

A Dangerous Folly: Why Individual Attack Prediction Can't Be Our Goal

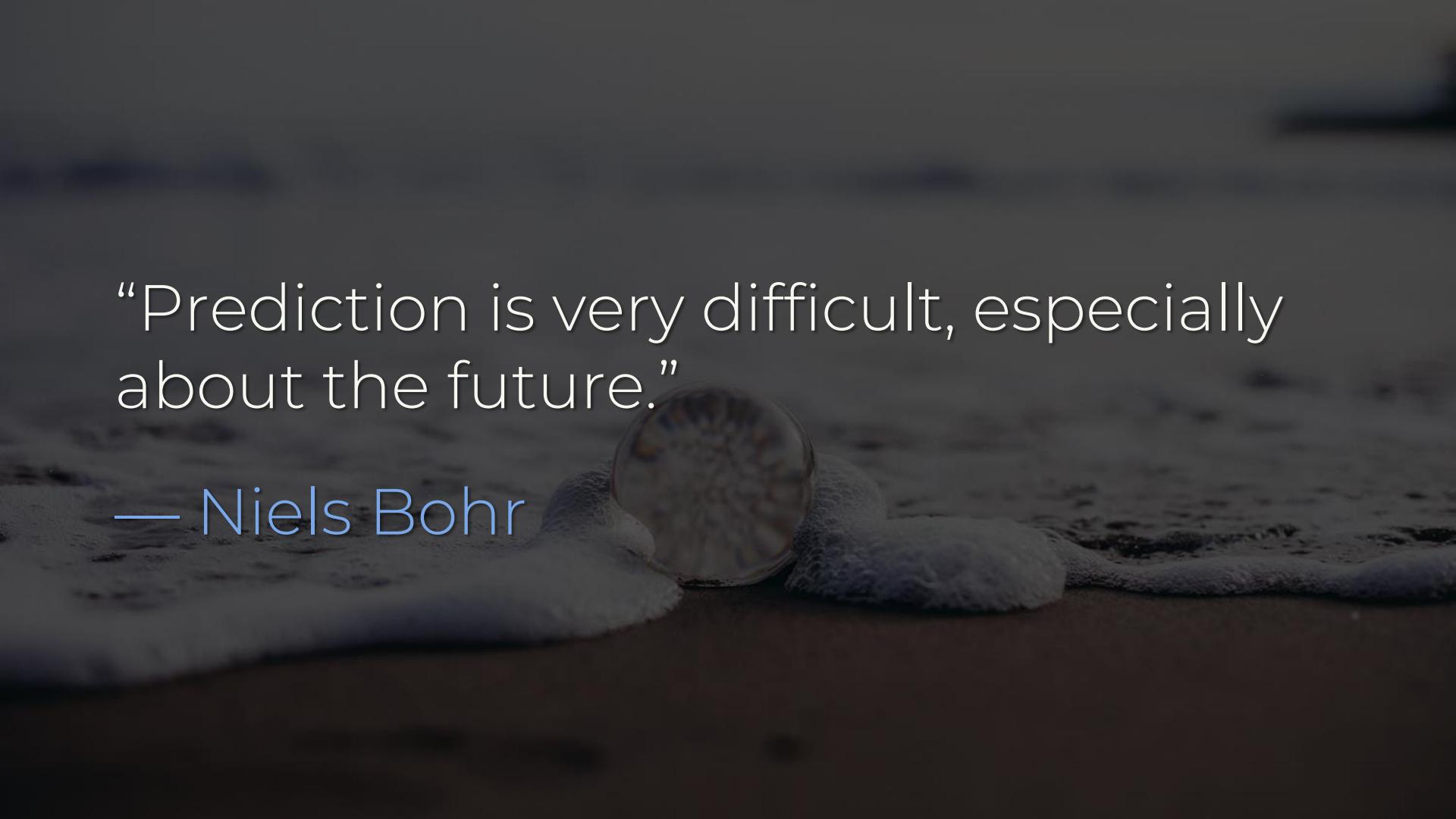
Kelly Shortridge (@swagitda_)
Art into Science 2018



Hi, I'm Kelly

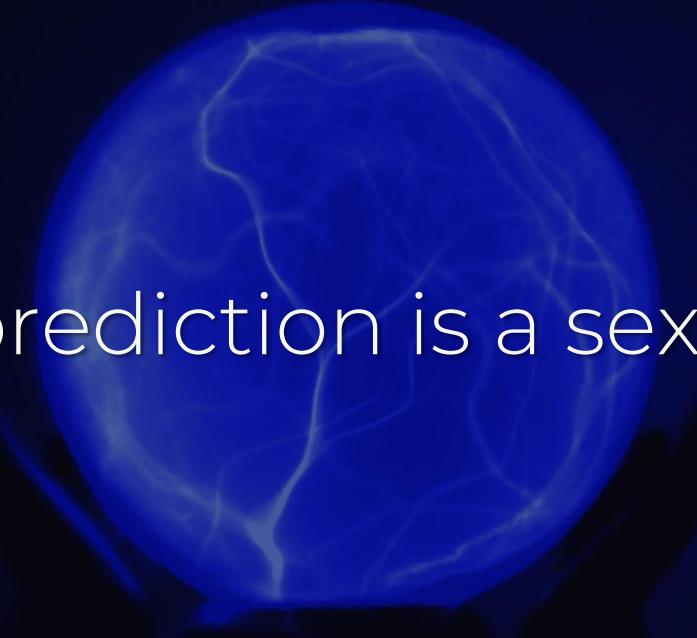


SecurityScorecard



“Prediction is very difficult, especially about the future.”

— Niels Bohr



Problem: prediction is a sexy problem

A nighttime photograph of the Austin, Texas skyline reflected in the Colorado River. The city lights are illuminated against a dark sky. In the foreground, the calm water of the river reflects the lights of the buildings, creating a symmetrical pattern of vertical light streaks.

