Findings From The Field

Two Years of Studying Incidents Closely

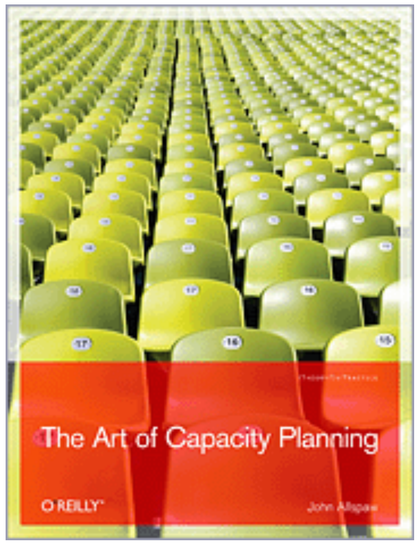
John Allspaw

Adaptive Capacity Labs

about me

flickr

Etsy



LUND UNIVERSITY

SNAFU CATCHERS

Consortium for Resilient
Internet-Facing Business IT

Adaptive
Capacity
Labs

disclosure

1. these are only a ***few*** of the most common patterns

2. these are not judgements/comments on ***any single organization***

Bottom Line, Up Front:
what we've observed across the industry

1. The state of maturity in the industry on *learning from incidents* is **low**.

2. Significant gaps exist between ***technology leaders*** ↔ ***hands-on practitioners*** on what it means to *learn from incidents*.

3. Learning from incidents is given **low** priority, resulting in a narrow focus on *fixing.*

4. Overconfidence in what *shallow* incident metrics mean and significant energy wasted on tabulating them.

Technology Leaders ↔ Hands-on Practitioners

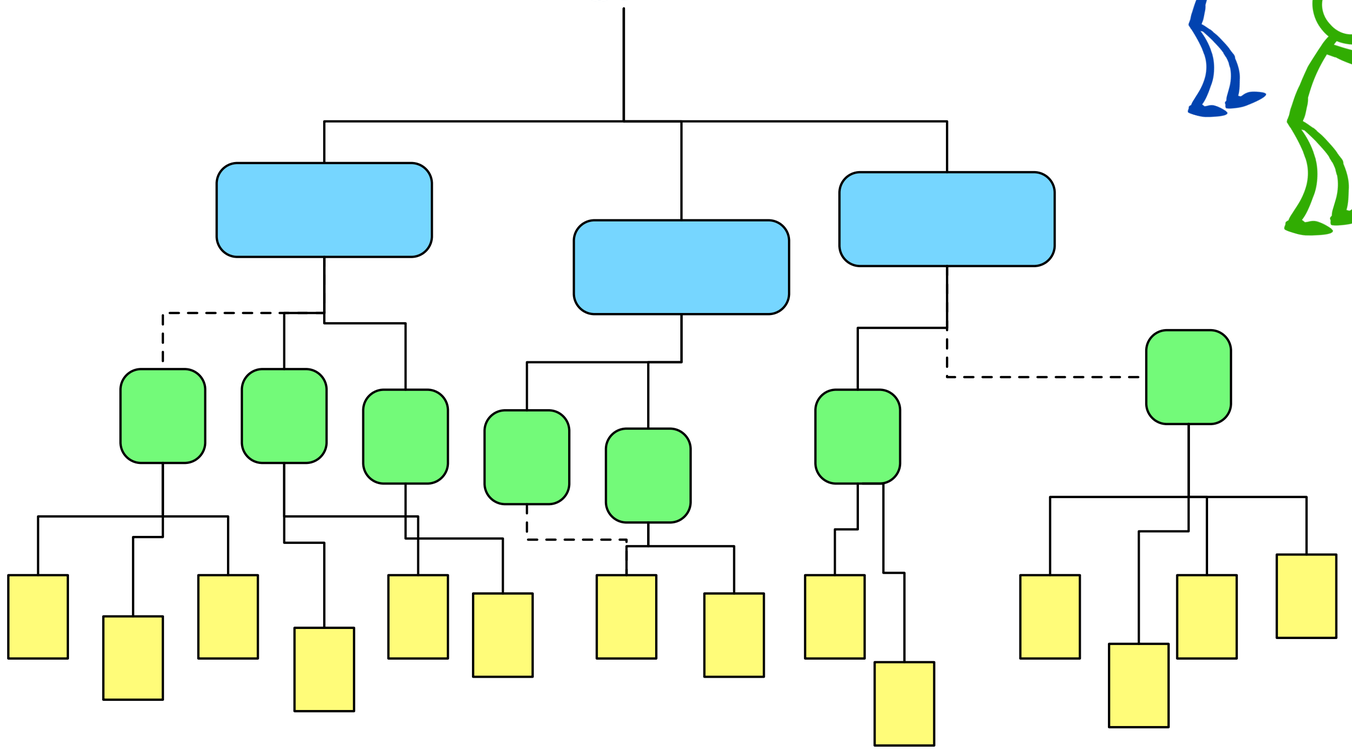
a gap exists here

- **what** is actually learned
- **how** learning actually takes place
- **what** the incident actually *means* *(for the past, for now, and for the future)*

