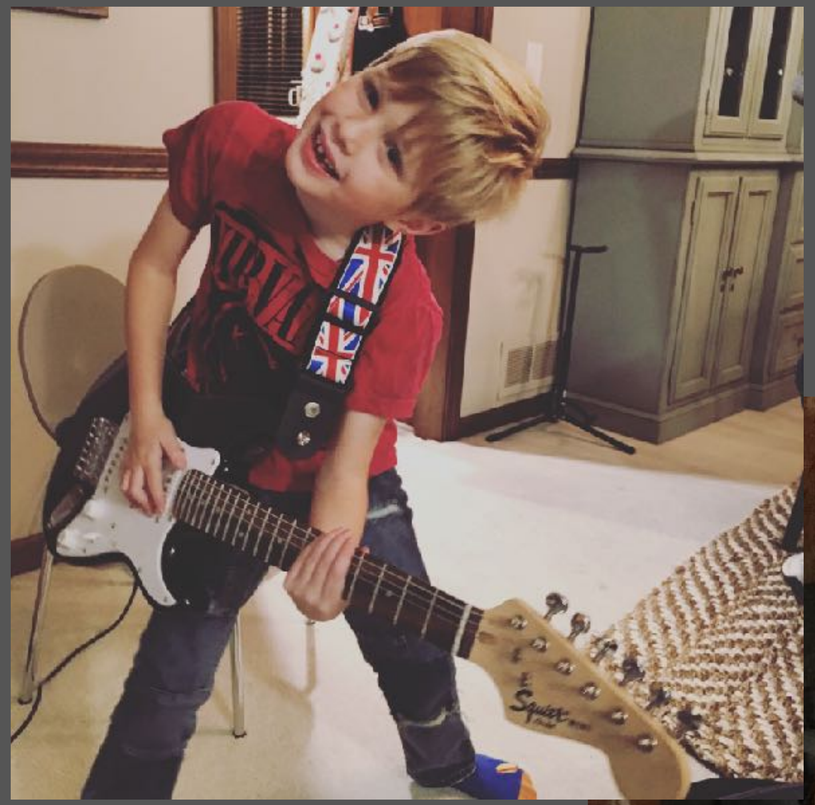
pagerduty

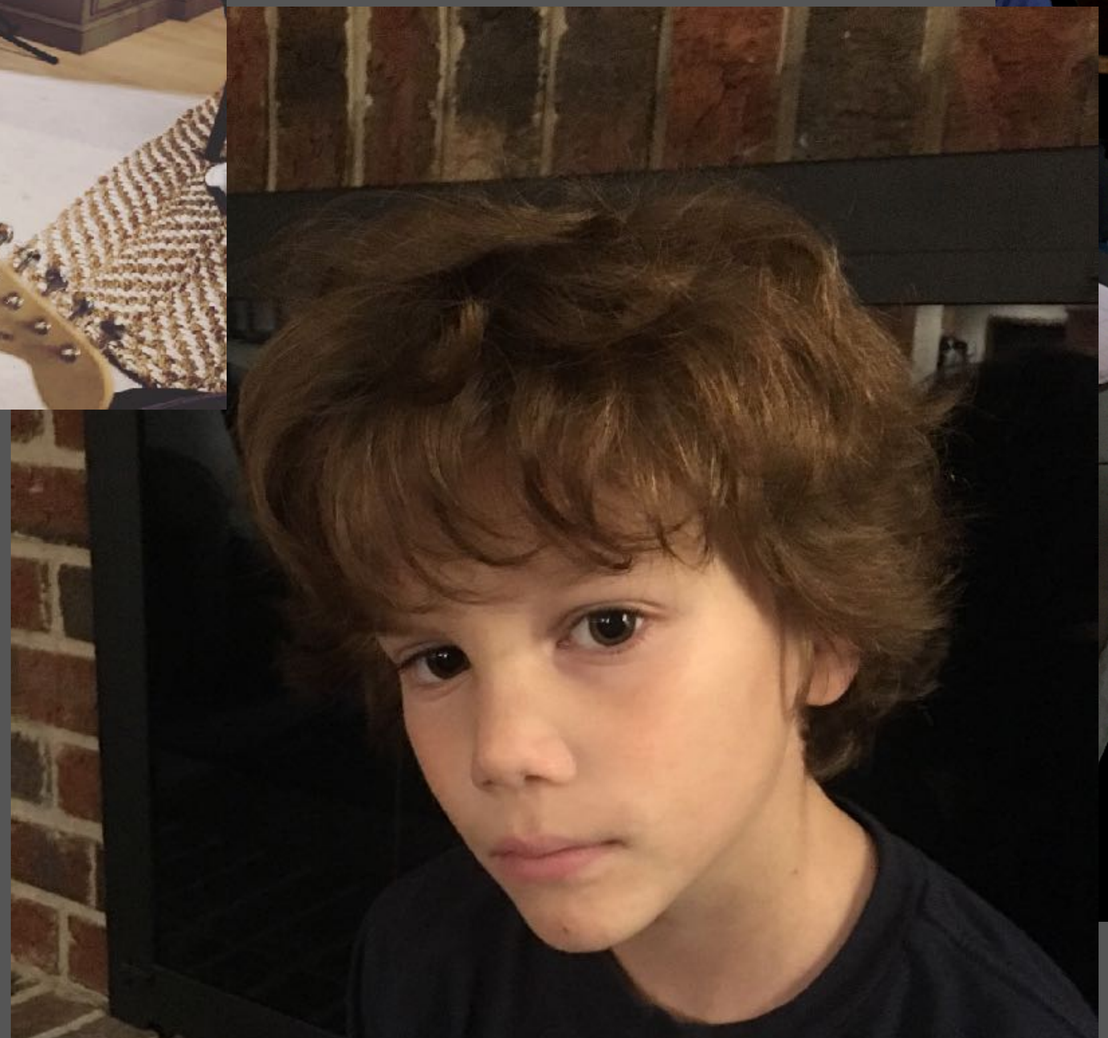
Incidents & Accidents

