3 Lies We Tell Ourselves About Disaster Recovery

… and what to do about them





IBM





Uptime Labs





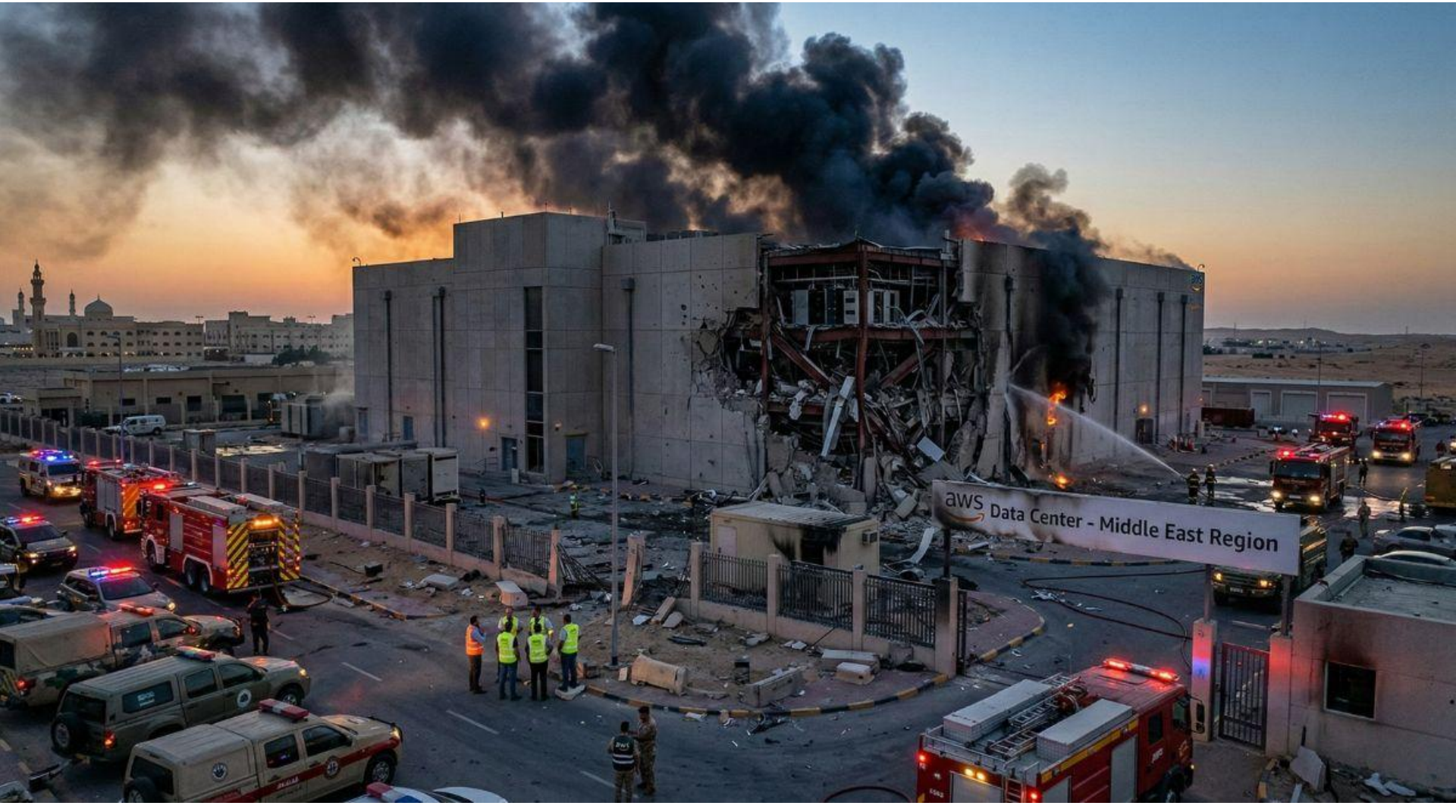


RESILIENCE IN SOFTWARE FOUNDATION

THIS IS FINE!



COGNITE


aws Data Center - Middle East Region

What we’ll talk about today…

- All DR plans that exist in the world are bullshit

What we'll talk about today…

- All DR plans that exist in the world are bullshit
  - (Yes, your DR plans, specifically, are bullshit)

What we'll talk about today…

- All DR plans that exist in the world are bullshit
  - (Yes, your DR plans, specifically, are bullshit)
  - *** That doesn't mean that they're worthless!