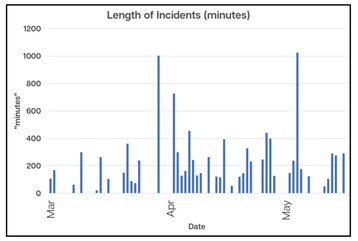
“Blunt” End

“Sharp” End

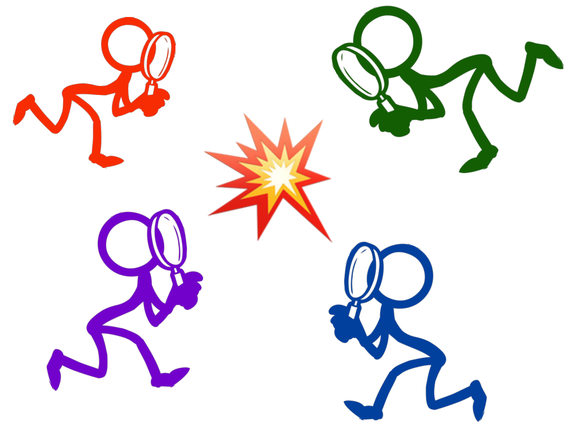
Technology Leaders



Hands-on Practitioners



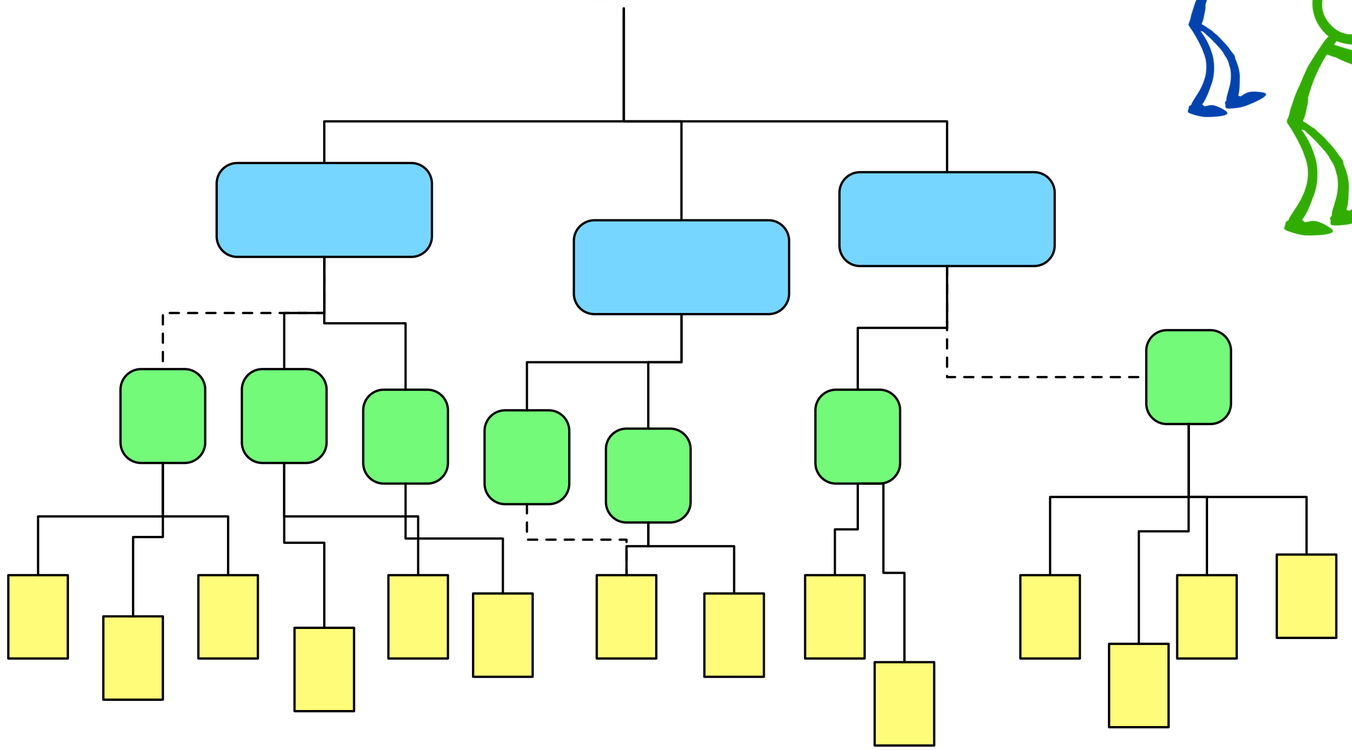
- summaries
- simplifications
- abstractions
- statistics