Designing building codes is not

Act 1:

Why is everyone hyped on prediction
& what methods do they propose?

Act 2:

What lessons exist from other areas &
what should we do instead?

Spoiler tl;dr: predicting attacks isn't as valuable as hazard reduction

A close-up, profile photograph of a woman's face. She is wearing large, round sunglasses with dark lenses. Her hair is long and light-colored. The background is a vibrant, abstract pattern of red and white organic shapes, possibly leaves or petals, creating a dreamlike atmosphere.

Act 1

Why the interest in attack
prediction?



Fundamentally, uncertainty feels bad

A dark, moody photograph of a woman with long dark hair, wearing a blue top, leaning over a dark wooden railing. She is looking down at a city street below, where blurred lights from buildings and traffic create a bokeh effect. The scene is set at night, with the city lights providing the primary light source.

Ambiguity of potential future threats
fuels stress & anxiety

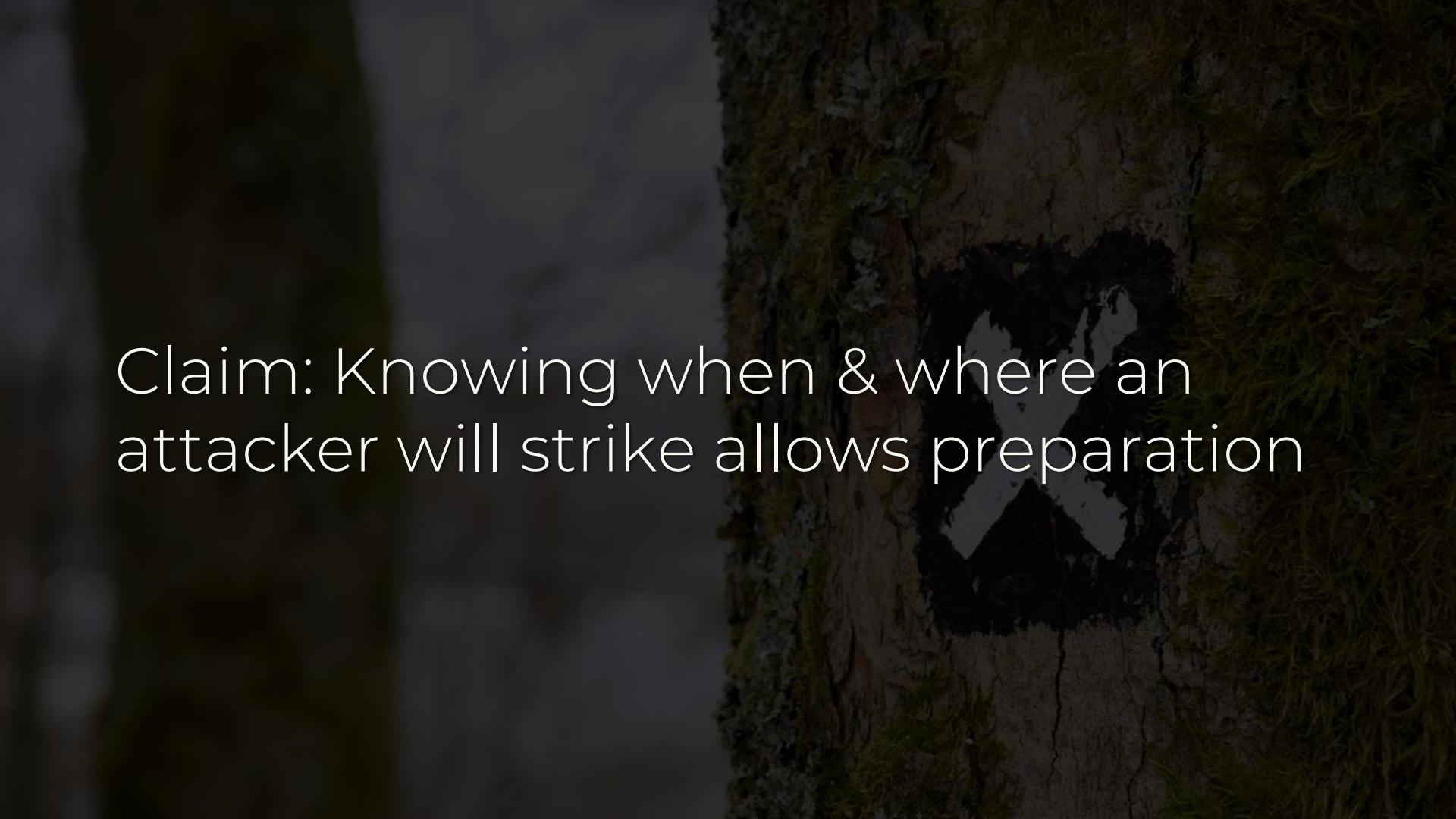
Predictable negative events are less
stressful than uncertainty

A dark, moody photograph showing two people lying in a field of tall, dry grass. The person on the left is curled up, while the person on the right is lying on their side. The background is a vast, cloudy sky.

Like reading the plot of a scary movie
before watching it

Unfortunately, predictions can give a
false sense of security

There are some “unemotional”
reasons used to justify prediction, too



Claim: Knowing when & where an attacker will strike allows preparation

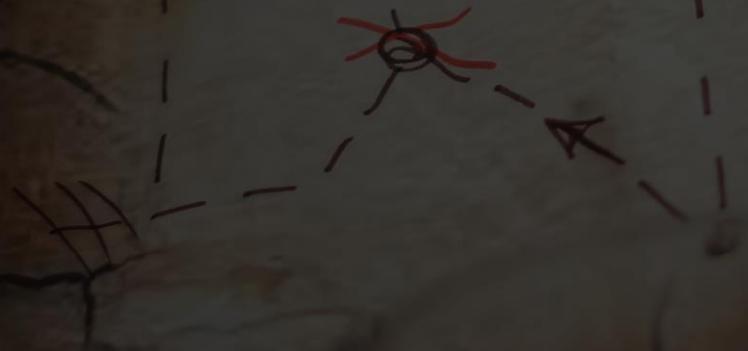
Claim: Knowing the attacker's next move helps with resource allocation

A close-up profile of a woman's face, facing right. Her skin is dark, and numerous small, glowing green particles are scattered across her face, particularly around her eyes, nose, and mouth, giving her a mysterious, futuristic appearance.

