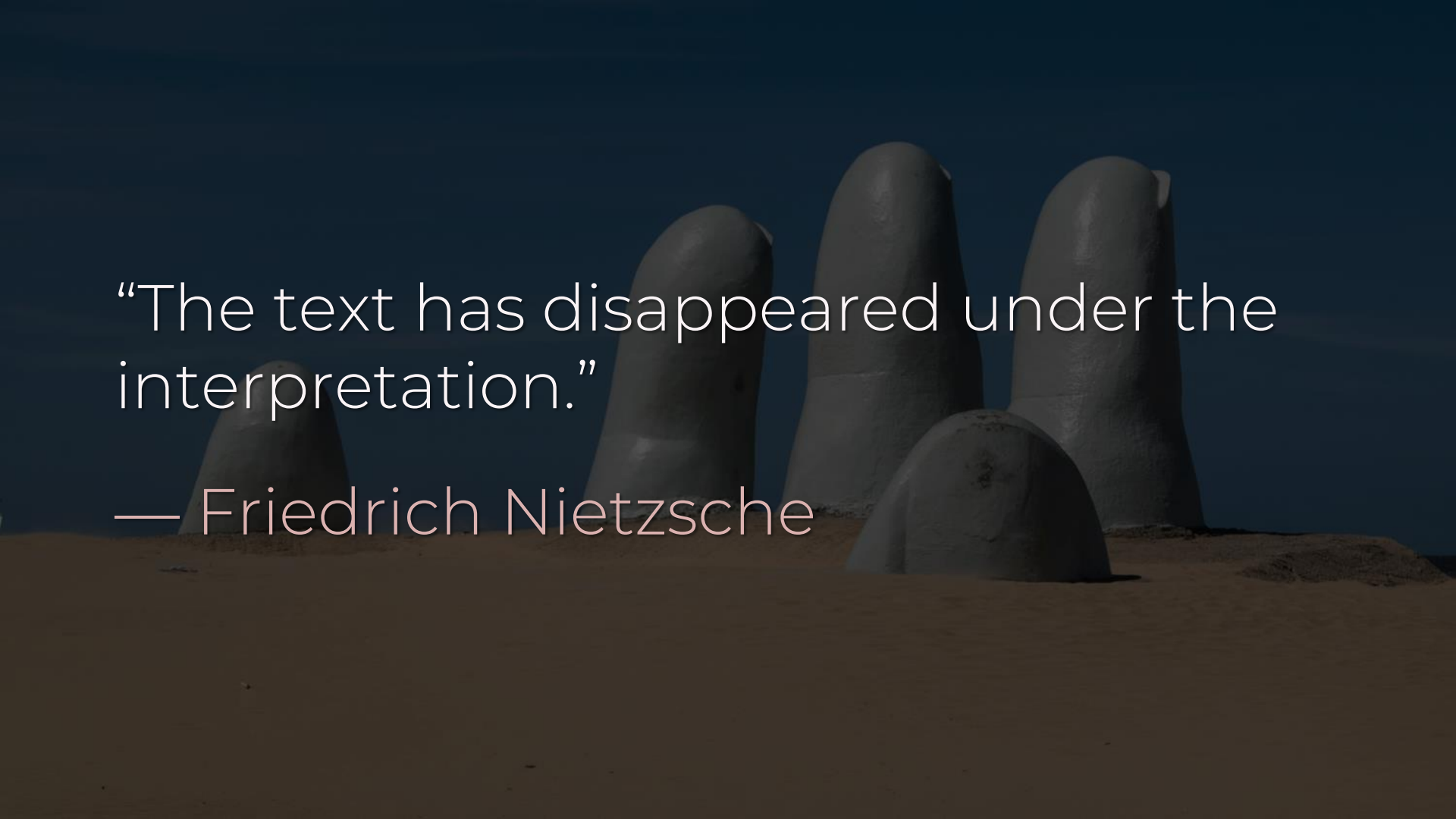
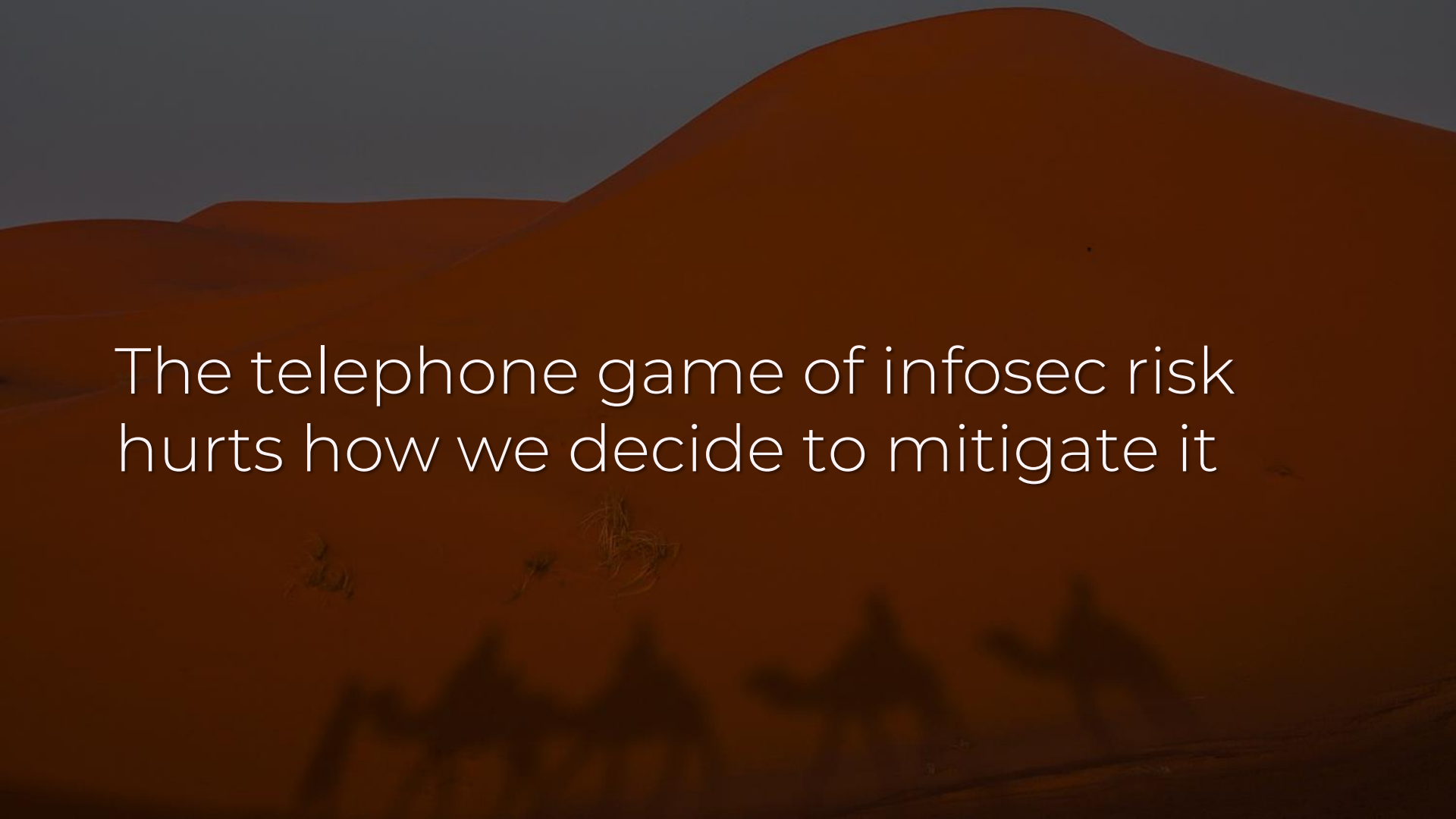
Risk Quicksand in Information Security

Kelly Shortridge (@swagitda_)

Art into Science 2019


Hi, I'm Kelly


“The text has disappeared under the interpretation.”
— Friedrich Nietzsche


The telephone game of infosec risk
hurts how we decide to mitigate it


Full implications of transitions &
feedback are not properly uncovered


Uncertainty is seen as a threat, drying up our range of potential responses

Bias influences how people interpret risk, but we aren’t countering it


How can we avoid sinking & ensure infosec risk is properly considered?