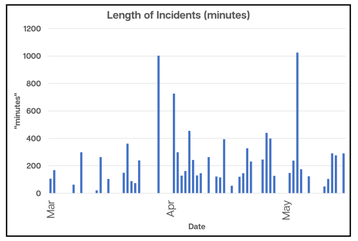
“Blunt” End

“Sharp” End

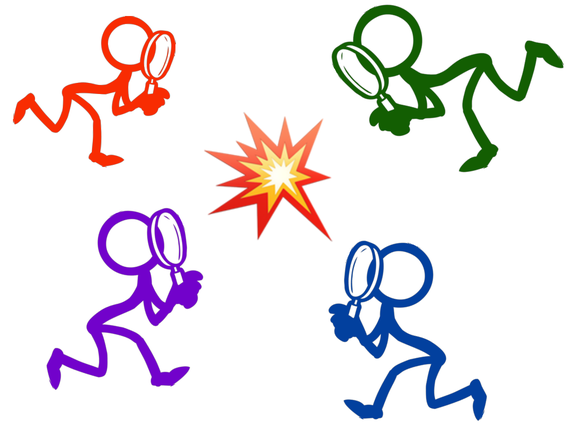
Technology Leaders



Hands-on Practitioners



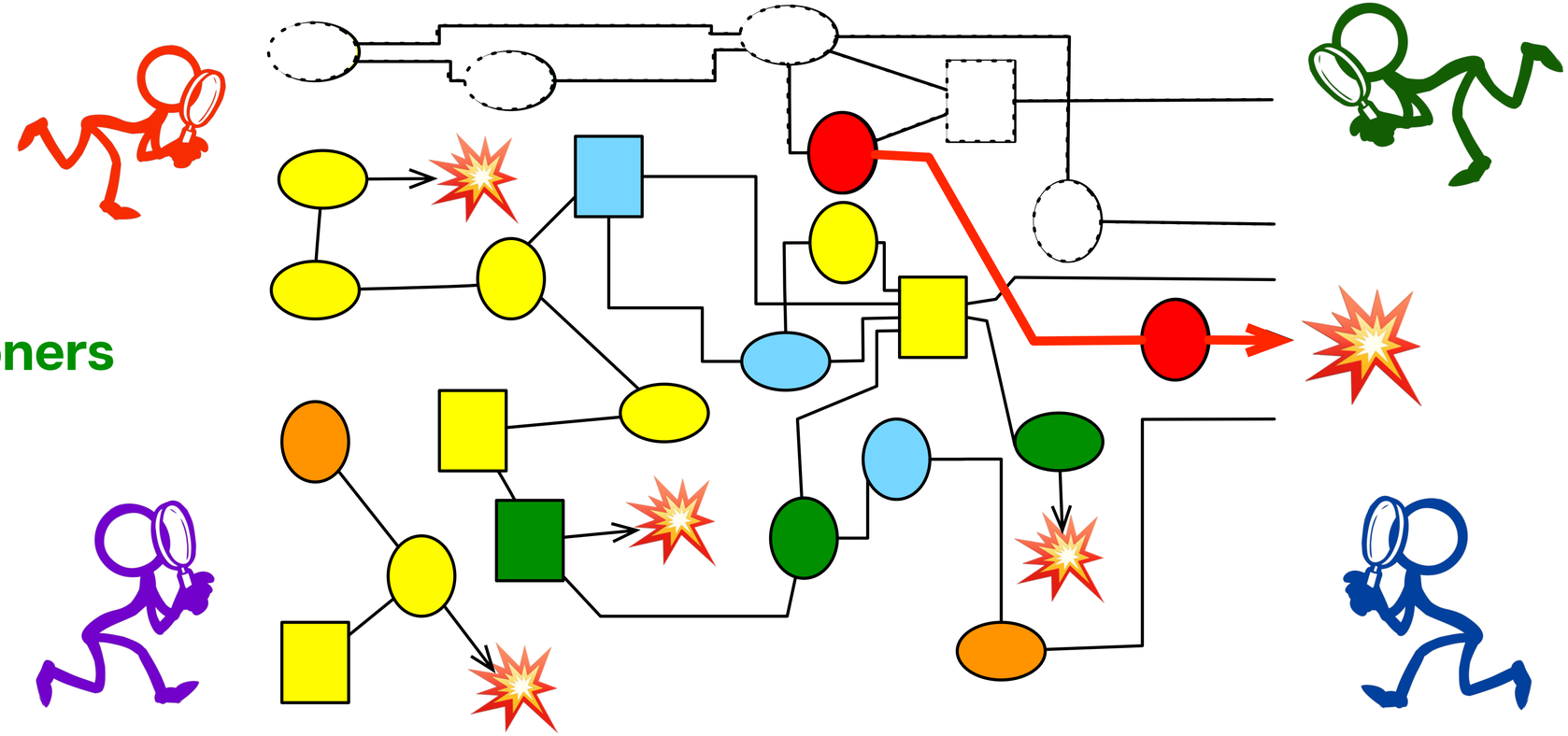
- summaries
- simplifications
- abstractions
- statistics