What we'll talk about today…

- All DR plans that exist in the world are bullshit
  - (Yes, your DR plans, specifically, are bullshit)
  - *** That doesn't mean that they're worthless!
- There are three important lies we tell ourselves about DR that are worth examining

What we'll talk about today…

- All DR plans that exist in the world are bullshit
  - (Yes, your DR plans, specifically, are bullshit)
  - *** That doesn't mean that they're worthless!
- There are three important lies we tell ourselves about DR that are worth examining
- There are practical things we can do in response to these lies, to mitigate their harm and do better by the people we work with



Prosaic Organizational Failure

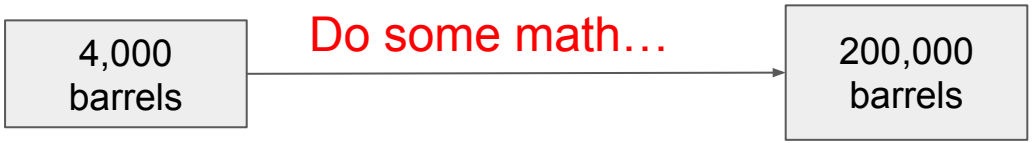
LEE CLARKE
Rutgers University
CHARLES PERROW
Yale University

We use the case of the now-dead Shoreham Nuclear Power Station to pose some questions, and a few answers, about organizational failure. The analysis centers on the symbolism of organizational plans, specifically how organizations use plans to justify increasingly complex systems to themselves and to others. That such plans are based on sparse or nonexistent experience, and that they are often wildly unrealistic, suggests some reasons why high-technology, high-risk systems do not foster organizational learning.

Organizations fail often and they fail in important ways. Police departments become corrupt. Banks invest unwisely. Schools do not educate. Investment houses make bad bets. But large or powerful organizations rarely disappear, though one would think that failure would mean extinction. Only one work deals


EXXON VALDEZ

How you get from 4k -> 200k barrel spill plan



Two Oil Spill Scenarios for Prince William Sound, Alaska

4,000-Barrel Spill	200,000-Barrel Spill
• seas less than 5 feet	• seas less than 5 feet
• currents less than 1.6 knots	• currents less than 1.6 knots
• waves less than 2 feet	• waves less than 2 feet
• at least 2 miles visibility	• at least 2 miles visibility
• weather conducive to cleanup	• weather conducive to cleanup
• winds at 8 knots	• winds at 5 knots
• ship, shore boomed within 3 hours	• ship boomed within 5 hours, shore "immediately"
• dispersants on site in 9 to 17 hours	• dispersant arrival not estimated, presumably 9 to 17 hours
• communications flawless	• communications flawless
• all agencies coordinated	• all agencies coordinated
• 100 barrels unrecoverable	• 10,000 barrels unrecoverable

Sources: Alyeska Pipeline Service Company, Oil Spill Contingency Plan; Clarke, "The disqualification heuristic."

How you get from 4k -> 200k barrel spill plan

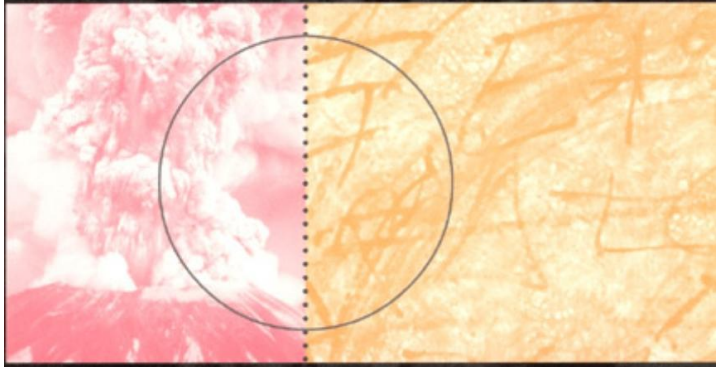
The earlier plan . . . I think it was just a continuation of what was done before. I don't think anyone made the decision that "no, we don't need the maps," so eliminate these. I think Alyeska just did somewhat of a repeat of the old plan and we commented on where we thought it needed to be updated and made current, and perhaps in a few places in the earlier plan where it was not complete enough or where there were mistakes to correct those. So I don't think there was a great deal of revision from the earlier plan on the new plan. If mistakes were made, I think it was unfortunately a continuation of the earlier plan that nobody felt had the power by himself to say "no, we don't need this, let's delete this."

Exxon Valdez spill - Alyeska's plan vs. reality

	200,000 barrels **plan**	240,000 barrels **reality**
Initial response with minimal gear via barge	Under 5 hours	12 hours
Major recovery gear arrives for containment	9-17 hours	1-2 weeks
Clean up time	2 months	3 years
Unrecovered barrels	10,000	~38,400
Directly recovered	100,000	16,800-34,000
"Naturally dispersed"	90,000	168,000

A critical look at how governments and corporations plan for accidents and disasters

MISSION IMPROBABLE



LEE CLARKE

Using Fantasy Documents to Tame Disaster

Now a question

- Do you have disaster recovery plans where you work?

Now ~~a~~ some question*s*

- Do you have disaster recovery plans where you work?
- How many of you would bet $40 that they would work as planned if they needed to facilitate a recovery in real life?