Tacit reason: precogs are cool

But do the goals align with the methods actually being proposed?

What prediction methods
are being proposed?



General theme: predict future attacks
from past & current attack behavior

Why now? Sufficient storage,
processing power, & we math better

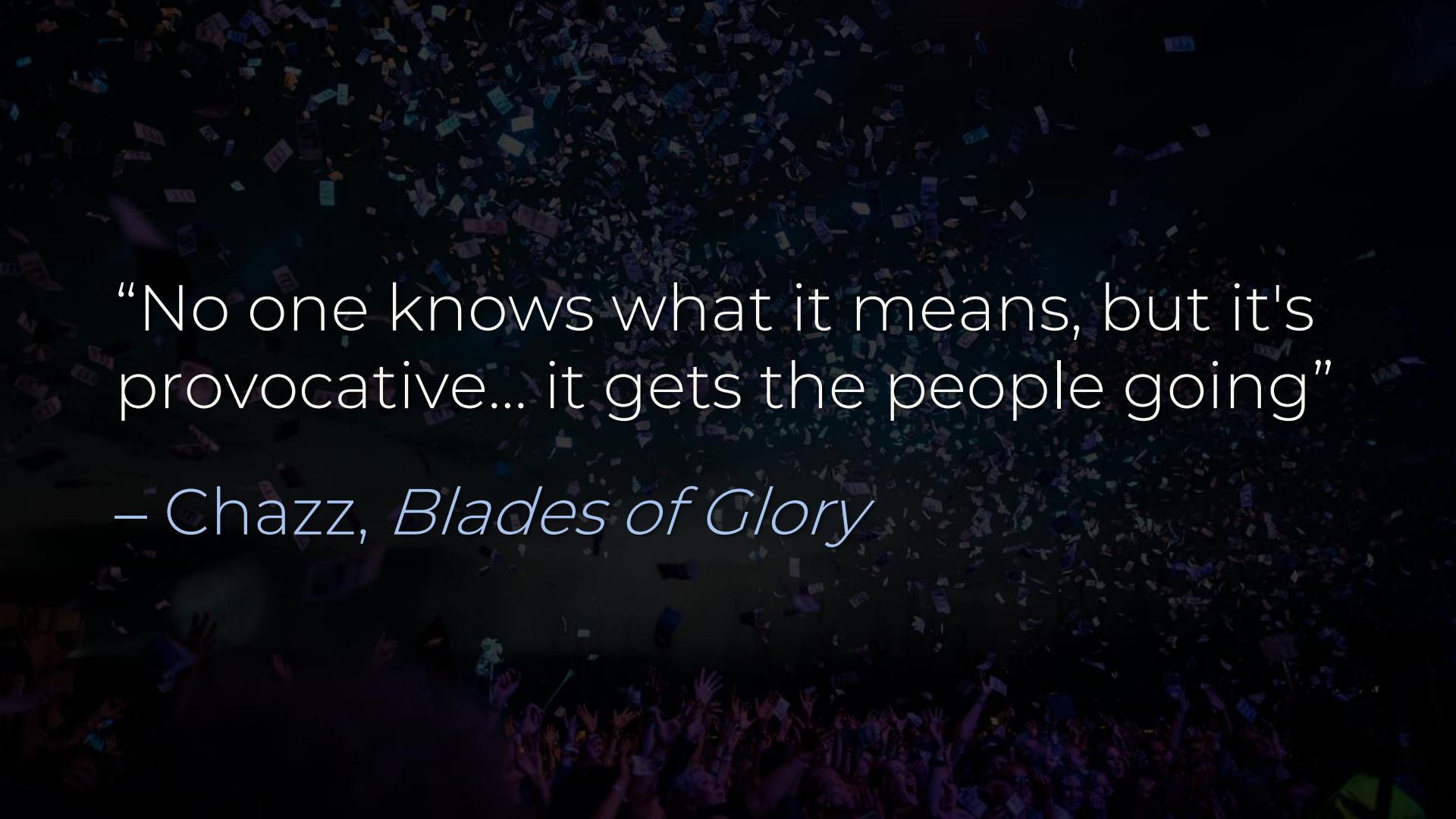
mysheen lerning mysheene lerning
masheene lerning mashene learning
mashine learning machine learning