Technology Leaders

24.53 *Mean Time To Resolve*
32.13 *Mean Time To Oversimplify*
14.45 *Mean Time To Something*
22 *incidents in Q3*
12 *SEVERITY DEFCON events*

Hands-on Practitioners



Technology Leaders

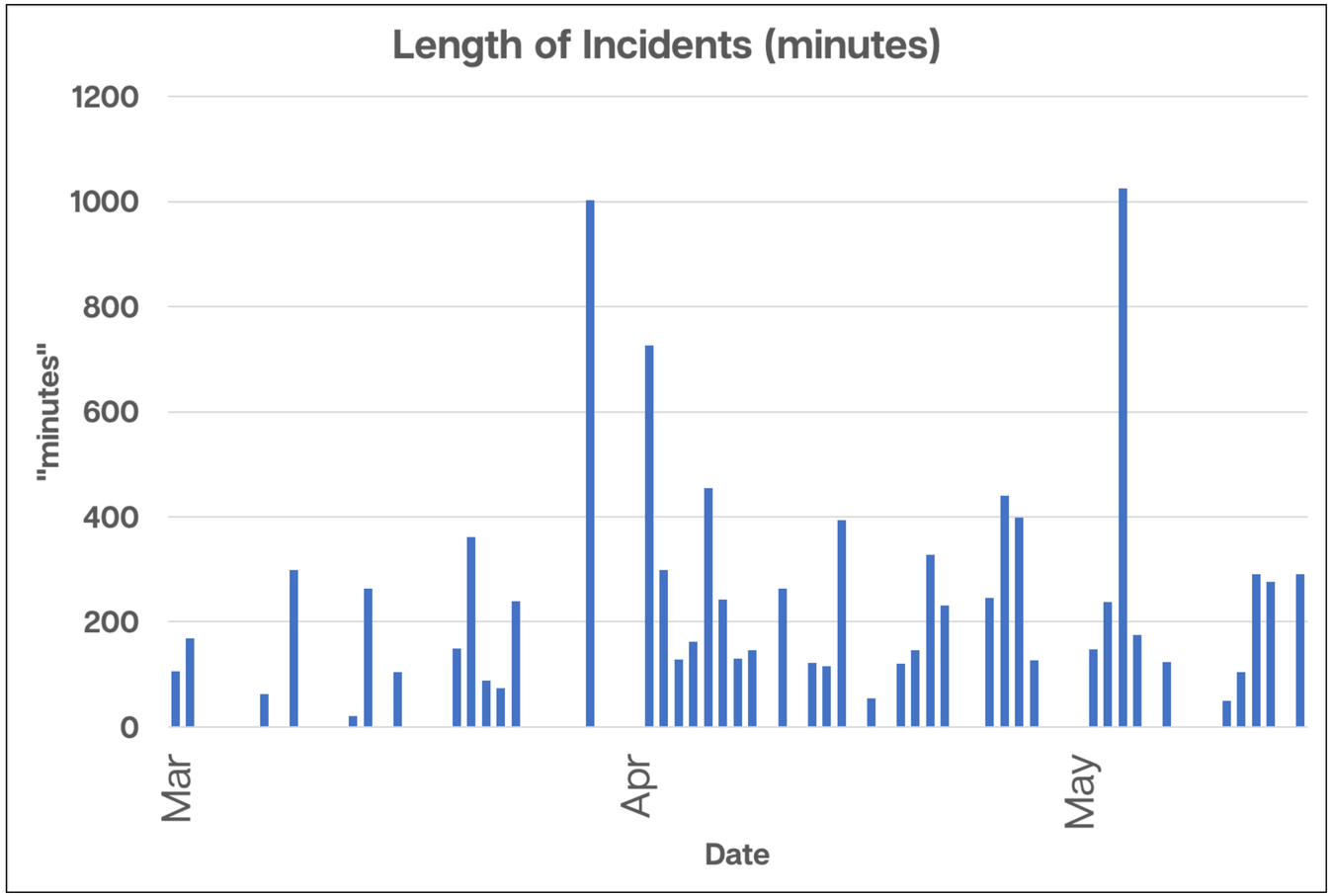
- typically are far away from the “messy details” of incidents
- frequently believe their presence and participation in incident response channels (chat, bridges, etc.) has a positive influence (it doesn’t)
- typically believes incidents are adverse events in an otherwise “quiet” and healthy reality (they’re not)
- typically fear how incidents reflect poorly on *their performance* more than they fear practitioners not learning effectively from them

Technology Leaders

- typically believe abstract incident metrics tell enough of a story for them to understand the state of the “system” (they don’t)
- typically believe abstract incident metrics reflect more about their teams’ performance than it reflects the complexity those teams have to cope with
- typically **believe the above observations don’t apply to them** 😀

shallow metrics

(M)TTR/(M)TTD
Frequency
Severity
Customer impact
...



no ***predictive*** value forward
no ***explanatory*** value backward

“but they help us ask deeper questions”

You don’t need this chart to ask deeper questions about incidents.