Matty Stratton, DevOps Evangelist, PagerDuty

@mattstratton

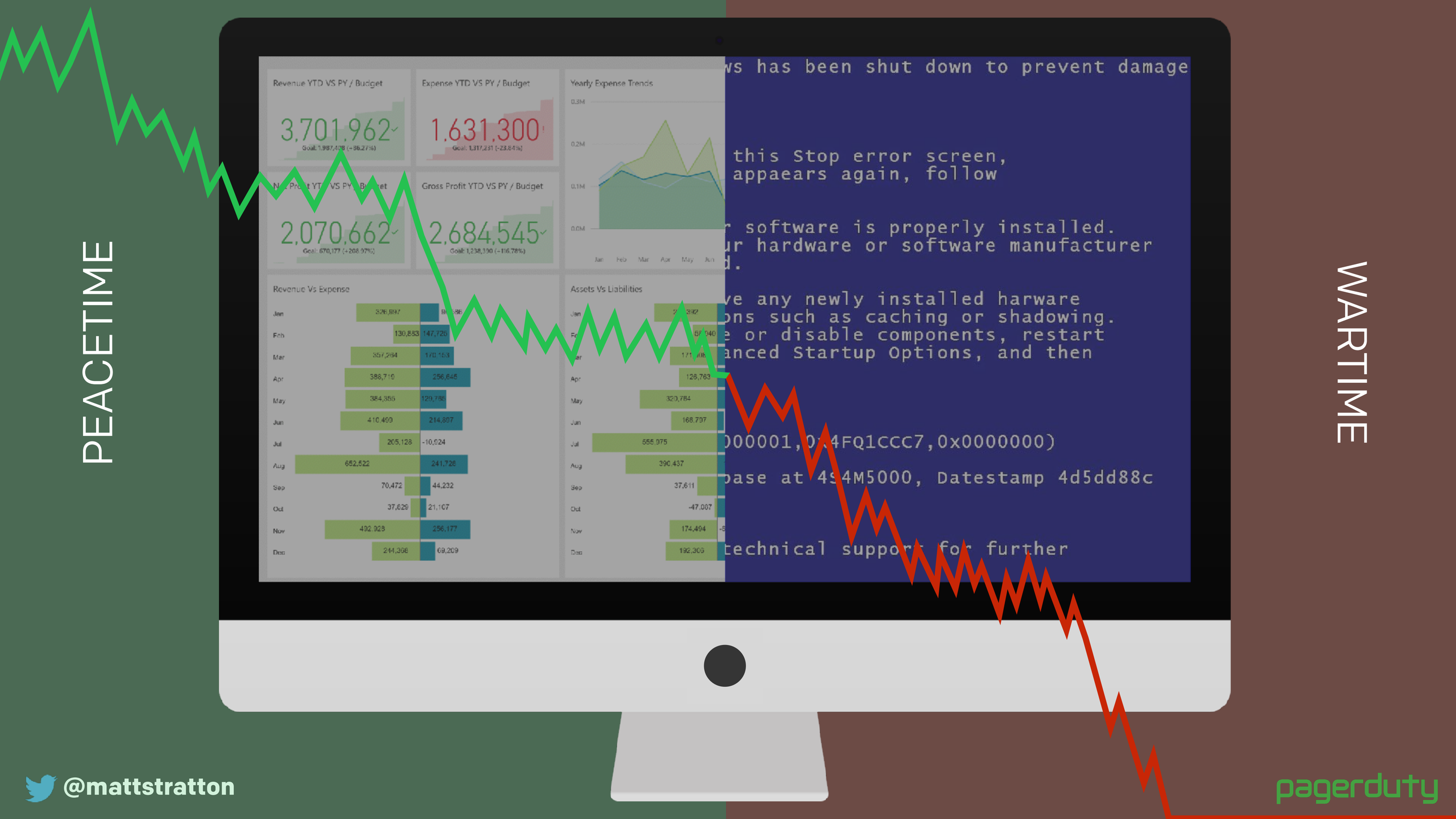
Gratuitous slide of kids to get you on my side