Common idea: unsupervised machine learning to avoid false negatives



AI – i.e. a magic black box of math

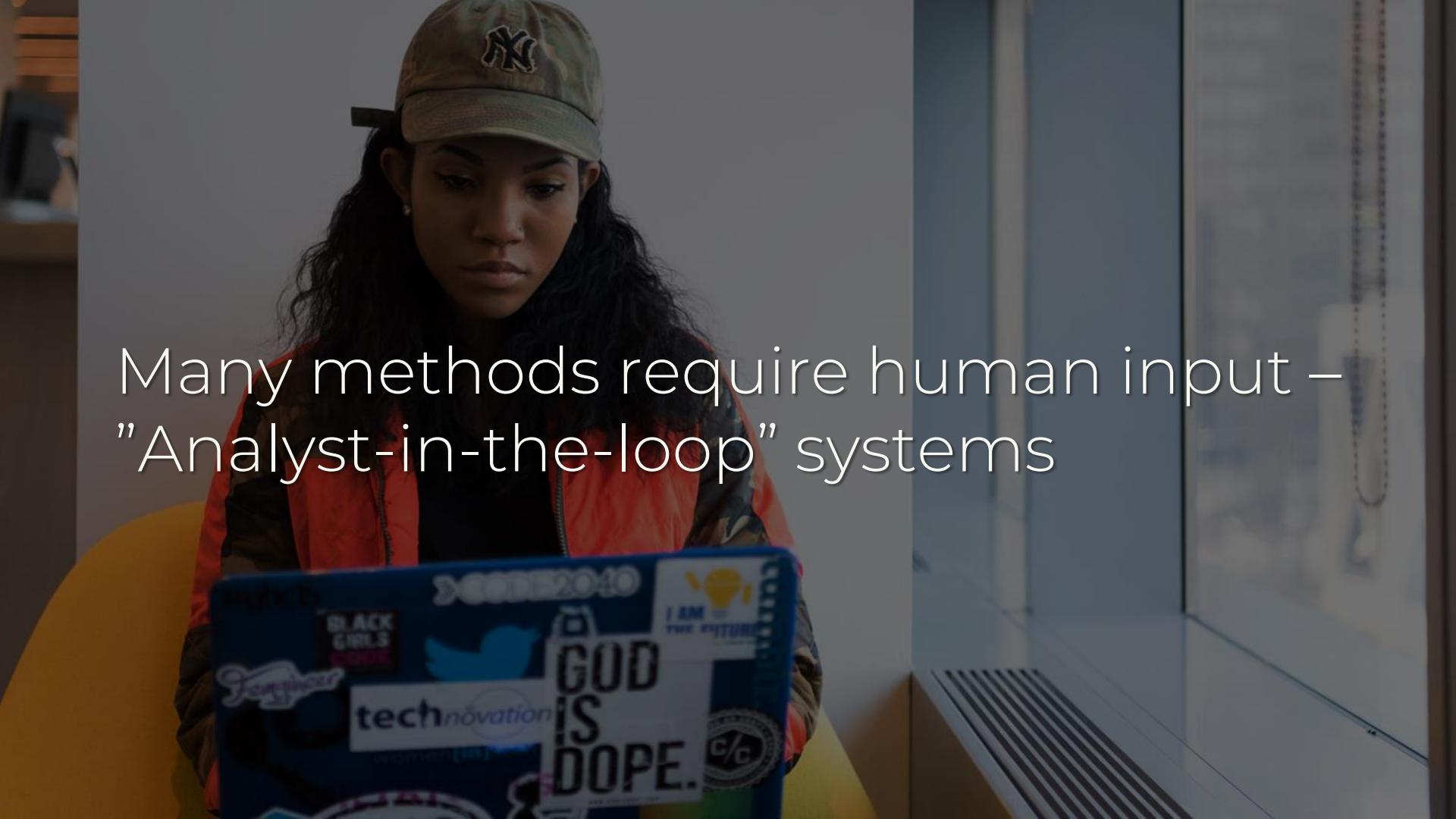
Deep learning threat prediction using
actionable behavioral analytics...



“No one knows what it means, but it's provocative... it gets the people going”

– Chazz, *Blades of Glory*

Caveat: behavioral analytics for
detection already plagued by FPs

A photograph of a young woman with long dark hair, wearing a camouflage baseball cap with a NY logo and an orange safety vest over a black shirt. She is looking down at a laptop screen which displays various logos and text. The background is a blurred indoor setting.

Many methods require human input –
“Analyst-in-the-loop” systems

AI² : fuses 3 unsupervised-learning methods & shows top events to analysts for them to label

Caveat: still focused on detection –
calling it “prediction” is a stretch

(Also, the paper reads like an ad for
IBM Watson & QRadar...)

Idea: use attacker TTPs to train your
data sci models



Caveat: it's really hard to attribute
TTPs, let alone collect them

Reallocating resources on-the-fly
based on predictions? Good luck...

Idea: social data analysis (using OSINT) to predict data breaches

Caveat: does “news” always know about breaches before the org itself?



(Also, how is it predictive if they're finding news post-breach?)

Cause analysis: what allowed the attack to happen?

Caveat: past performance is not an indicator of future performance

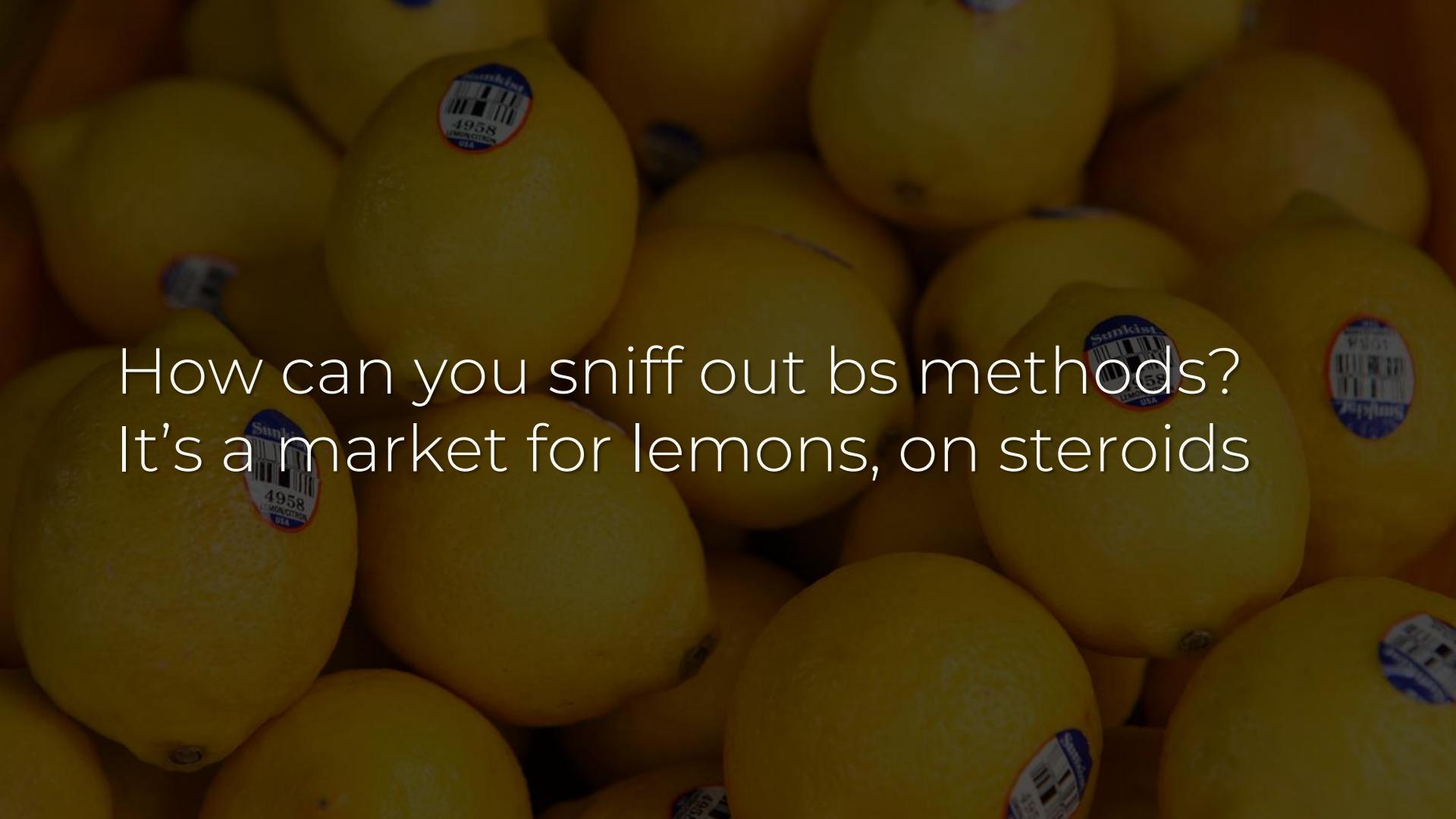
Plausible: detecting preparations
helps stop attacks before they start