Just ask the questions.

and record both the questions and answers so others can find them in the future

Technology Leaders

How can you tell the difference between...

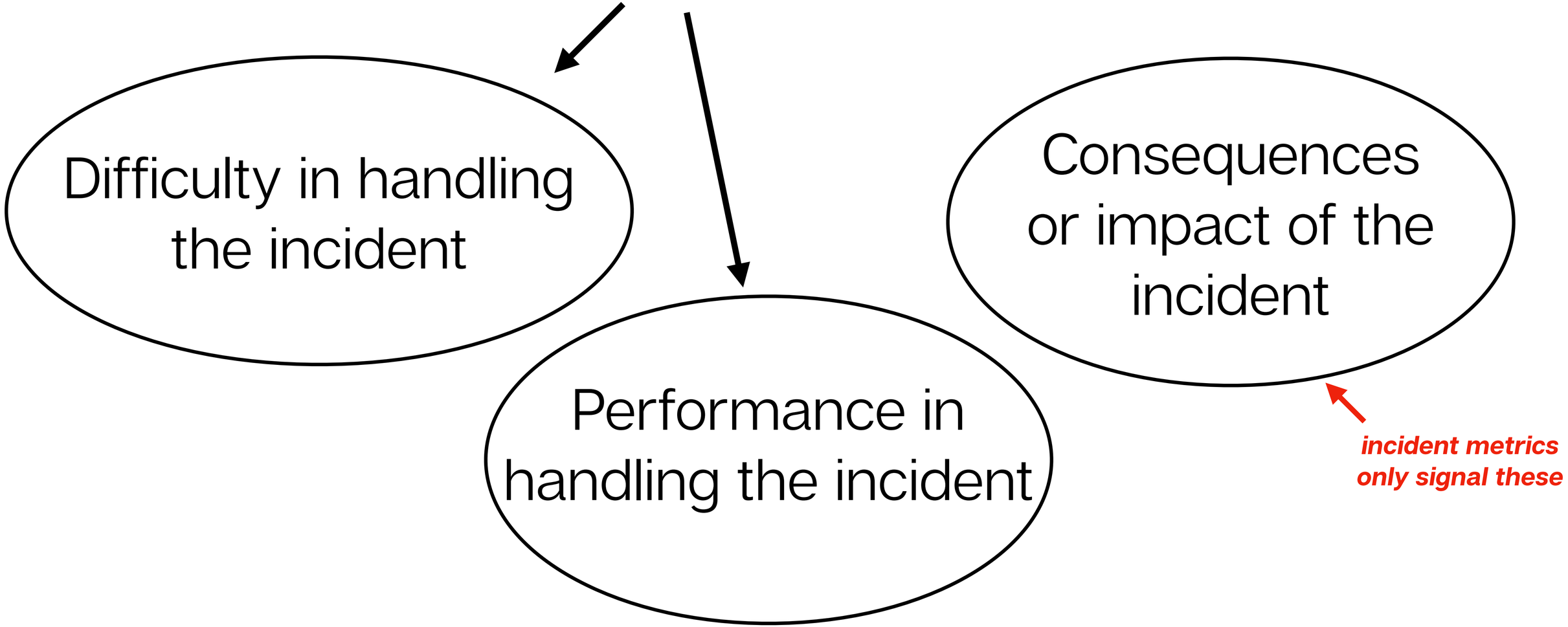
A difficult case handled *well*.

A straightforward case handled *poorly*.

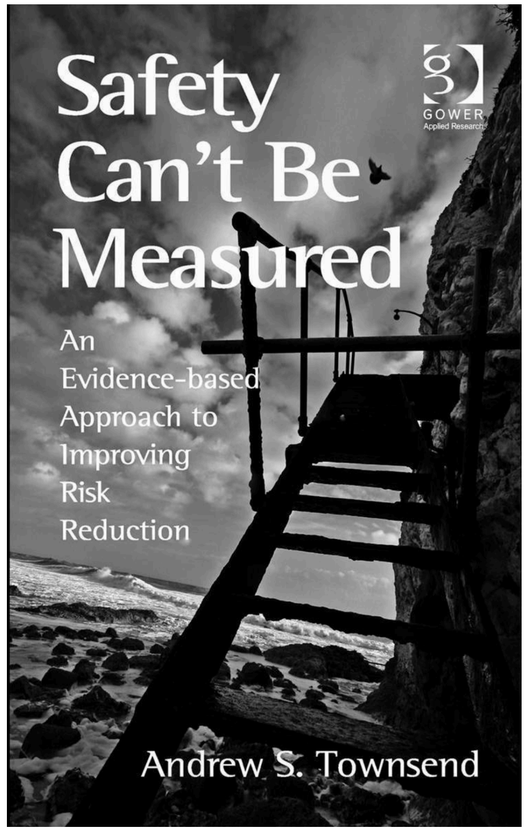
?