1. Understanding transitions
2. Uncertainty management
3. Communicating risk


Understanding Transitions

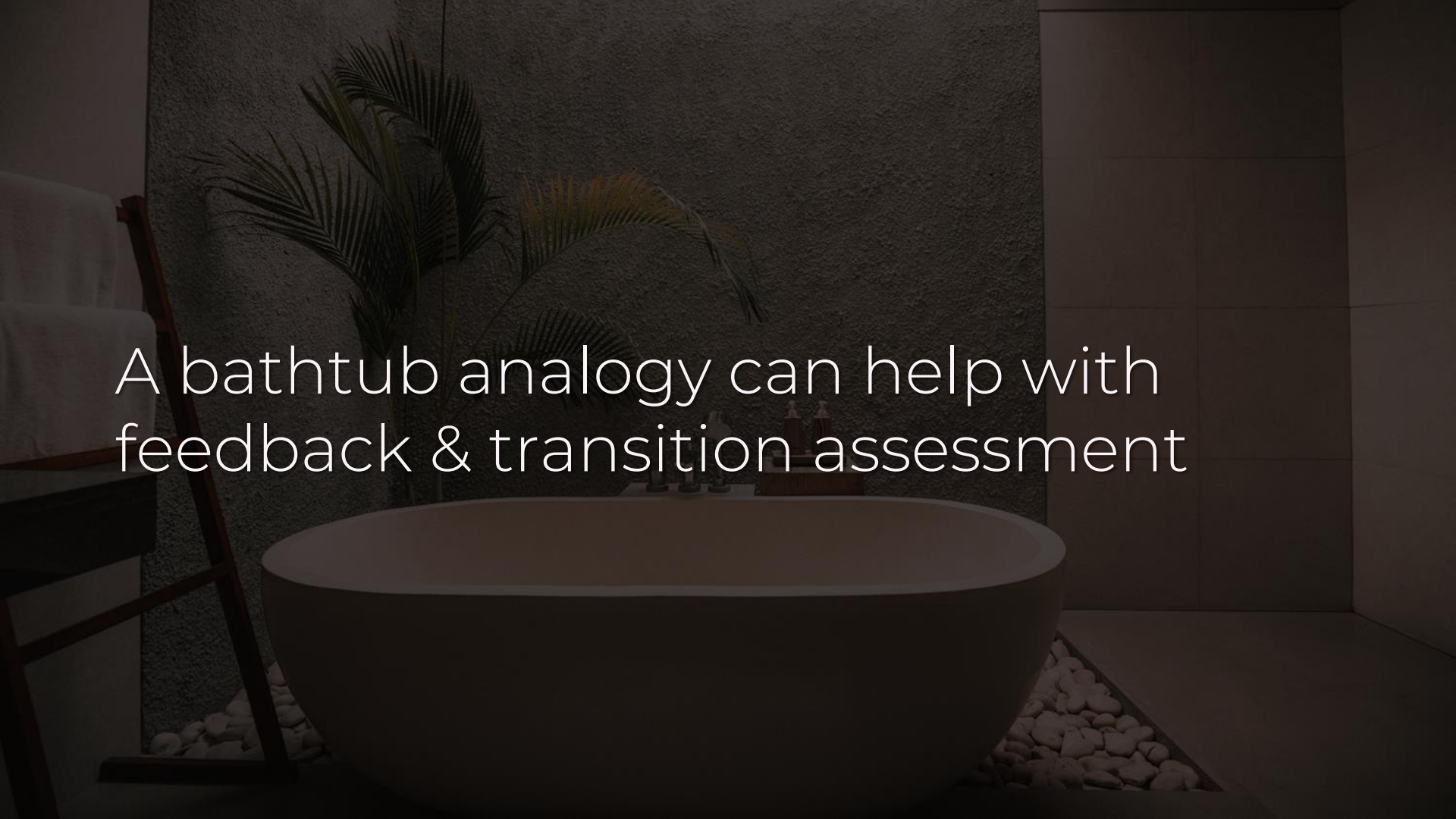
What is the riskiness of implementing a mitigation?


Adaptation Deficit – gap between
current status & goal implementation

ZTN takes years to fully deploy; are transition costs in your risk model?

Transition costs don’t justify inaction, but you do need to quantify them

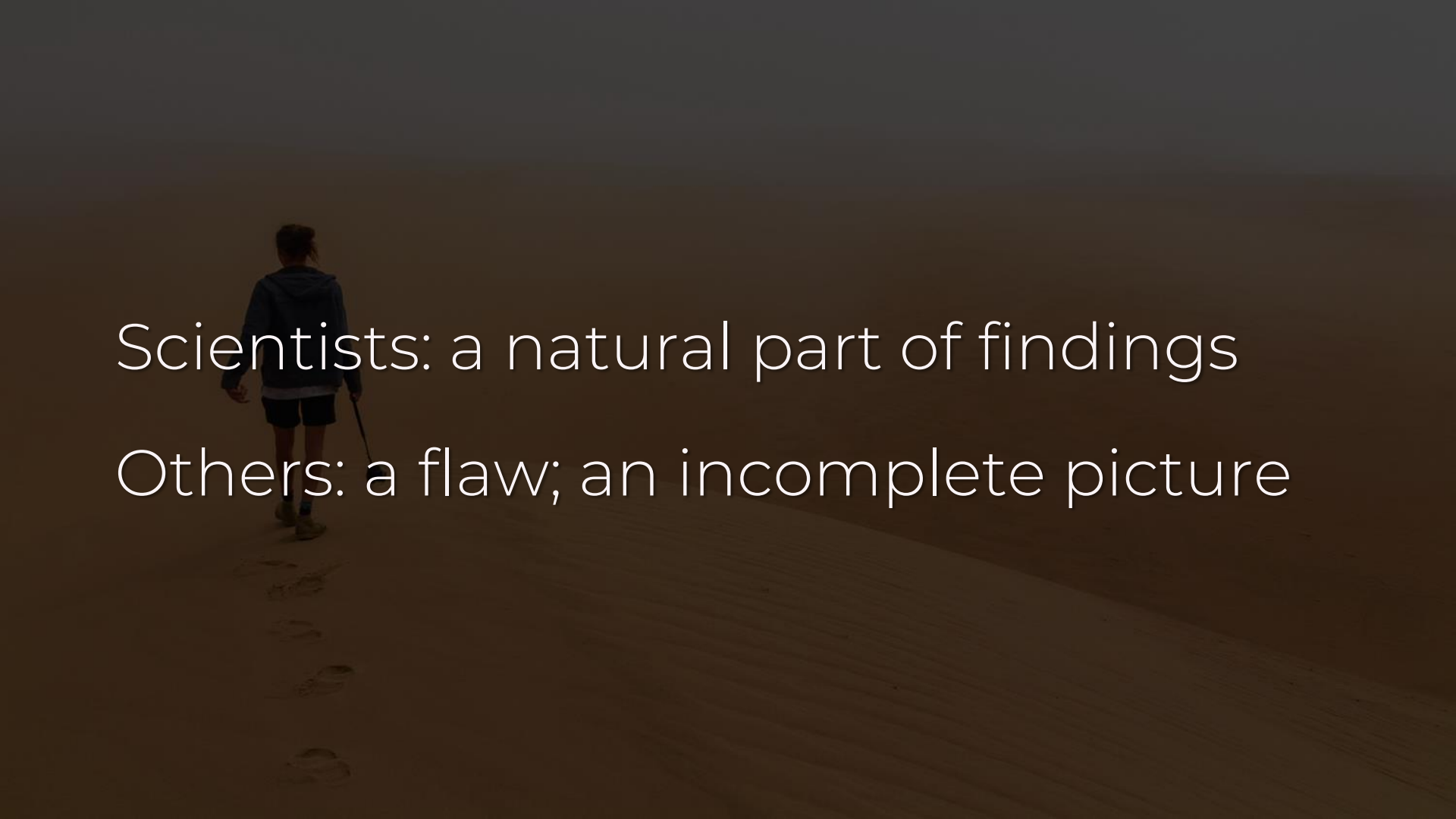
Ignoring Adaptation Deficits creates a false sense of resolution


A bathtub analogy can help with feedback & transition assessment

The “Cyber Tub” – the infosec version of the bathtub analogy

Uncertainty Management

What do we mean by uncertainty?