A close-up photograph of a vibrant yellow canary perched on a dark, textured branch. The bird's feathers are a bright, saturated yellow, with darker greenish-yellow streaks on its wings and back. A small, metallic tracking device is attached to its right leg. The background is a solid, dark blue.

Caveat: how much does a predictive system add vs. using canaries?

Where does this leave us?

Barriers: FPs, attackers are quick to adapt behaviors, limited time/people

A close-up photograph of a large pile of ripe, yellow lemons. Several lemons have small, round stickers attached to them, which read "Sunkist", "4958", "LEMON CITRUS", and "USA".

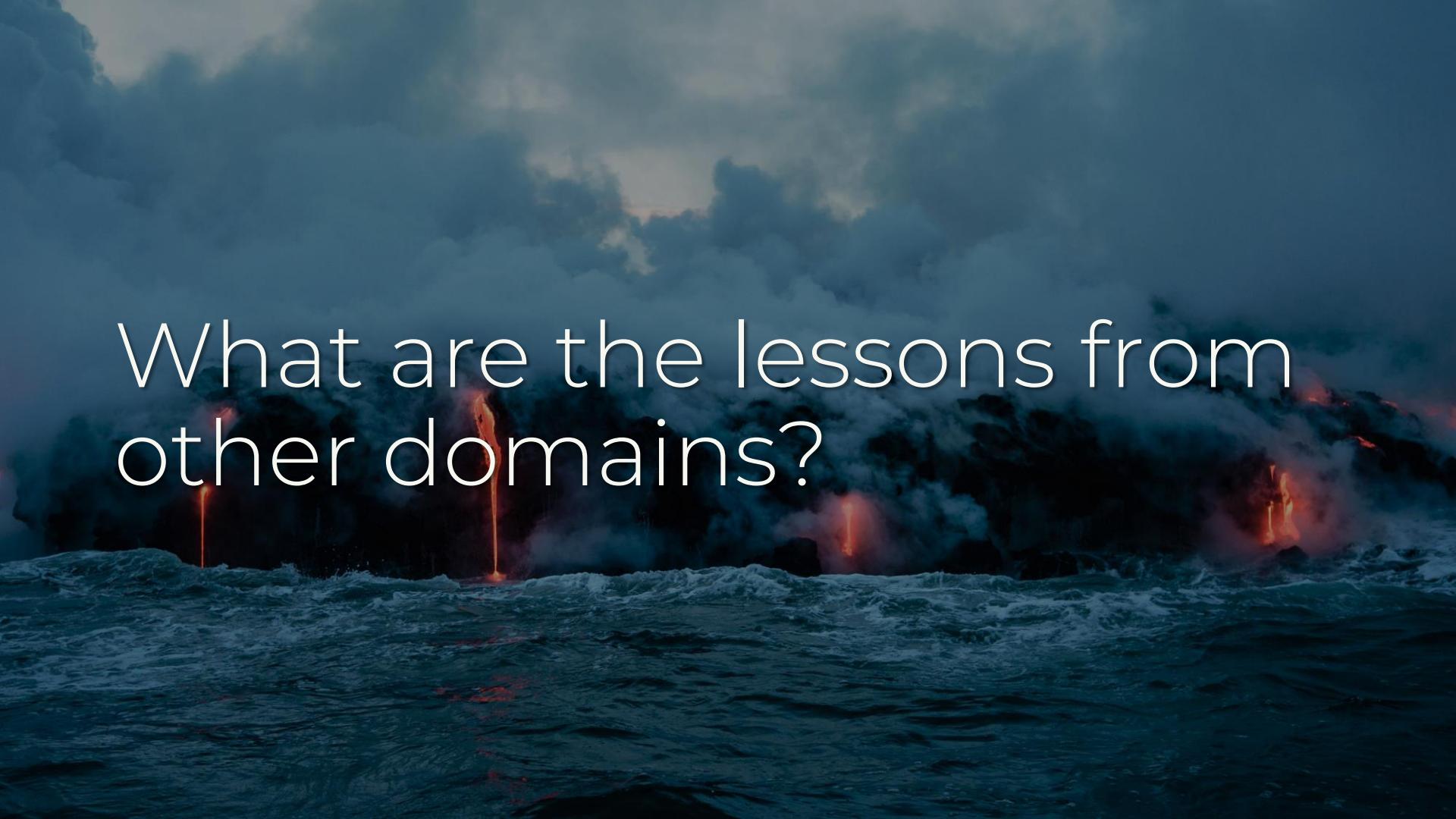
How can you sniff out bs methods?
It's a market for lemons, on steroids