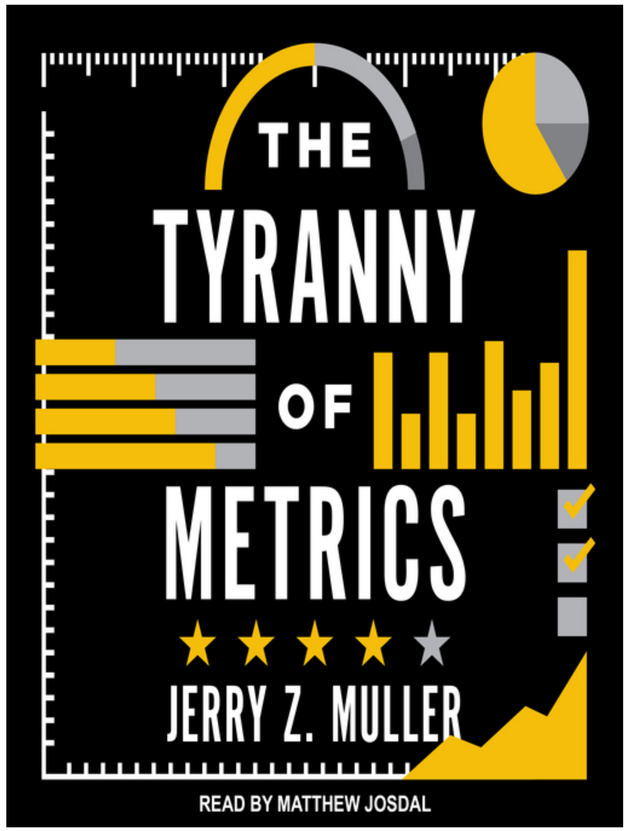
Technology Leaders

without these, you cannot understand
what incidents mean in context



incident metrics do not do what you think they do





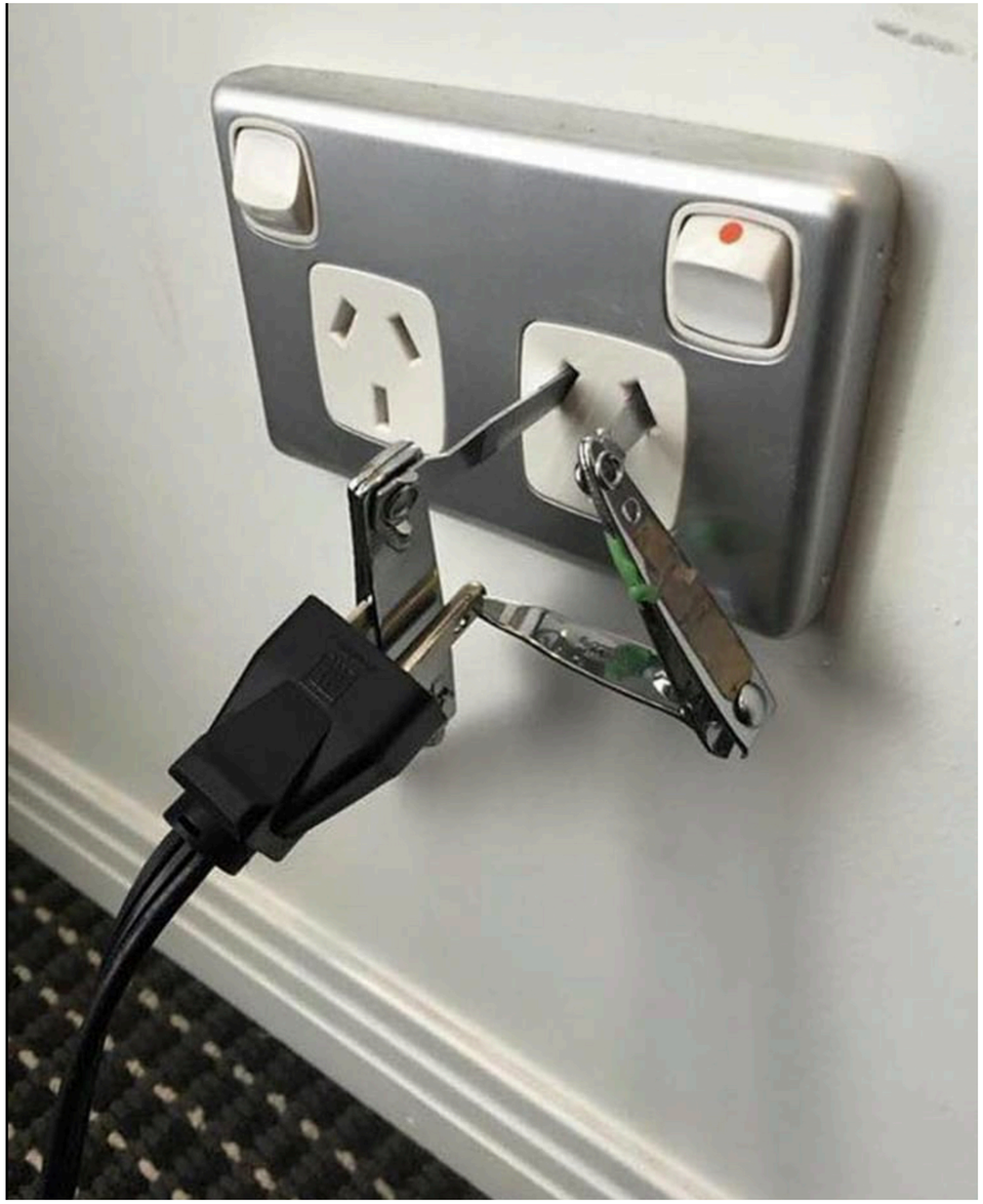
More on this topic:
https://bit.ly/beyond-shallow-data