Scientists: a natural part of findings

Others: a flaw; an incomplete picture

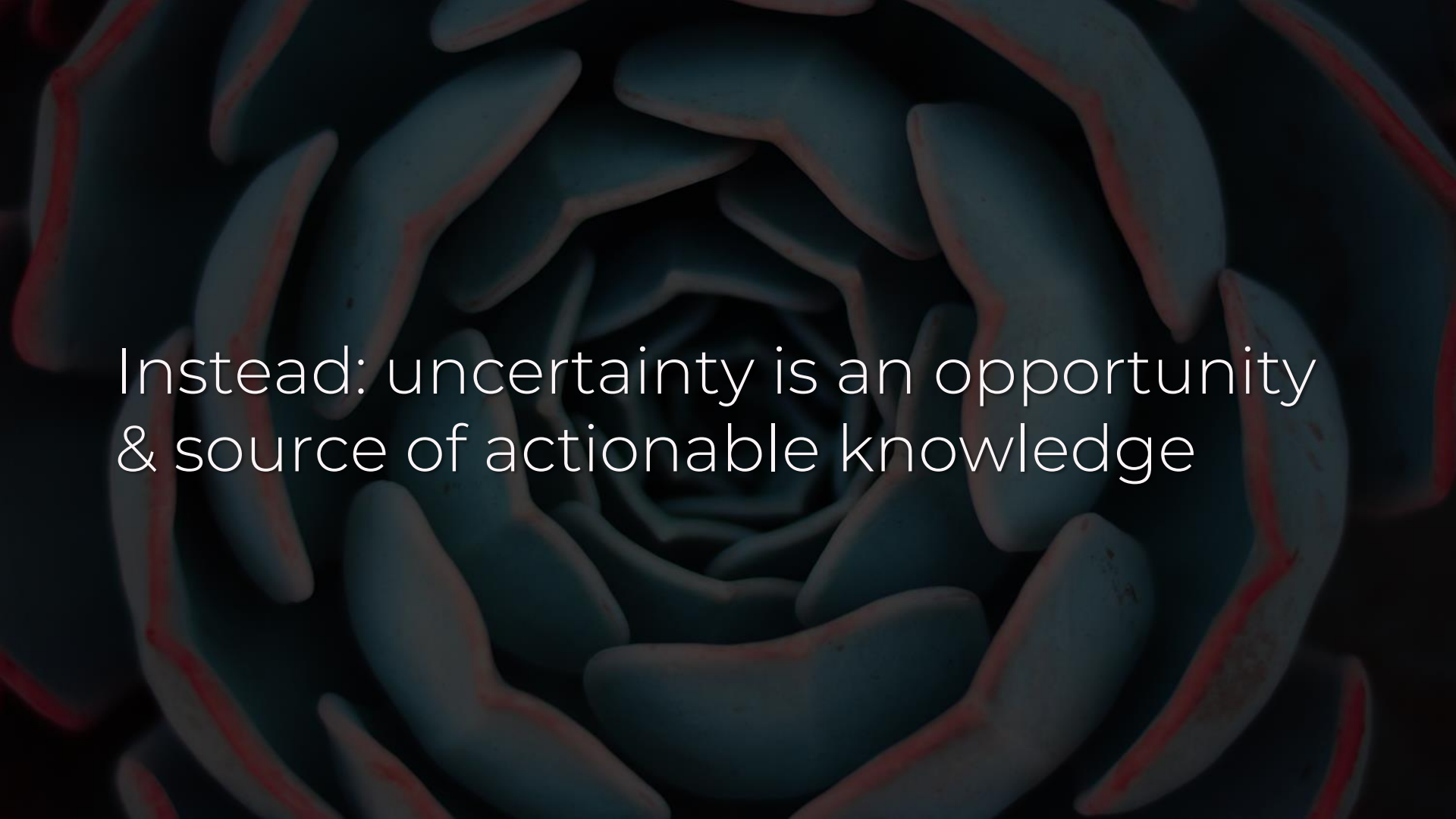
High uncertainty can encourage a “wait & see” approach for policy