How do you know what to do next?
Predictive vs. prescriptive

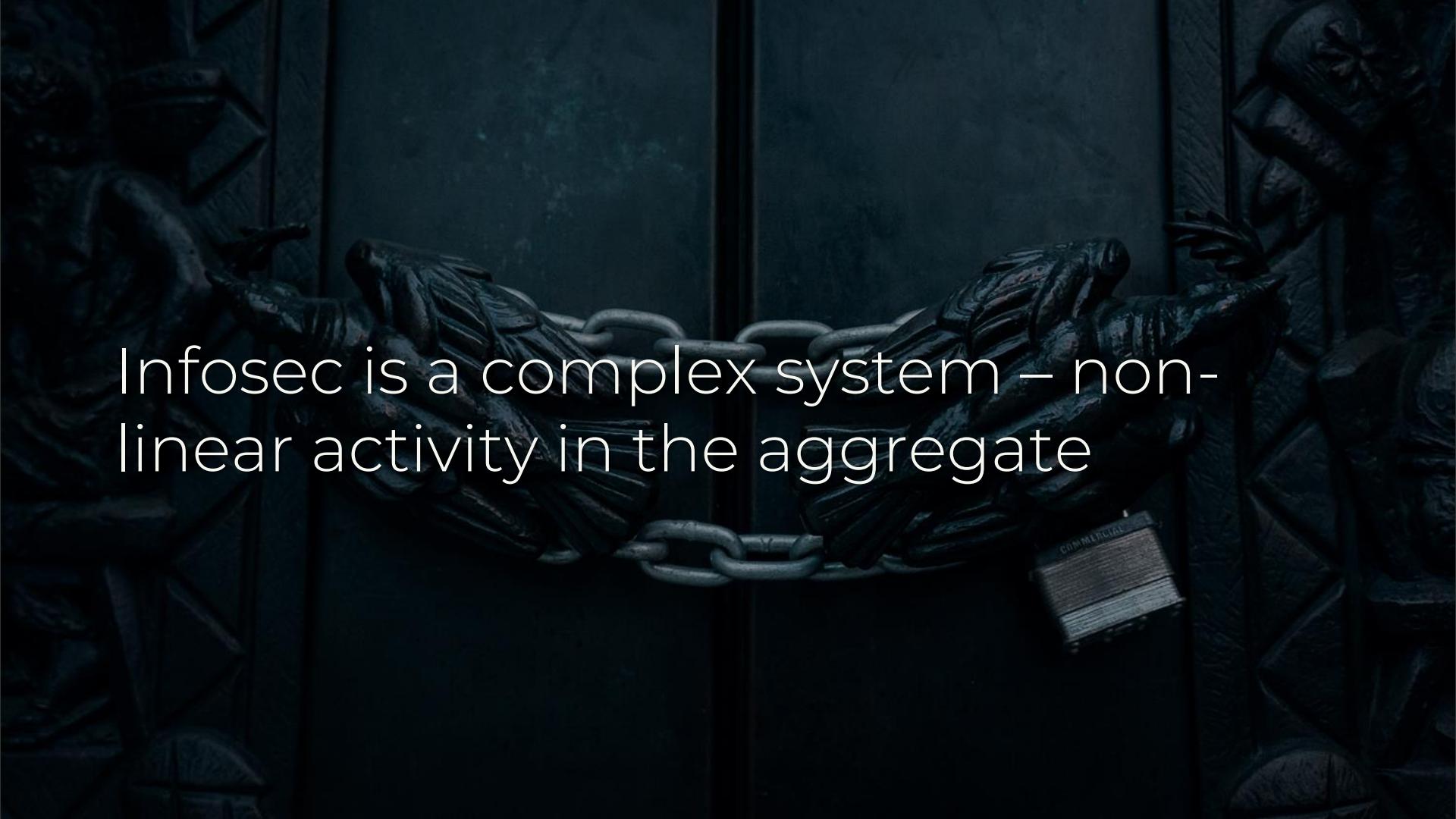
Alternative proposal: prepare your prioritized assets for the (probabilistic) worst, ahead of attack...