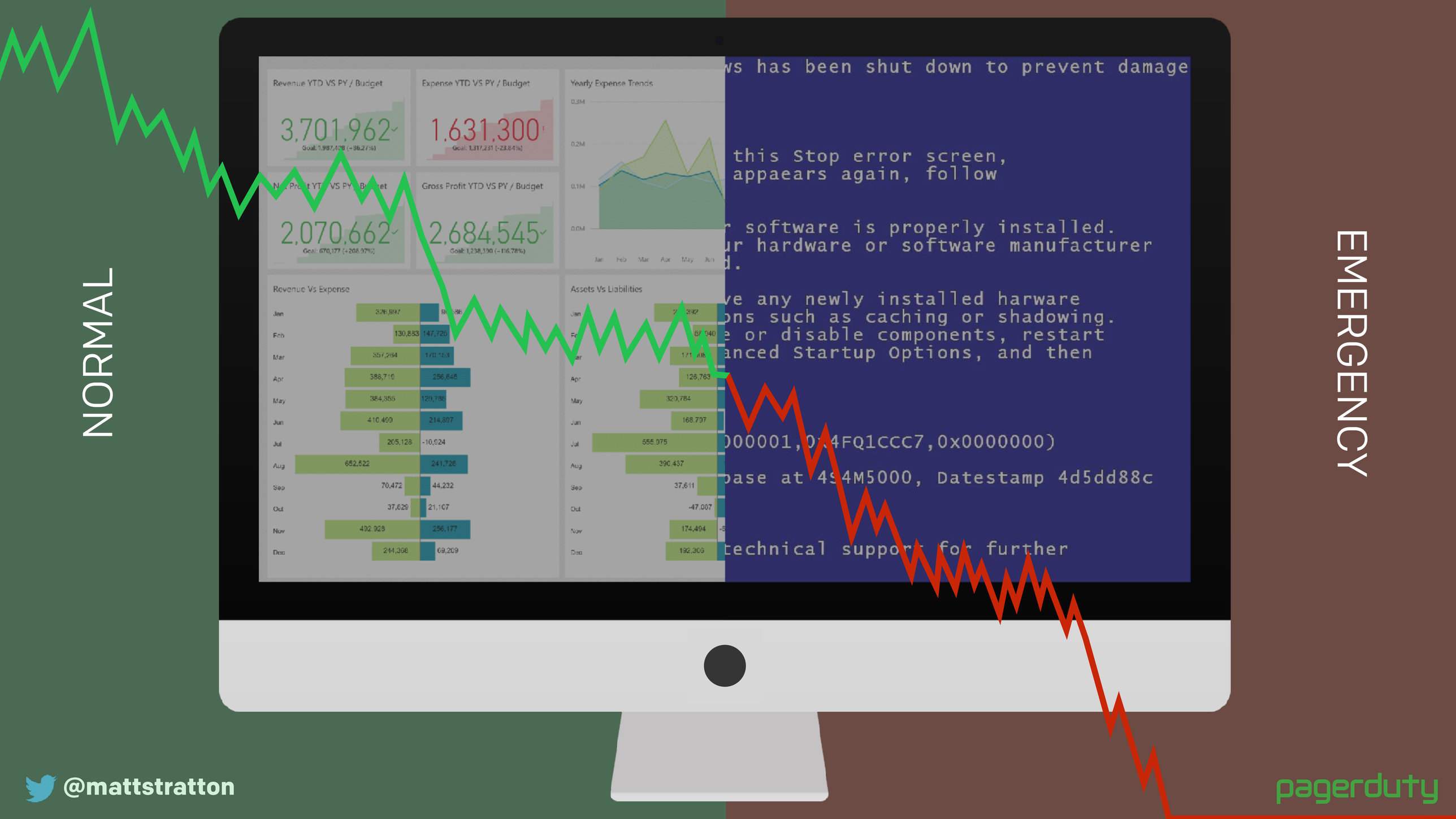




Disclaimer, part the first: Learn from other industries, do not take on their stresses.