“Wait & see” means the problem worsens & mitigation is too late

Action today can help lessen future uncertainty by creating data points

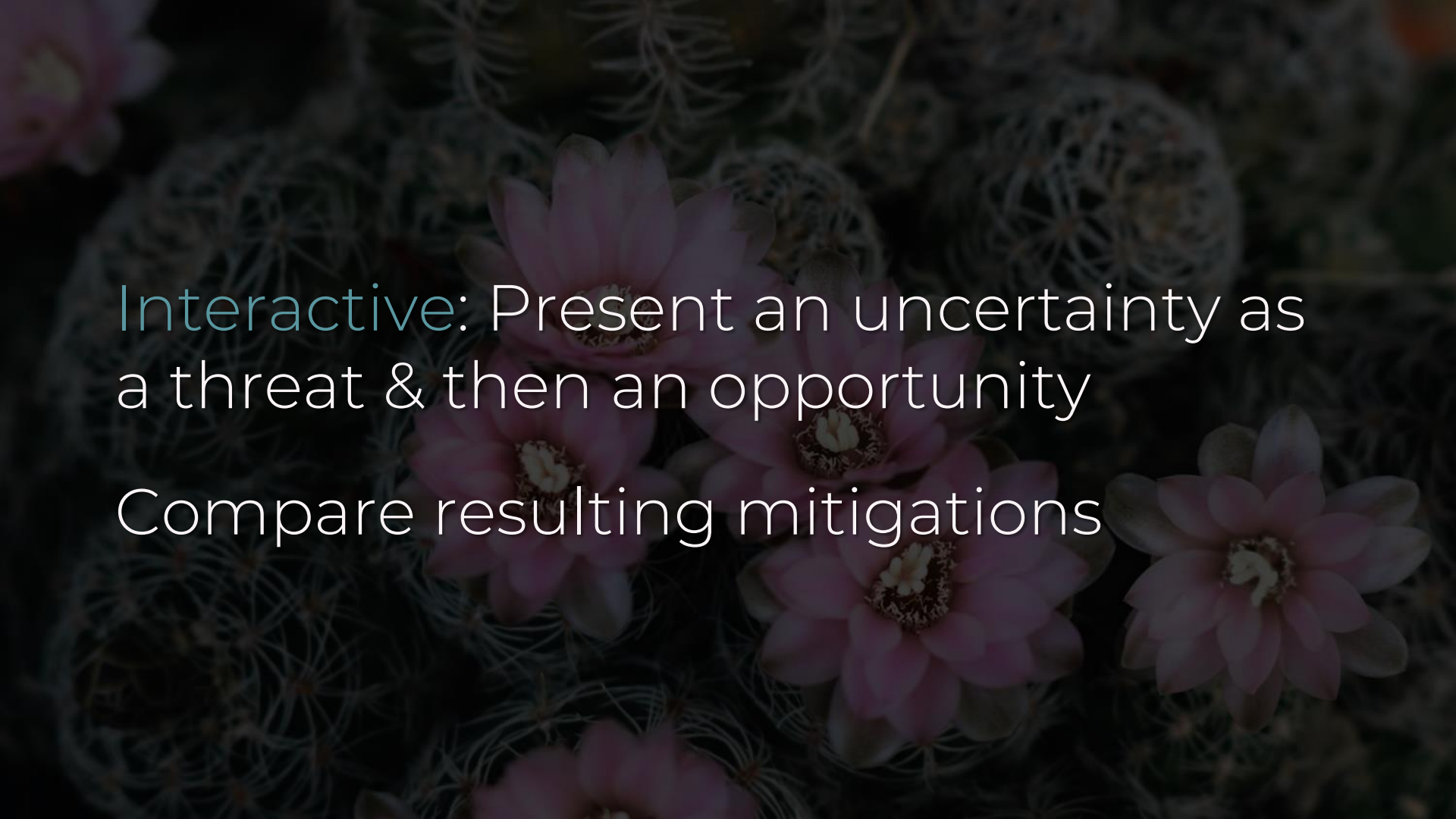

Mistake: trying to reduce uncertainty
to appease policy makers

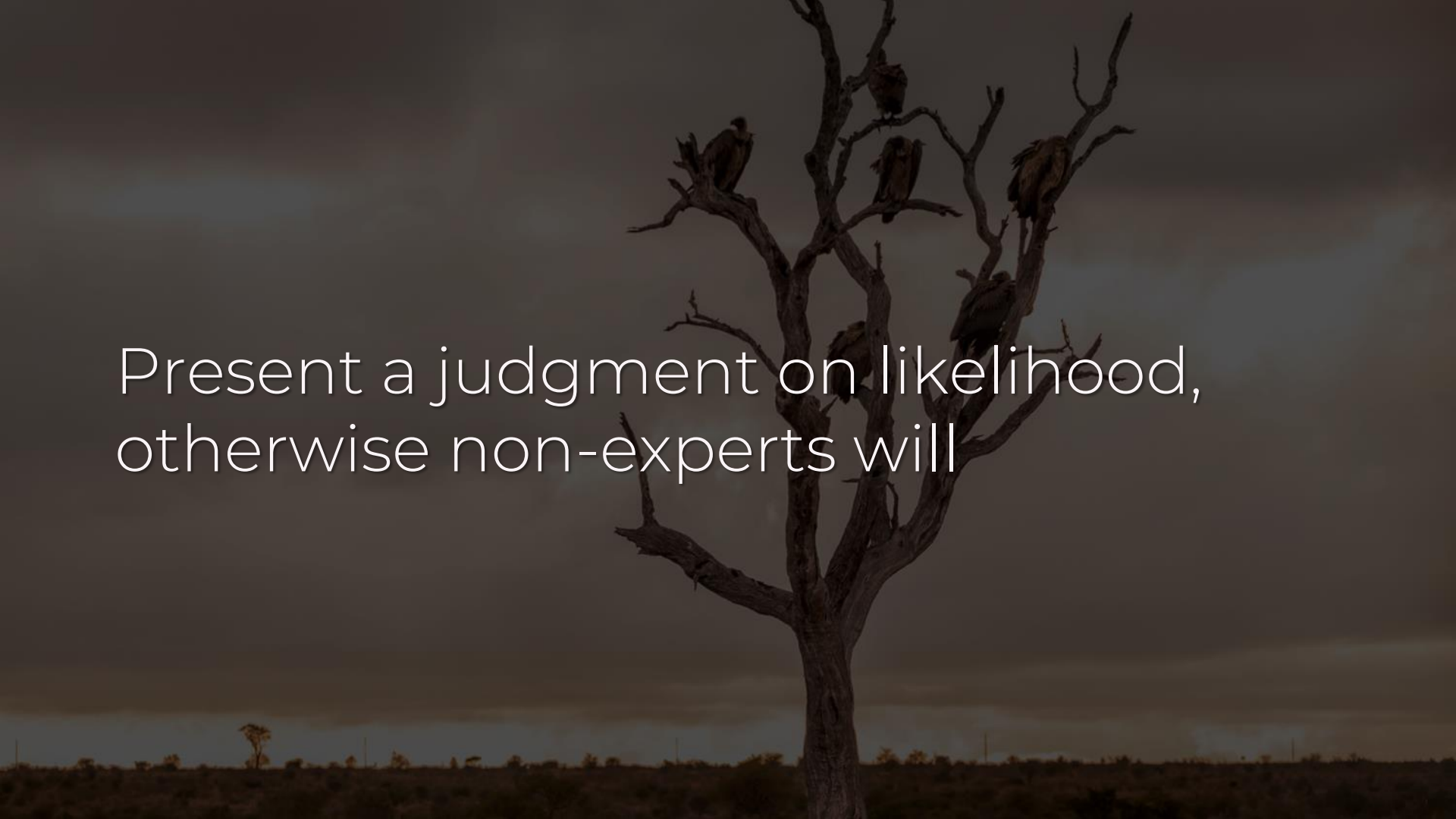
Risk people should craft the narrative – it’s not a threat, nor a call to inaction


Instead: uncertainty is an opportunity
& source of actionable knowledge

“Web app can be taken offline” vs.

“Uncertainty about app availability”


Interactive: Present an uncertainty as a threat & then an opportunity
Compare resulting mitigations