Now ~~a~~ some question*s*

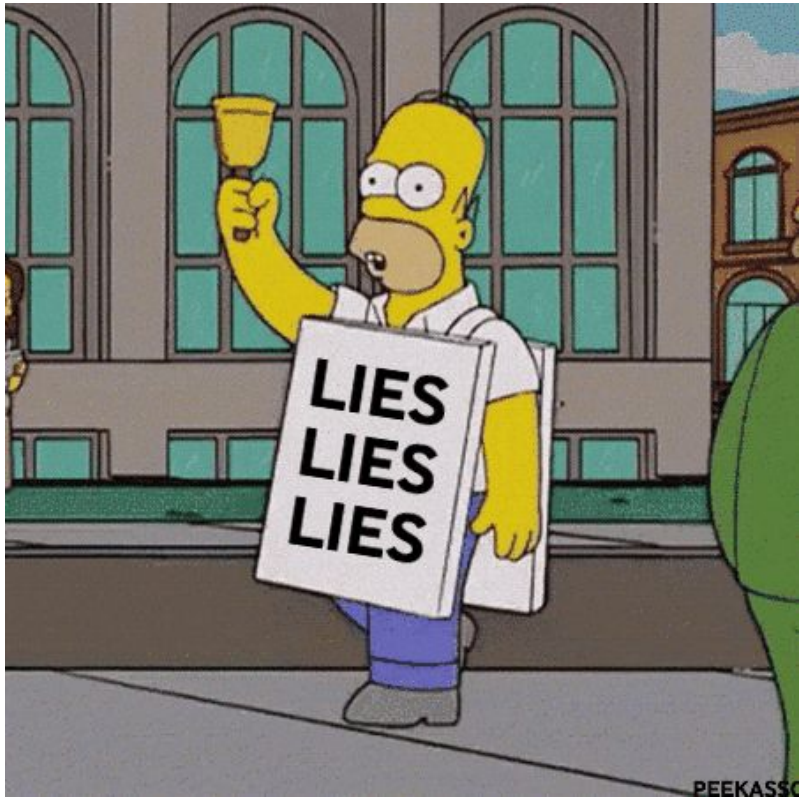
- Do you have disaster recovery plans where you work?
- How many of you would bet $40 that they would work as planned if they needed to facilitate a recovery in real life?
- What about $400?

Now ~~a~~ some question*s*

- Do you have disaster recovery plans where you work?
- How many of you would bet $40 that they would work as planned if they needed to facilitate a recovery in real life?
- What about $400?
- What about $4000?

One last question

- Are you certain about the cost of your DR plans being lies?
  - In other words, do you understand the the full impact that your plans have on the world around you?



…and why we tell them to ourselves

Lie 1: If you test it, it will work when it counts

The reality is that while some parts of your plan might work, it’s more likely than not that important parts of it will not when it counts.

Lie 2: A real-life disaster scenario will be unambiguous

In reality, operators more frequently face ambiguity when confronted with incidents, and small events can cascade into catastrophe over long or short periods of time.

Lie 3: The value in our DR plan is that it works perfectly when we need it

This is where we uncover the real value of your DR plan!

A DR test is more like incident practice. We can ***get more value*** when we *accept* that it can contribute to organizational learning rather than actually work as planned when needed.

Okay, wtf do I do now?



Lie 1: If you test it, it will work when it counts

Lie 1: If you test it, it will work when it counts

- The value of your DR plan is not that it works
  - You need to pass audits
  - Q: Do you need to also keep internal stakeholders ***too*** comfortable?
- You should still manage the plan across the organization
  - Talk to people who manage incidents on the ground - customer support and engineers, to write the plan with the most leeway for responders that you can.
  - Make sure executives understand the nuance here as much as possible
  - The ***best case scenario*** is that everyone in your organization understands the reality of the DR plan's weaknesses, rather than believing it to be something to follow to the letter in an actual emergency.



Lie 2: A real-life disaster scenario will be unambiguous

Lie 2: A real-life disaster scenario will be unambiguous

- Interview the folks who would be “pulling the lever”
  - How do they feel about that?
  - Help them practice it to feel better about it.
- Use real, past scenarios to feed into DR practice
  - The more realistic the scenario for execution (gradual realization, or difficult tradeoffs, for example), the better the practice will be for everyone



Lie 3: The value in our DR plan is that it works perfectly when we need it

Lie 3: The value in DR work is when it works perfectly as planned when we need it

- You will find out very quickly who the experts in parts of your systems are when you run into trouble
- So will all of the people in your organization participating in the test
- After the test, an action item worth considering is disseminating knowledge about the experts and technical system that has been involved in resolution to as many folks in your organization as possible.

What do you think?
(Thanks!)

Questions?

Image credits:

Slide: Definitely AI generated - https://technewsme.com/aws-middle-east-disrupted-after-objects-struck-datacenter-amid-escalating-iran-war/

Slide: Shoreham Nuclear Power Plant, Robert Chartuk, South Shore Press, 2025

Slide: NOAA's National Ocean Service - Exxon Valdez Oil Spill, 1989 (Public Domain)

Slide: Cover picture, Lee Clarke’s Mission Improbable, 2001 University of Chicago Press site.

Slide: Nederlands: Lies Terschelling, Rob Koster, 2007 (Creative Commons)