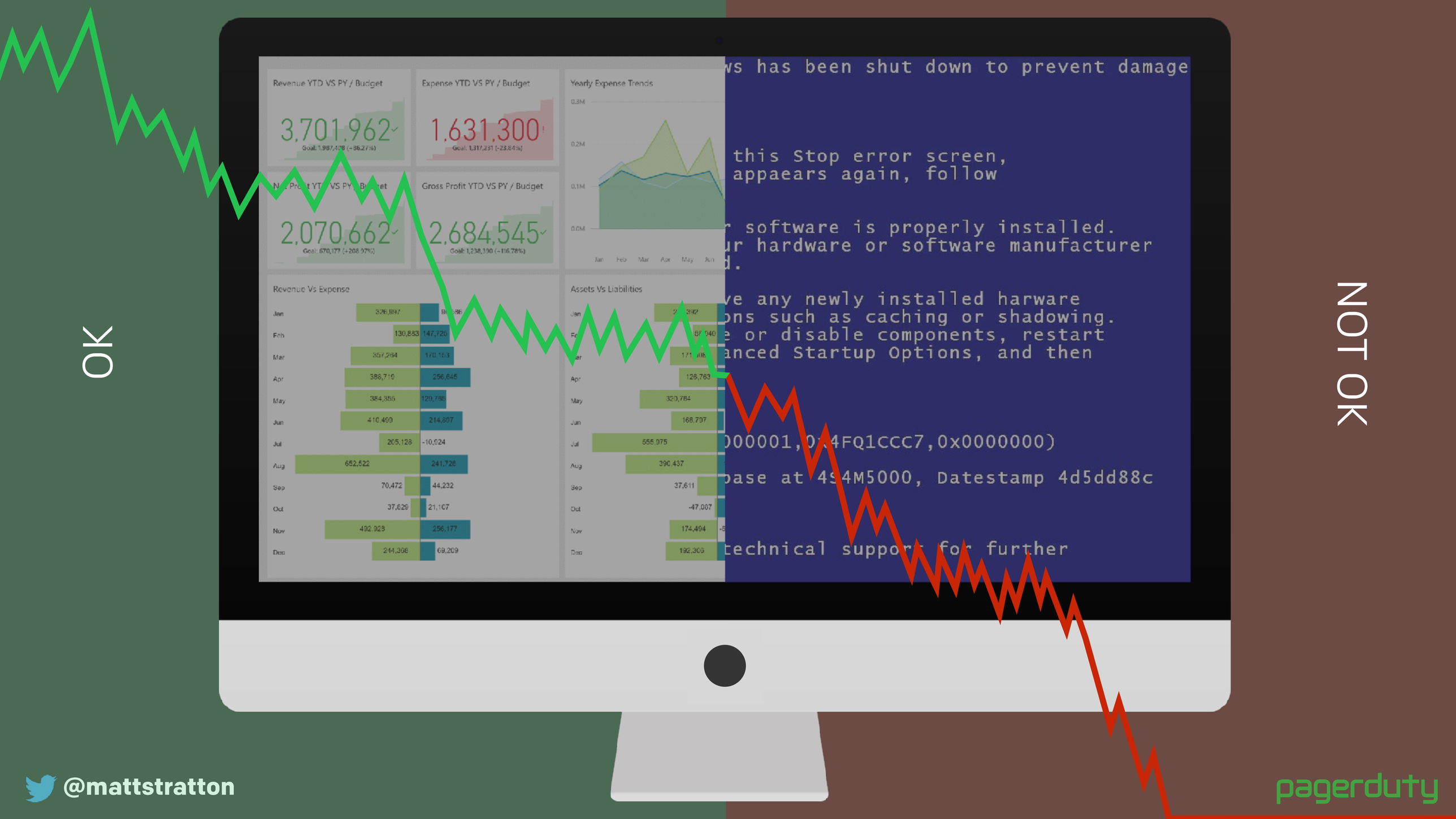
Disclaimer, part the second: This is a topic with a surprisingly large number of details.