Hands-on Practitioners

- typically view post-incident activities to be a “check-the-box” chore
- typically believe in a future world where automation will make incidents disappear
- typically do not capture what makes an incident *difficult*, only what technical solution there was for it.
- typically do not capture the post-incident writeup for readers beyond their local team

Hands-on Practitioners

- typically do not read post-incident review write-ups from other teams
- typically fear what leadership thinks of incident metrics **more** than they fear misunderstanding the origins and sources of the incident
- typically has to exercise significant restraint from immediately jumping to “fixes” before understanding an incident beyond a surface level
- typically **believe the above observations don’t apply to them** 😀



Learning **is not the same as** ***fixing*****.**

More about this here:
https://bit.ly/learning-not-fixing

Ok! We get it!
What are *solutions*, wiseguy?

Technology Leaders

Learning from incidents effectively requires skill and expertise that most do not have

These are skills that can be learned and improved.
Prioritize it when things are going *well*.
It will accelerate the expertise in your org.

More on this:
https://www.learningfromincidents.io/

Technology Leaders

Focus less on incident metrics and more on signals that people are *learning*

- analytics on ***how often*** incident write-up are being *read*
- analytics on ***who*** is reading the write-ups
- analytics on where incident write-ups are being ***linked from***
- support group incident review meetings being *optional*, and ***track attendance***
- track which write-ups that link to prior relevant incident write-ups