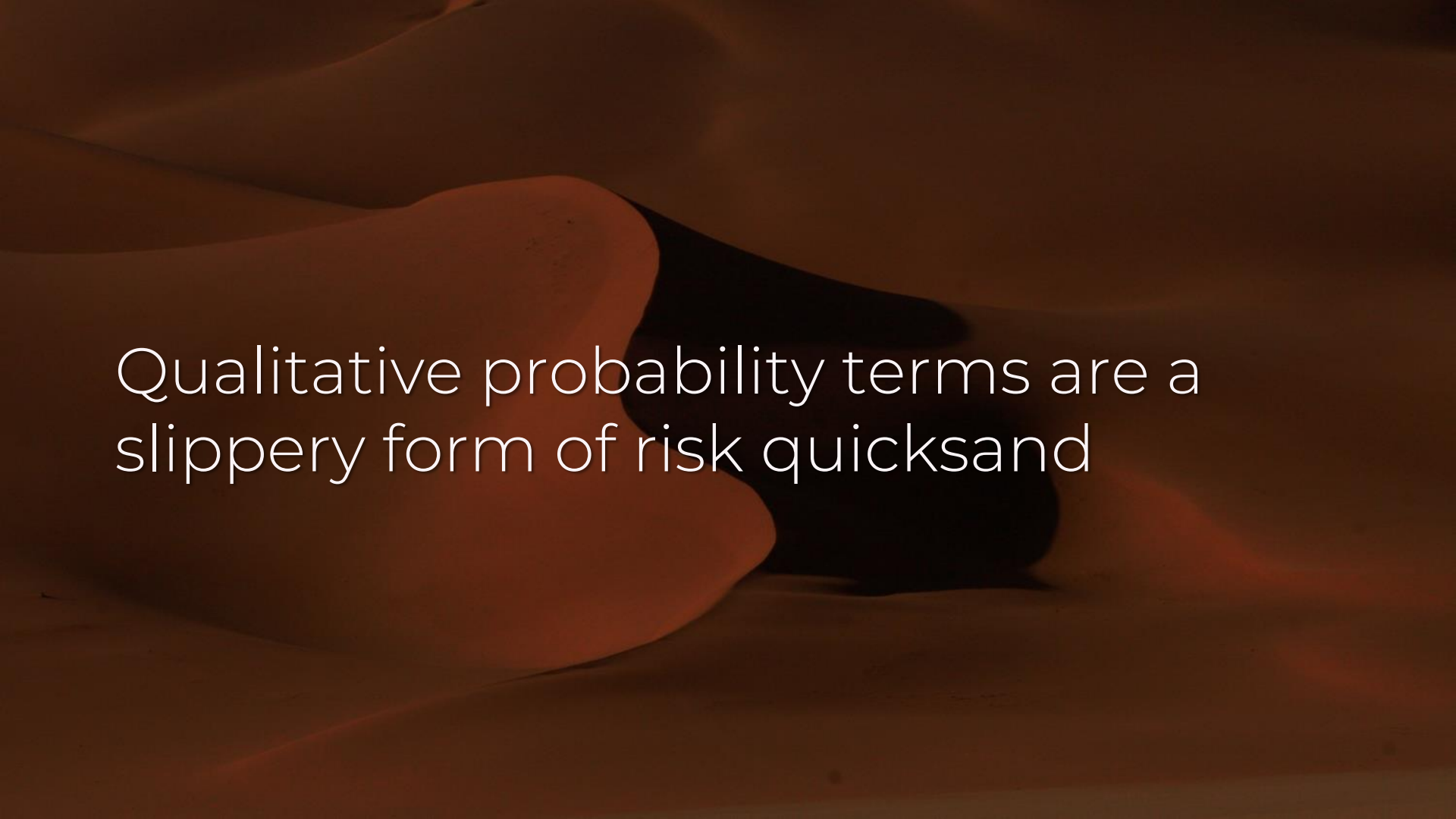

Present a judgment on likelihood,
otherwise non-experts will

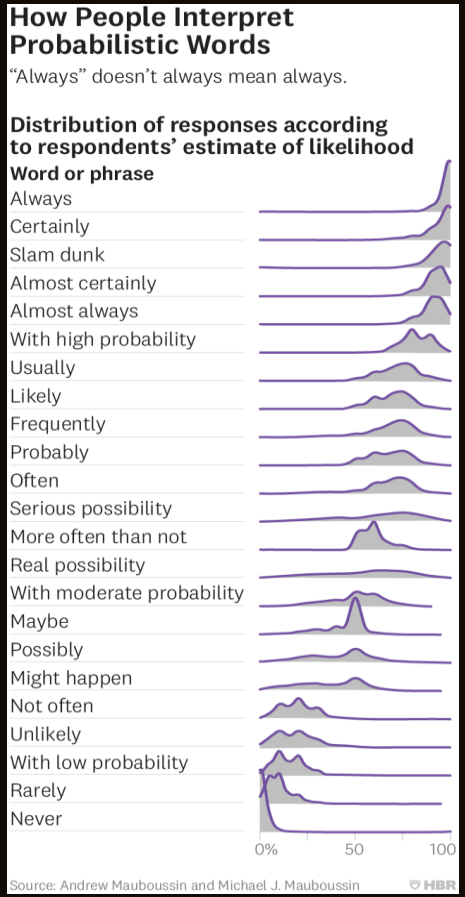
Probability density functions are your friends, full ranges are not

50% chance of 20mm user records &
90% chance of 5mm user records

vs. 100k – 50mm user records at risk

Science for policy = policymakers need expert judgement, even if it has a considerable degree of subjectivity

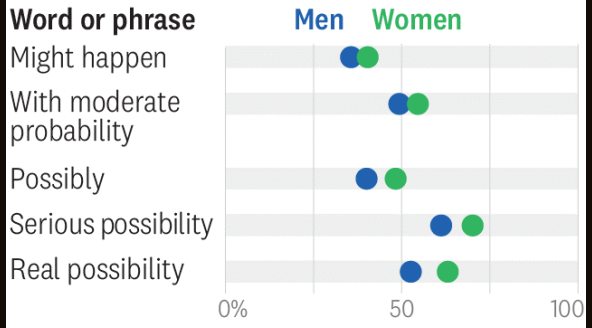

Qualitative probability terms are a
slippery form of risk quicksand


How People Interpret Probabilistic Words
"Always" doesn't always mean always.
Distribution of responses according to respondents' estimate of likelihood
Word or phrase
Always
Certainly
Slam dunk
Almost certainly
Almost always
With high probability
Usually
Likely
Frequently
Probably
Often
Serious possibility
More often than not
Real possibility
With moderate probability
Maybe
Possibly
Might happen
Not often
Unlikely
With low probability
Rarely
Never
0%
50
100
Source: Andrew Mauboussin and Michael J. Mauboussin
HBR

What's a "Real Possibility"? Men and Women Answer Slightly Differently

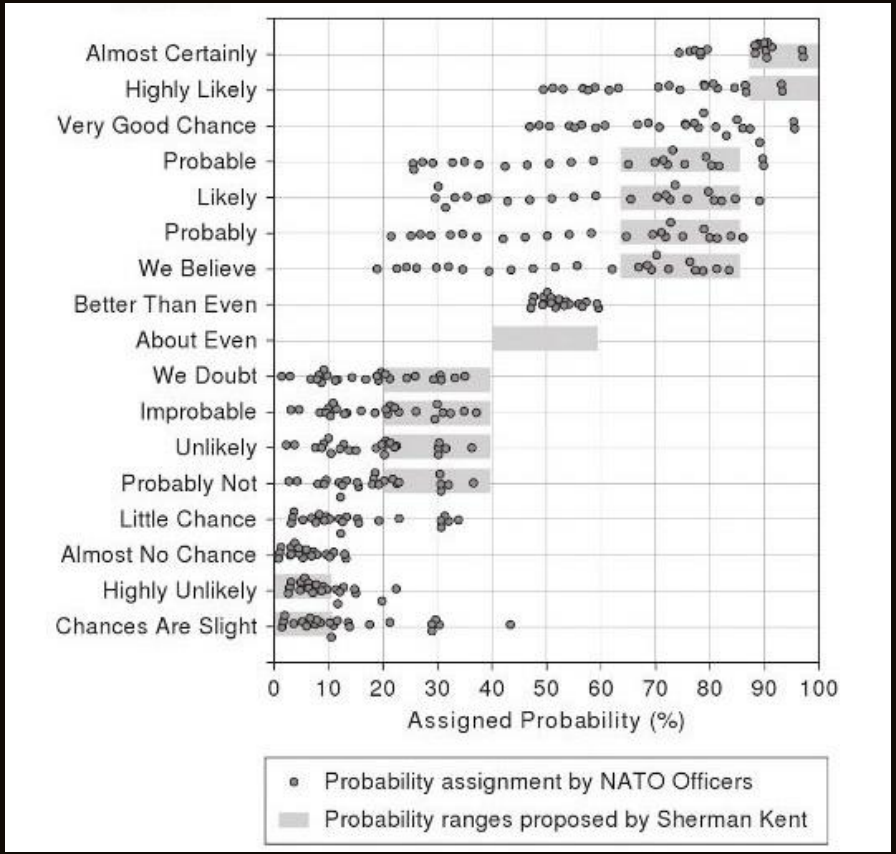
Women are more likely than men to interpret certain probabilistic words or phrases positively (i.e., as indicating that an event will occur).