PEACETIME
WARTIME
Revenue YTD VS PY / Budget
3,701,962
Expense YTD VS PY / Budget
1,631,300
Yearly Expense Trends
Gross Profit YTD VS PY / Budget
2,070,662
2,684,545
Revenue Vs Expense
Assets Vs Liabilities
ws has been shut down to prevent damage
this Stop error screen,
appaears again, follow
software is properly installed.
hardware or software manufacturer
ve any newly installed harware
ons such as caching or shadowing.
or disable components, restart
anced Startup Options, and then
000001,0x4FQ1CCC7,0x0000000)
pase at 4s4M5000, Datestamp 4d5dd88c
technical support for further
@mattstratton
pagerduty



@mattstratton

pagerduty



@mattstratton

pagerduty

Before, during, after

Before

Have criteria defined for when to have and not have a call.

Any unplanned disruption or degradation of service that is actively affecting customers' ability to use the product.

Post incident criteria widely. Don’t litigate during a call.

@mattstratton

Severities

Severity	Description
SEV-1	• SEV-2 co **minutes**
SEV-2	• Notificati • Notifi **accou** • Web know • An event • i.e. ar • i.e. th • Configura • Custome • Problems the **pdt-c**
	A
SEV-3	• Notificati • Email ev • Sales pip • Marke • Signu • Configura significan • Configura

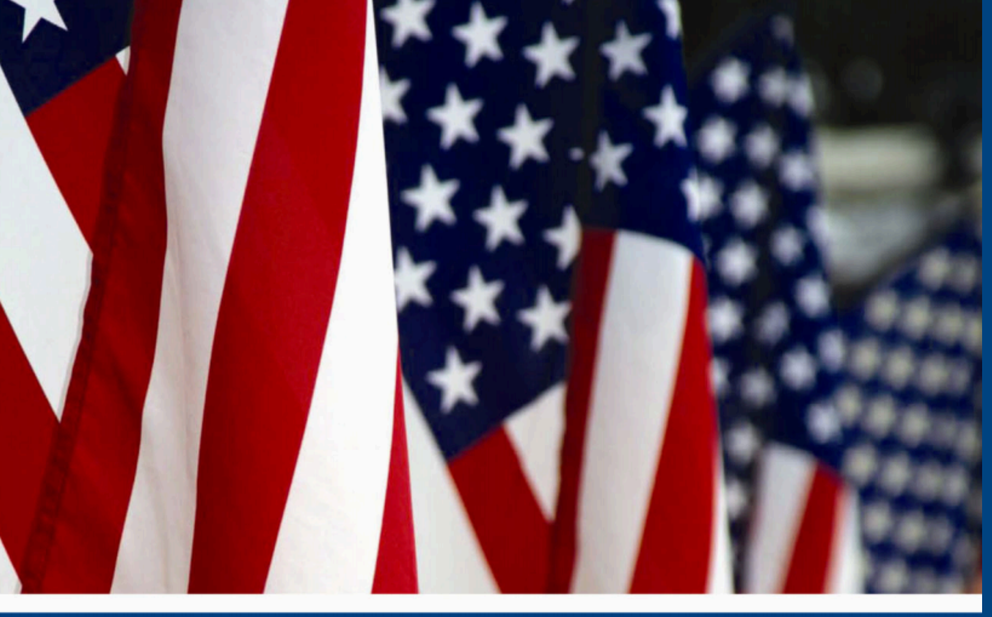
Monitor the business criteria, and act accordingly.

People are expensive.

Practice still makes perfect.

“Know your role”

Have a clear understanding of who is supposed to be involved in each role.