More about this here:
https://bit.ly/learning-markers

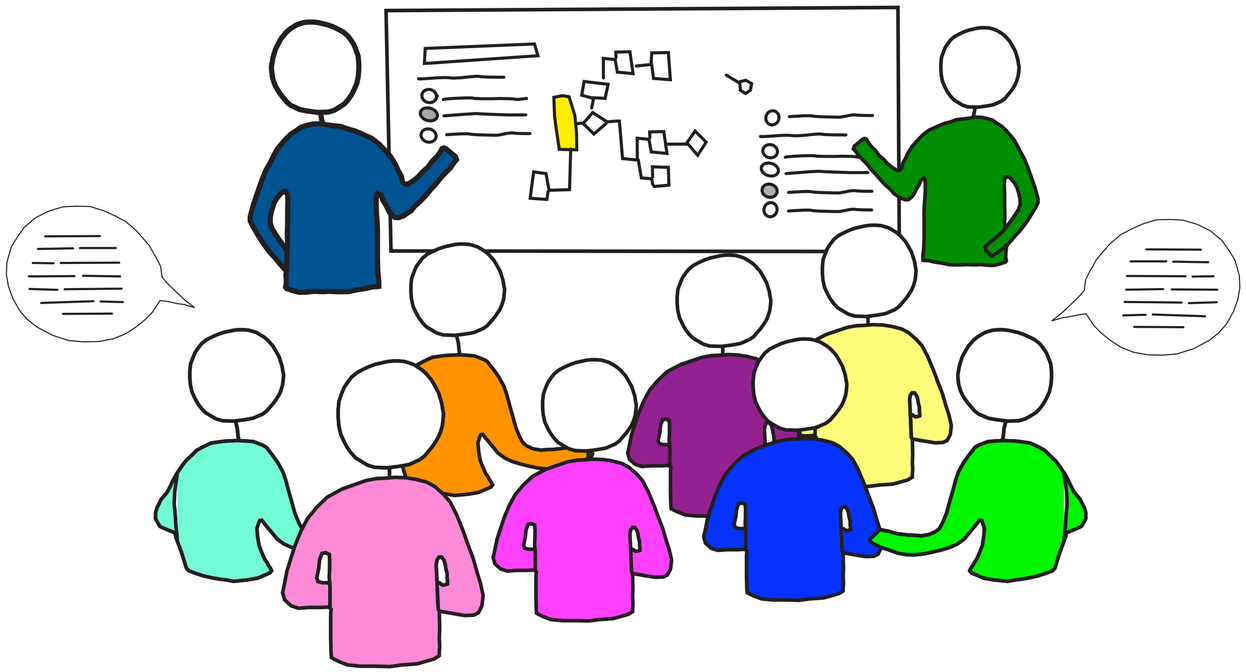
Practitioners

Don’t place *all* the burden on a group review meeting!

Use this meeting to present and discuss analysis ***that has already been done.***

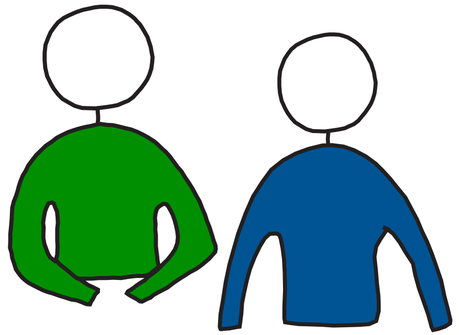
Too many potential pitfalls to bet everything on a single meeting…

- HiPPO (“highest paid person's opinion”)
- Groupthink
- Tangents
- Redirections
- Elephants in the room
- “Down in the weeds”



this is an important meeting — prepare for it like it’s expensive — because it is!

Practitioners

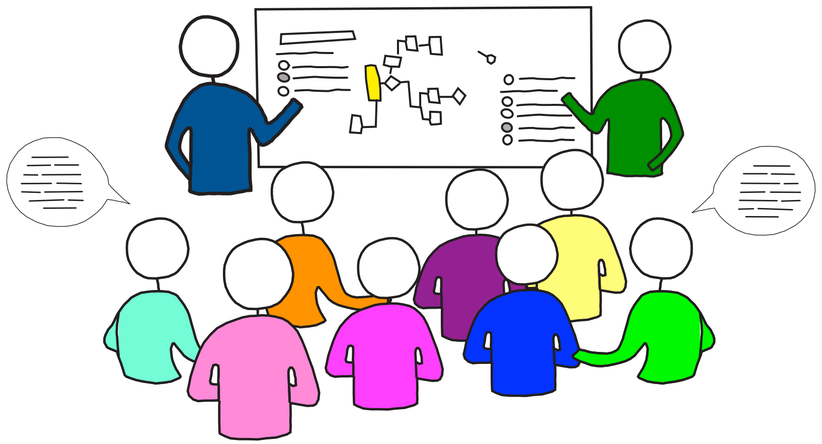


Incident analysts should *NOT* be stakeholders

- Your role is **not** to tell the One True Story™ of what happened.
- Your role is **not** to dictate or suggest what to do.
- Maintaining a ***non-stakeholder stance*** signals to others that you are willing too hear a minority viewpoint
- *Half of your job* is to get people to genuinely look forward to and participate in the next incident analysis.

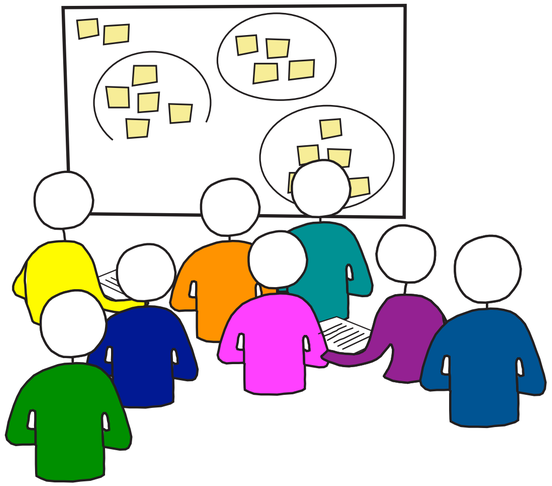
Practitioners

Separate generating action items from the group review meeting



Group Review Meeting

“soak time”



Action Items Generation

ACL Challenge

Technology Leaders

Start tracking how often post-incident write-ups are ***voluntarily read*** by people *outside of the team(s) closest to the incident.*

Start tracking how often incident review meetings are ***voluntarily attended*** *by people outside of the team(s) closest to the incident.*

Practitioners

For every incident that has a “red herring” episode...capture the red herring part of the story ***in detail*** in the write-up, especially on what made following the “rabbit hole” seem reasonable at the time.

Help I’m Looking For

Thank You!

Help I’m Looking For