Act 2

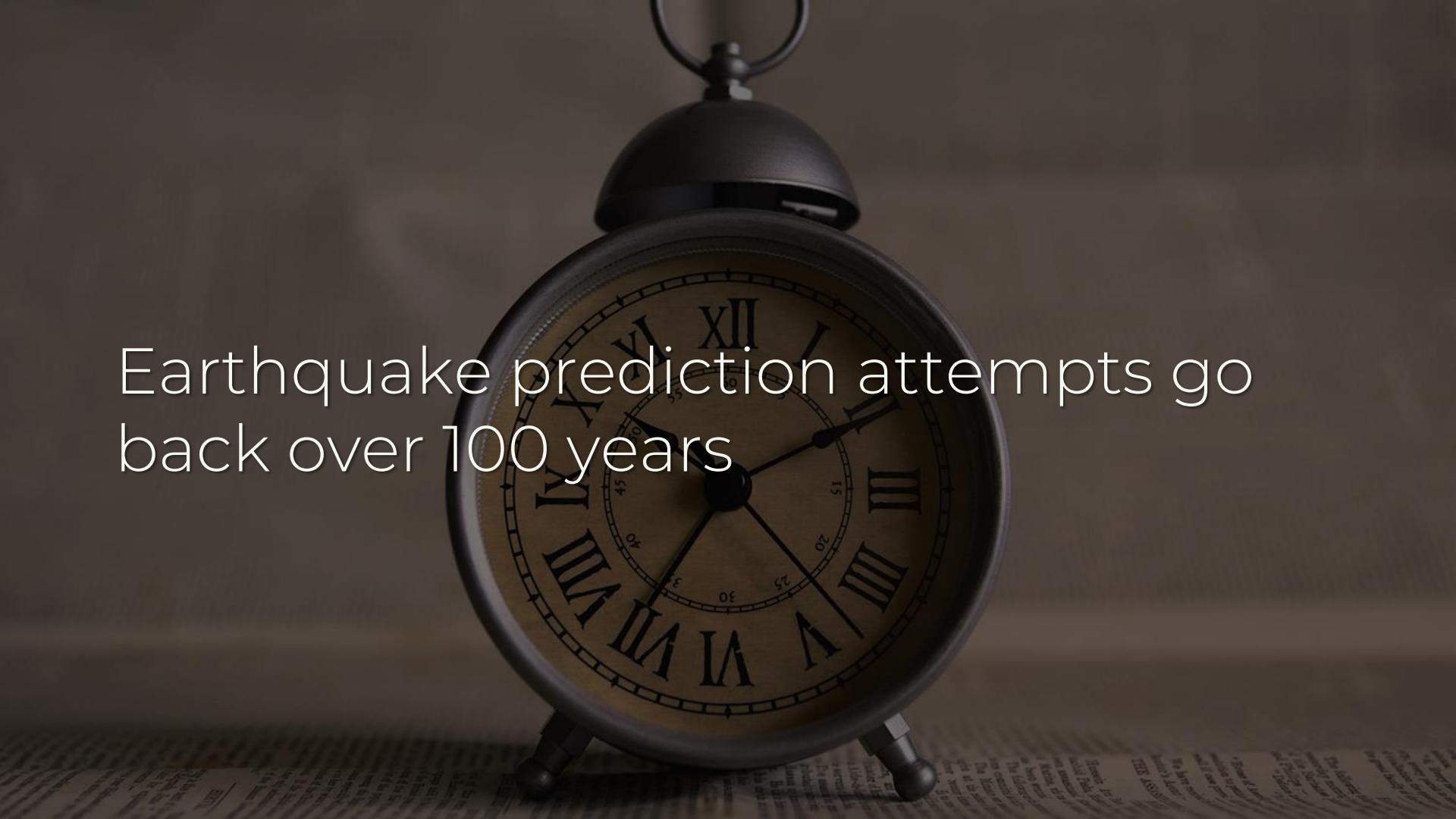
A dark, moody photograph showing a large amount of lava flowing from a volcano into the ocean. The lava is bright orange and red, contrasting sharply with the dark water and the dark, heavy clouds in the sky. The scene is lit from above, creating a somber and powerful atmosphere.

What are the lessons from
other domains?

The background is a dark, moody photograph. A thick metal chain runs horizontally across the middle of the frame. In the lower right foreground, there is a stack of papers or files. The top file in the stack has the word "CONFIDENTIAL" printed on it in capital letters. The overall lighting is low, with dramatic highlights on the chain and the edges of the papers.

Infosec is a complex system – non-linear activity in the aggregate

Prediction of natural disasters =
knowing time, location, and severity

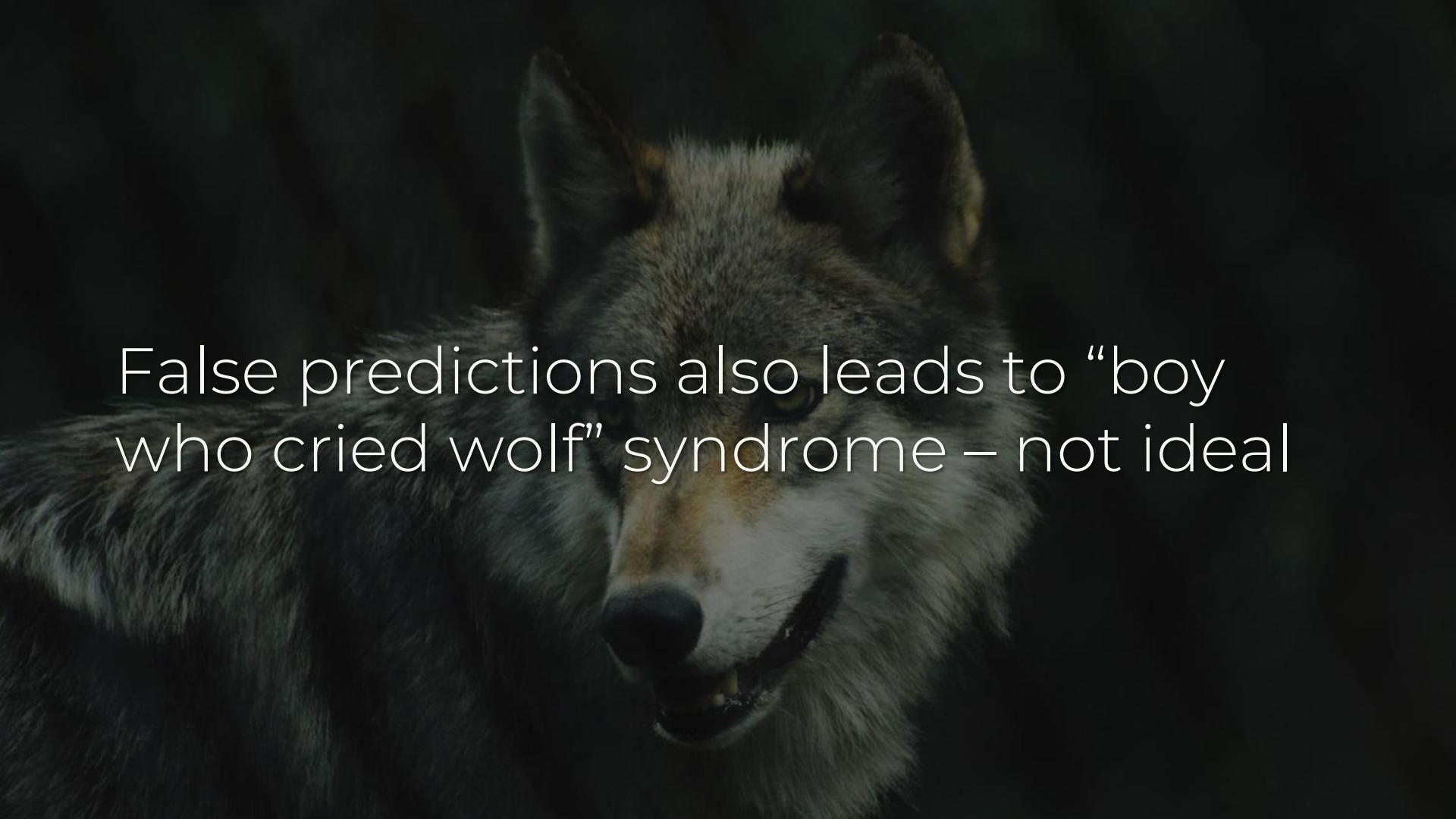
A close-up photograph of a vintage-style alarm clock. The clock has a dark metal case and a round face with Roman numerals for hours. The hands are black and thin. The clock is positioned in the center of the frame, slightly angled, and rests on a newspaper with visible text and columns.