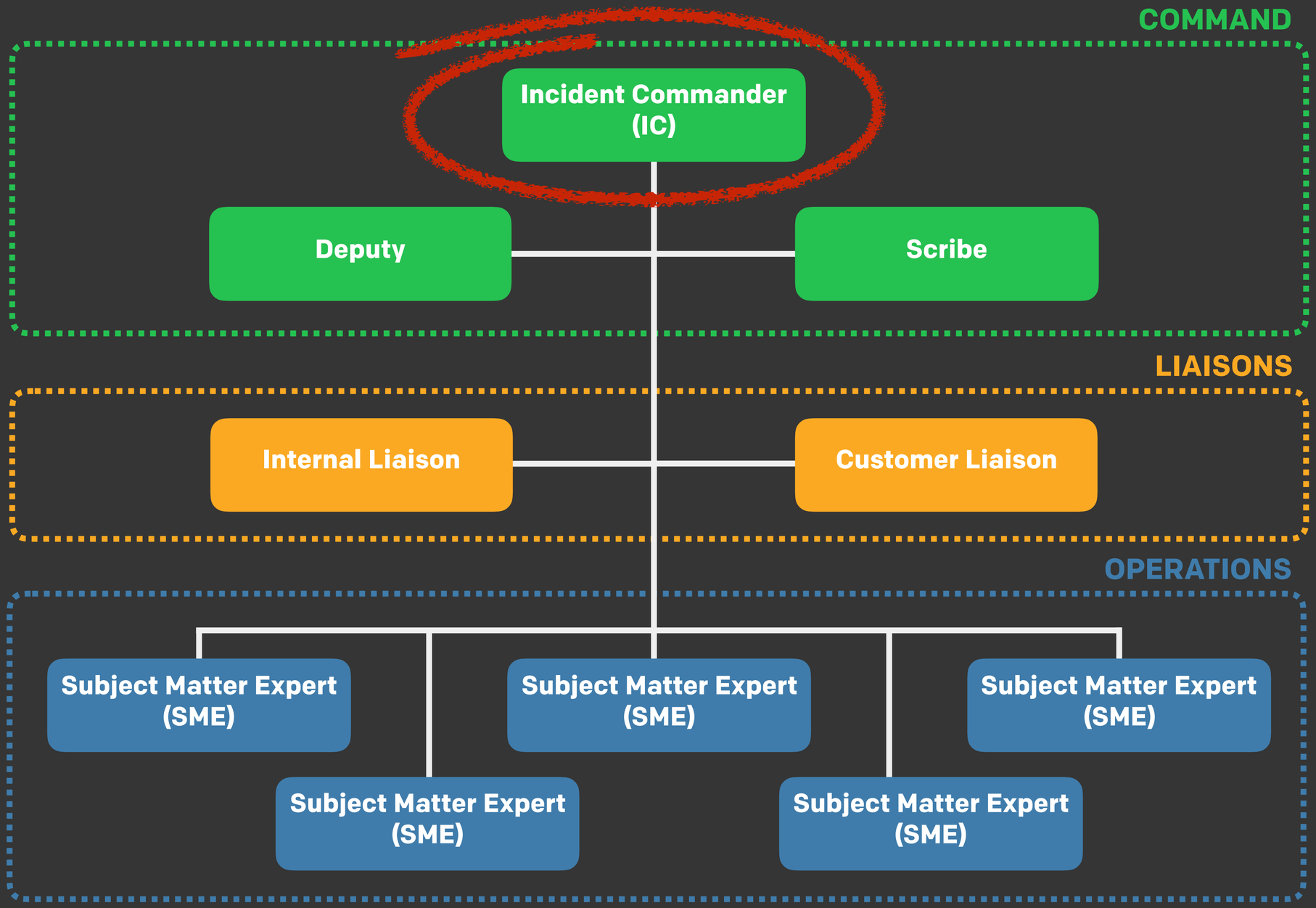


NATIONAL INCIDENT MANAGEMENT SYSTEM

December 2008
https://www.fema.gov/national-incident-management-system

Homeland Security

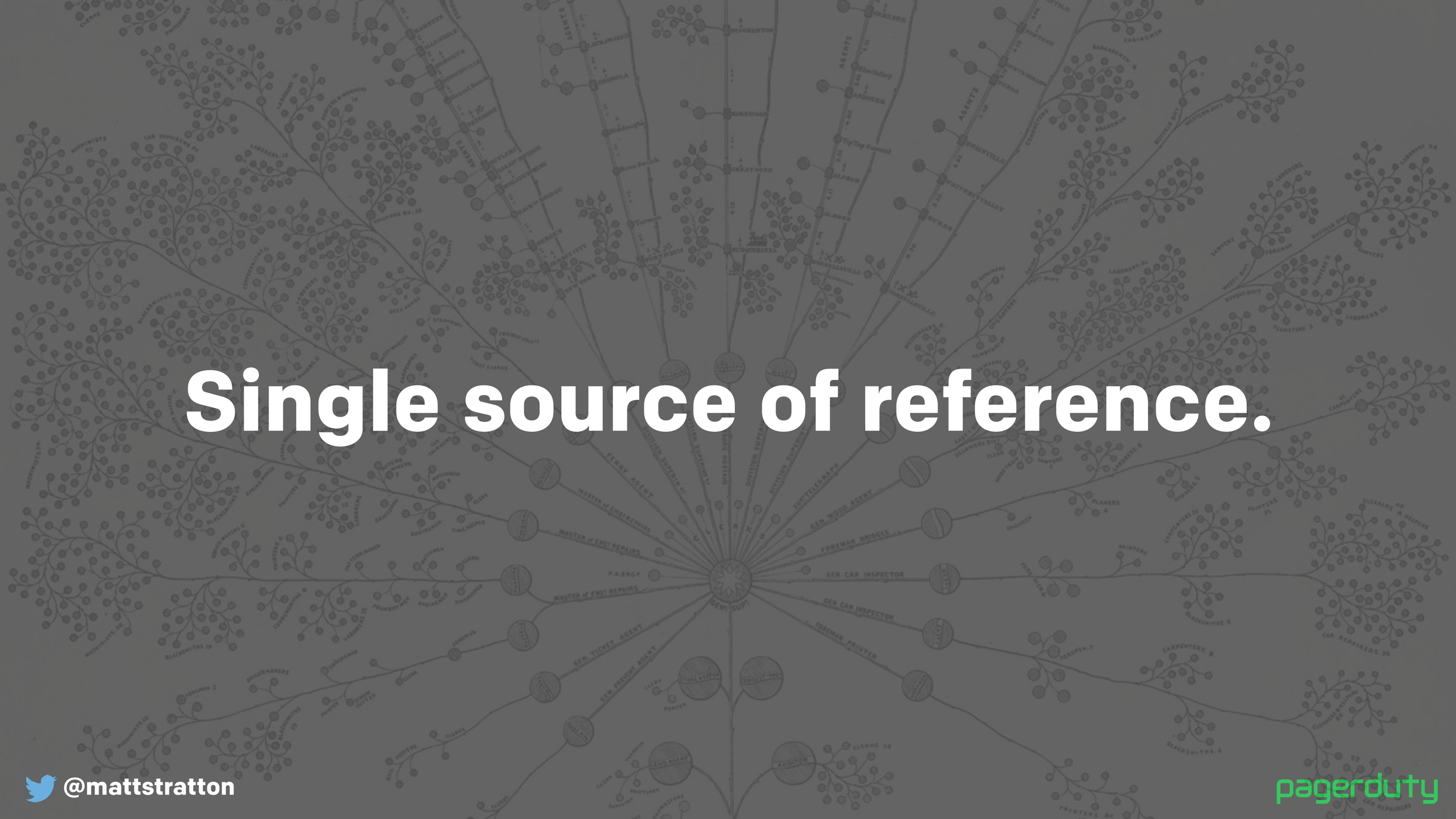
- "National Incident Management System" (NIMS)
- Incident Command System (ICS).
- Standardized system for emergency response.
- Hierarchical role structure.
- Provides a common management framework.
- Originally developed for CA wildfire response.


COMMAND
Incident Commander (IC)
Deputy
Scribe
LIAISONS
Internal Liaison
Customer Liaison
OPERATIONS
Subject Matter Expert (SME)
Subject Matter Expert (SME)
Subject Matter Expert (SME)
Subject Matter Expert (SME)
Subject Matter Expert (SME)

During

I'm Matty.

I'm the Incident Commander.


Single source of reference.

Becomes the highest authority.

(Yes, even higher than the CEO)

KEY TAKEAWAY

Not a resolver.
Coordinates and delegates.

DON’T DO THIS

Let’s get the IC on the RC, then get a BLT for all the SME’s.

KEY TAKEAWAY

Clear is better than concise.

The IC manages the flow of conversation.

What's wrong?

What actions can we take?

What are the risks involved?

“Can someone...”