Average of responses according to respondents' estimate of likelihood



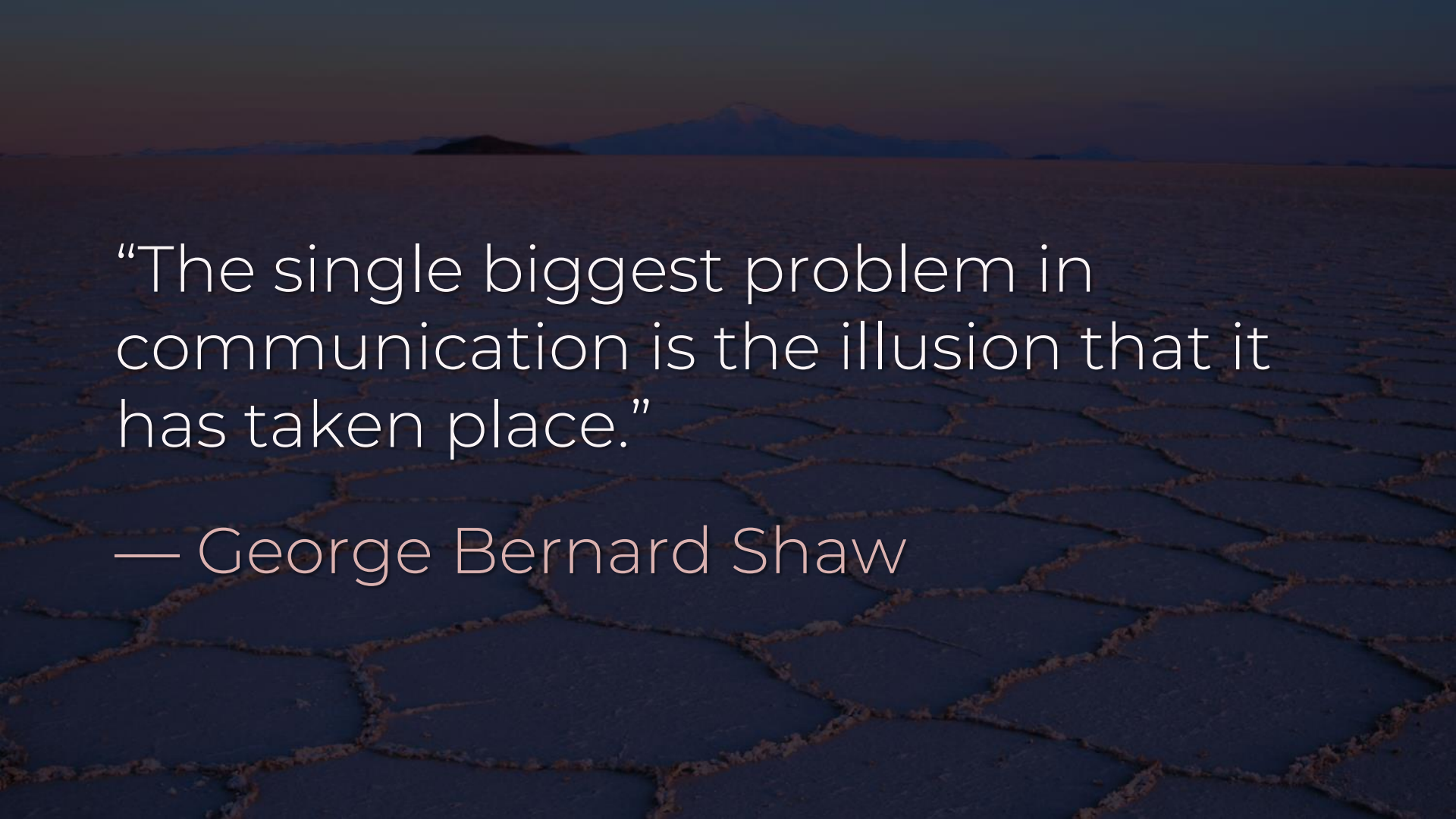
Source: Andrew Mauboussin and Michael J. Mauboussin

HBR


Almost Certainly
Highly Likely
Very Good Chance
Probable
Likely
Probably
We Believe
Better Than Even
About Even
We Doubt
Improbable
Unlikely
Probably Not
Little Chance
Almost No Chance
Highly Unlikely
Chances Are Slight
0 10 20 30 40 50 60 70 80 90 100
Assigned Probability (%)
Probability assignment by NATO Officers
Probability ranges proposed by Sherman Kent

Use percentages & PDFs when possible to avoid misinterpretation

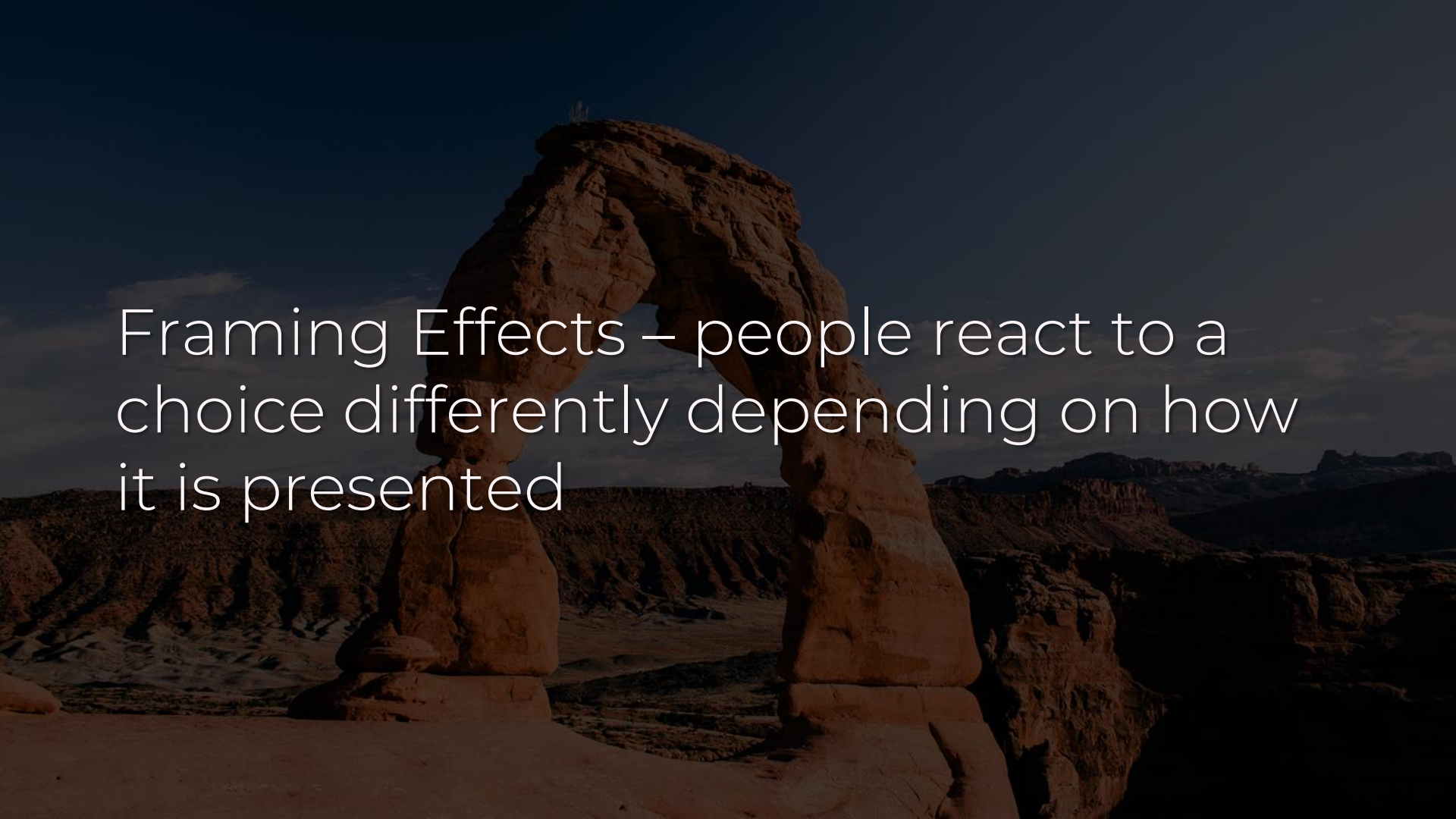
Communicating Risk


“The single biggest problem in communication is the illusion that it has taken place.”
— George Bernard Shaw

Risk is not an abstract concept – attitudes & tolerance to risk by decision makers influence it


“Science as policy” – provide info in order of its impact on decisions

Consider biases – & gently remind others when they succumb to them


Framing Effects – people react to a choice differently depending on how it is presented

Portray the risk in both past and present terms

“We’ll have less client confidence than in the past” / “Our ability to attract new clients will be eroded”

Availability bias – how easily you recall an event affects your perception

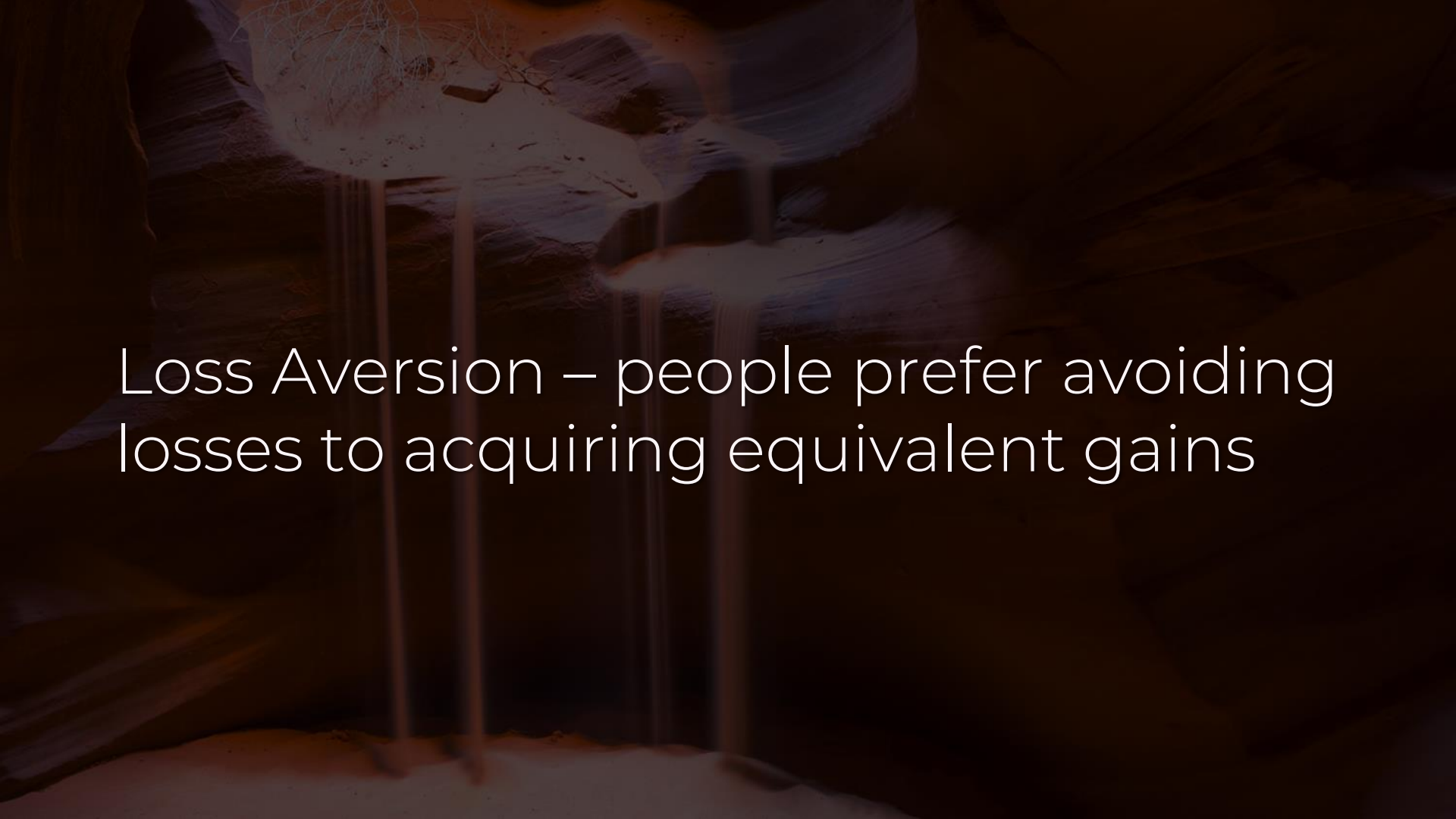

Dramatic headlines will be top of
mind & influence risk perception

Counter: anticipate what might be top of mind or not & come with data

Status quo bias – moving away from current plans can be seen as failure

“We can create our own canaries!” but then you never do, wasting more time than it would cost to buy & deploy

Counter: delay decision time & present a narrow range of options

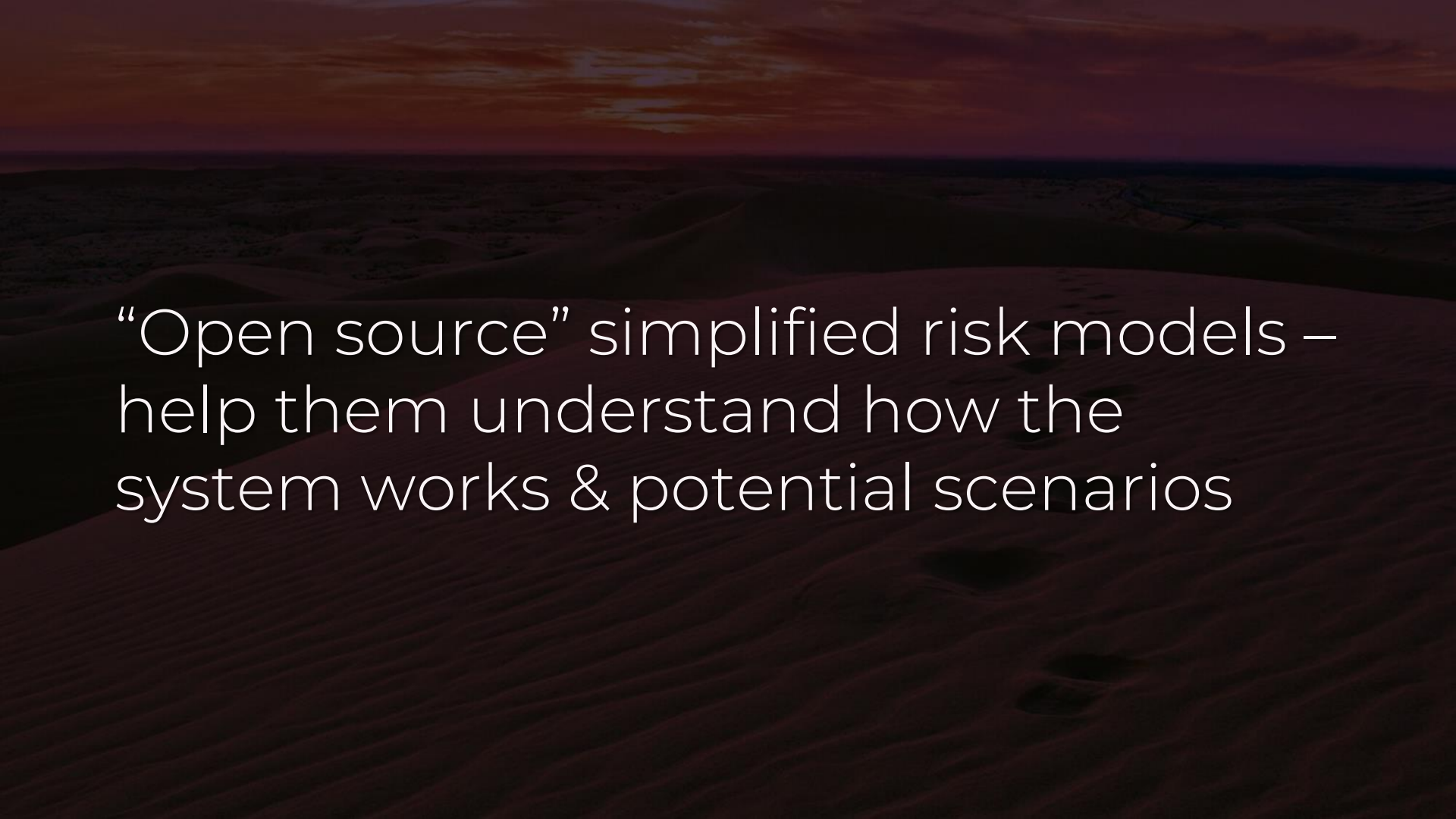

Loss Aversion – people prefer avoiding losses to acquiring equivalent gains

Counter: Use the endowment effect to emphasize irreversible loss

“We will lose our software velocity, with a 90% chance of slowing our time to deploy by 33% if ___ happens.”