Rich, I'd like you to investigate the increased latency, try to find the cause. I'll come back to you in 5 minutes. Understood?

Understood.

Humor is best in context.

DT5: Roger that

GND: Delta Tug 5, you can go right on bravo

DT5: Right on bravo, taxi.

(...): Testing, testing. 1-2-3-4.

GND: Well, you can count to 4. It's a step in the right direction. Find another frequency to test on now.

(...): Sorry

Have a clear roster of who's been engaged.

Rally fast, disband faster.

Have a way to contribute information to the call.

Have a clear mechanism for making decisions.

“IC, I think we should do X”
“The proposed action is X,
is there any strong objection?”

Capture everything, and call out what's important now vs. later.

“One last thing...”
(Assign an owner at the end of an incident)

After

“After action reports”, “Postmortems”, “Learning Reviews”

The impact to people is a part of your incident review as well.

Record incident calls, review them afterwards.

Regularly review the incident process itself.

Have structure in place beforehand

Practice, practice, practice

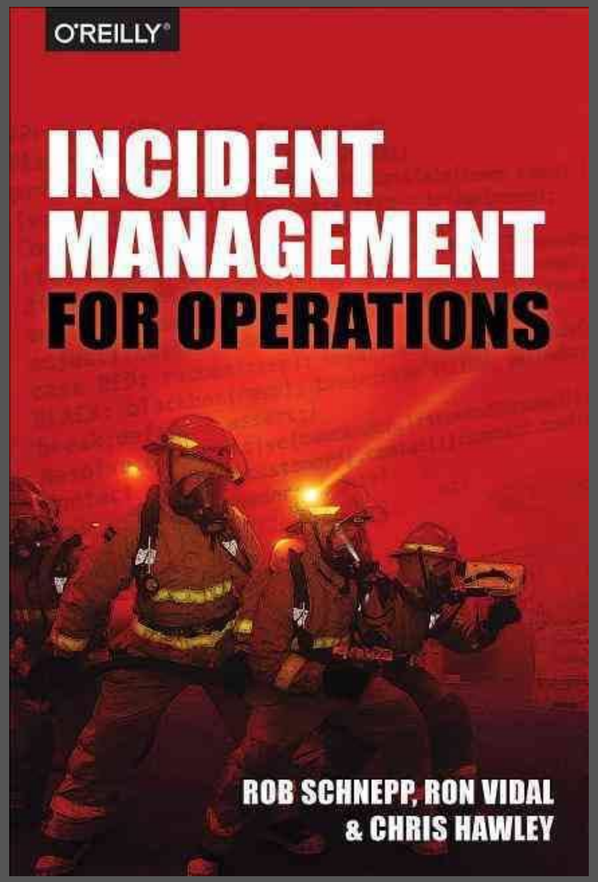
Have clearly delineated roles

Manage the conversation flow

Make clear decisions

Rally fast, disband faster

Review regularly


O'REILLY
INCIDENT MANAGEMENT FOR OPERATIONS
ROB SCHNEPP, RON VIDAL & CHRIS HAWLEY

Don’t panic.
Stay calm.
Calm people stay alive.

https://response.pagerduty.com

Credit: NASA

So you want to be an incident commander? You've come to the right place! You don't need to be a senior team member to become an IC, anyone can do it providing you have the requisite knowledge (yes, even an intern)!

Purpose

If you could boil down the definition of an Incident Commander to one sentence, it would be,

> *Take whatever actions are necessary to protect PagerDuty systems and customers.*

The purpose of the Incident Commander is to be the decision maker during an major incident; Delegating tasks and listening to input from subject matter experts in order to bring the incident to resolution.

The Incident Commander becomes the highest ranking individual on any major incident call, regardless of their day-to-day rank. Their decisions made as commander are final.

Your job as an IC is to listen to the call and to watch the incident Slack room in order to provide clear coordination, recruiting others to gather context/details. **You should not be performing any actions or remediations, checking graphs, or investigating logs.** Those tasks

Resources:

- Angry Air Traffic Controllers and Pilots - https://youtu.be/Zb5e4SzAkkI
- Blameless Post-Mortems (Etsy Code as Craft) - https://codeascraft.com/2012/05/22/blameless-postmortems/
- Incidents And Accidents: Examining Failure Without Blame (Arrested DevOps) - https://www.arresteddevops.com/blameless/
- PagerDuty Incident Response Process - https://response.pagerduty.com/

Thank you!

Questions?