Scientists learn through iterative,
interactive learning processes

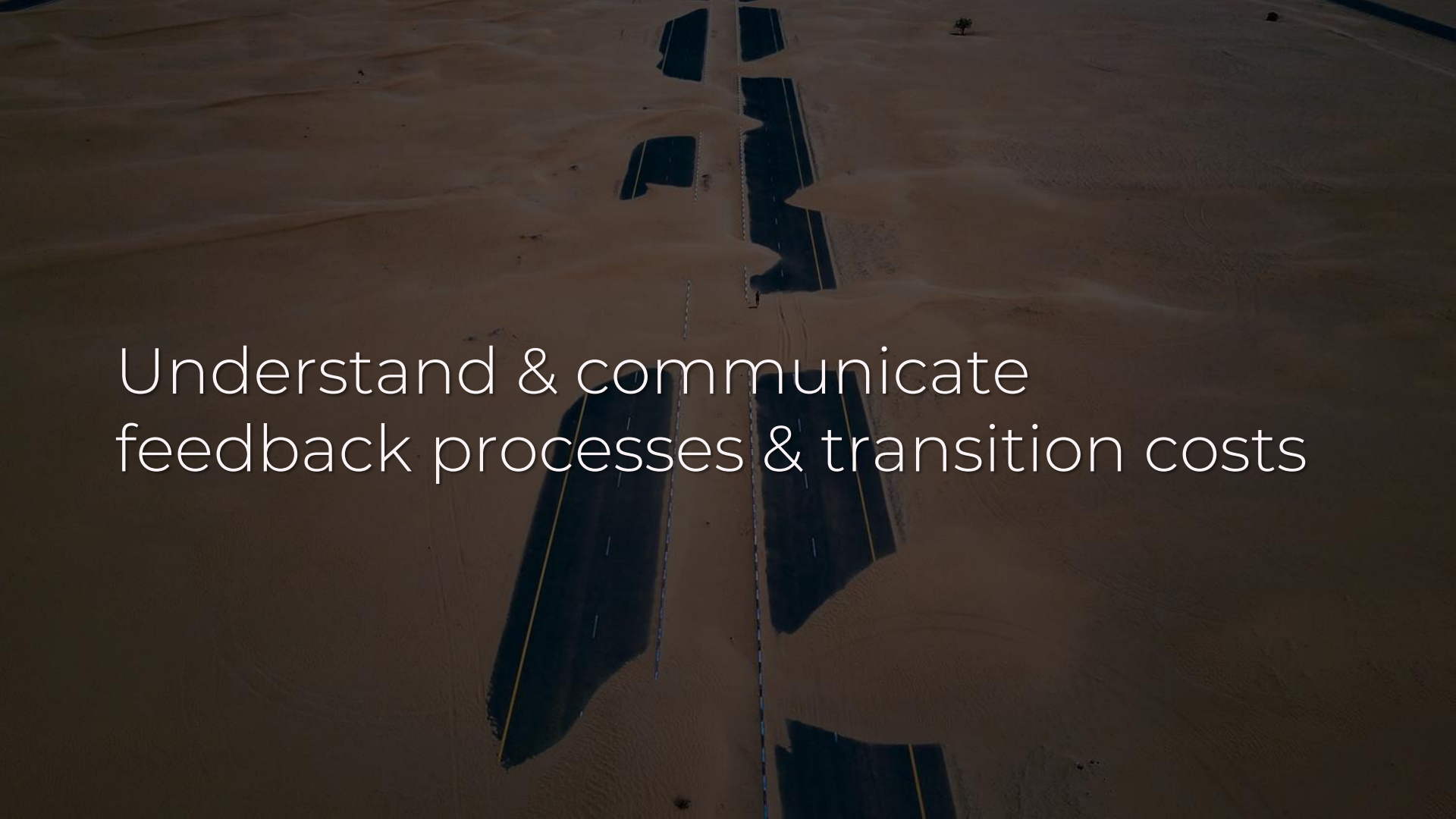
But we tell results to others with presentations, facts, & figures


“Open source” simplified risk models –
help them understand how the
system works & potential scenarios

Create your own “Cyber Tub,” or use straightforward causal diagrams

Choose the right data – aim for the highest impact vs. completion

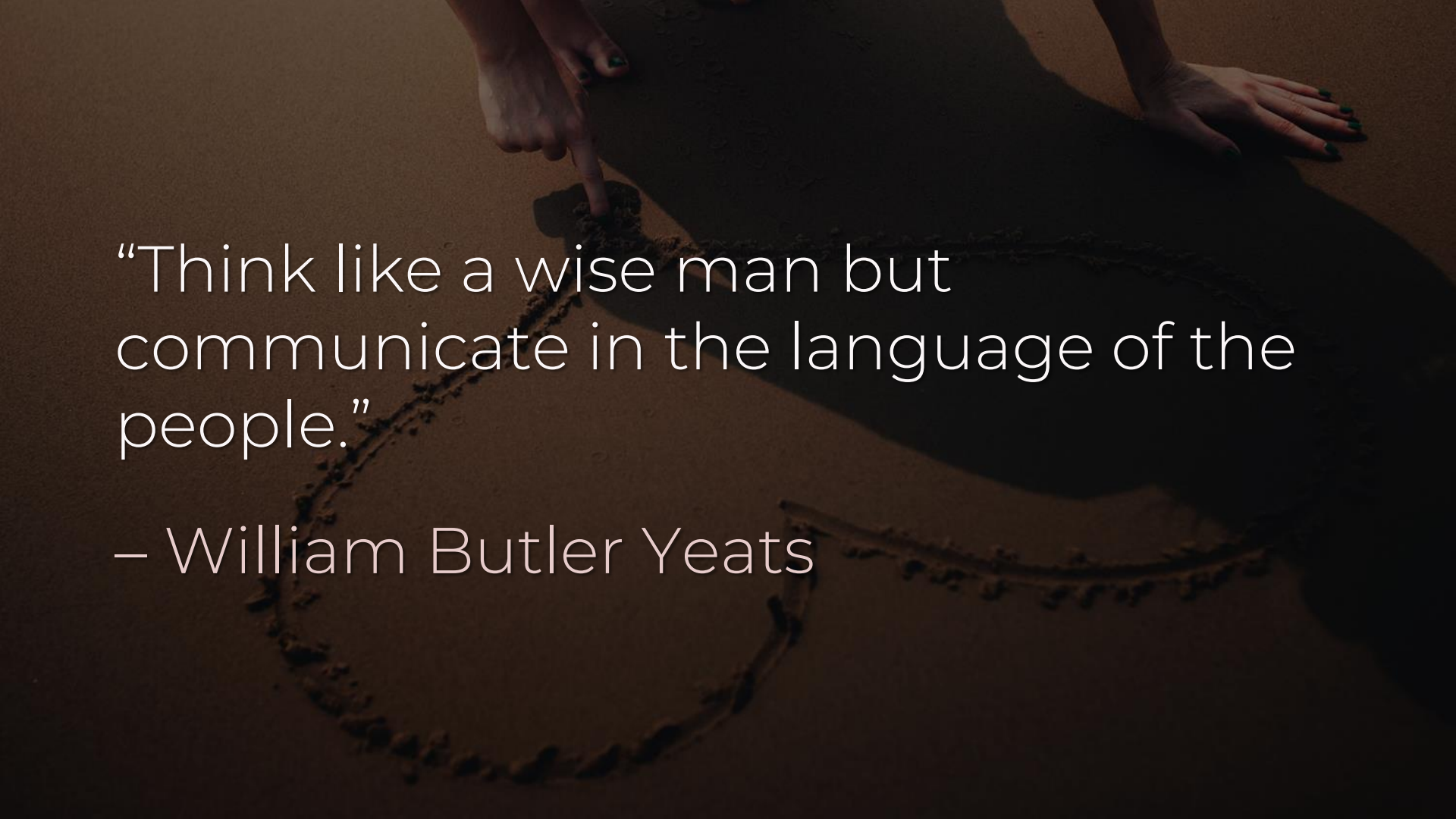

Conclusion


Understand & communicate
feedback processes & transition costs


Embrace uncertainty as an
opportunity, not a threat


Communicate through a “science for policy” lens & give your expert stance


Anticipate bias & frame data so
decision makers are empowered


“Think like a wise man but
communicate in the language of the
people.”
– William Butler Yeats

@swagitda_

/in/kellyshortridge

kelly@greywire.net