Earthquake prediction attempts go
back over 100 years

1970s: success within the next 10 years

2000s: prediction is (probably) impossible – or at least far off

We still can't predict earthquakes,
despite tons of funding



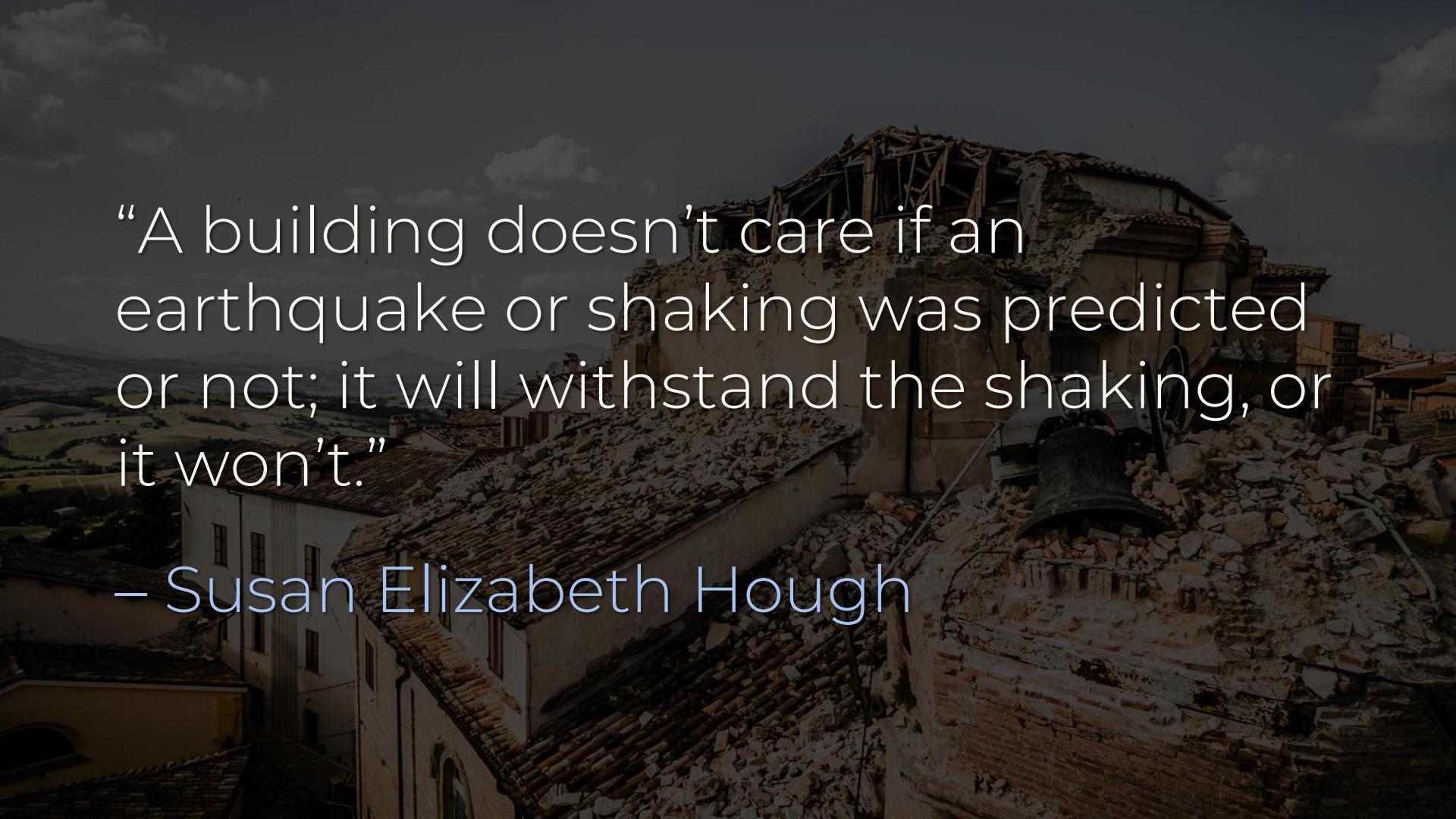
False predictions also leads to “boy who cried wolf” syndrome – not ideal

Earthquake **forecasting** vs.
earthquake **prediction**

We know which areas are risky, but
not where & when a quake will occur

This is enough info to inform us that
we need to be prepared

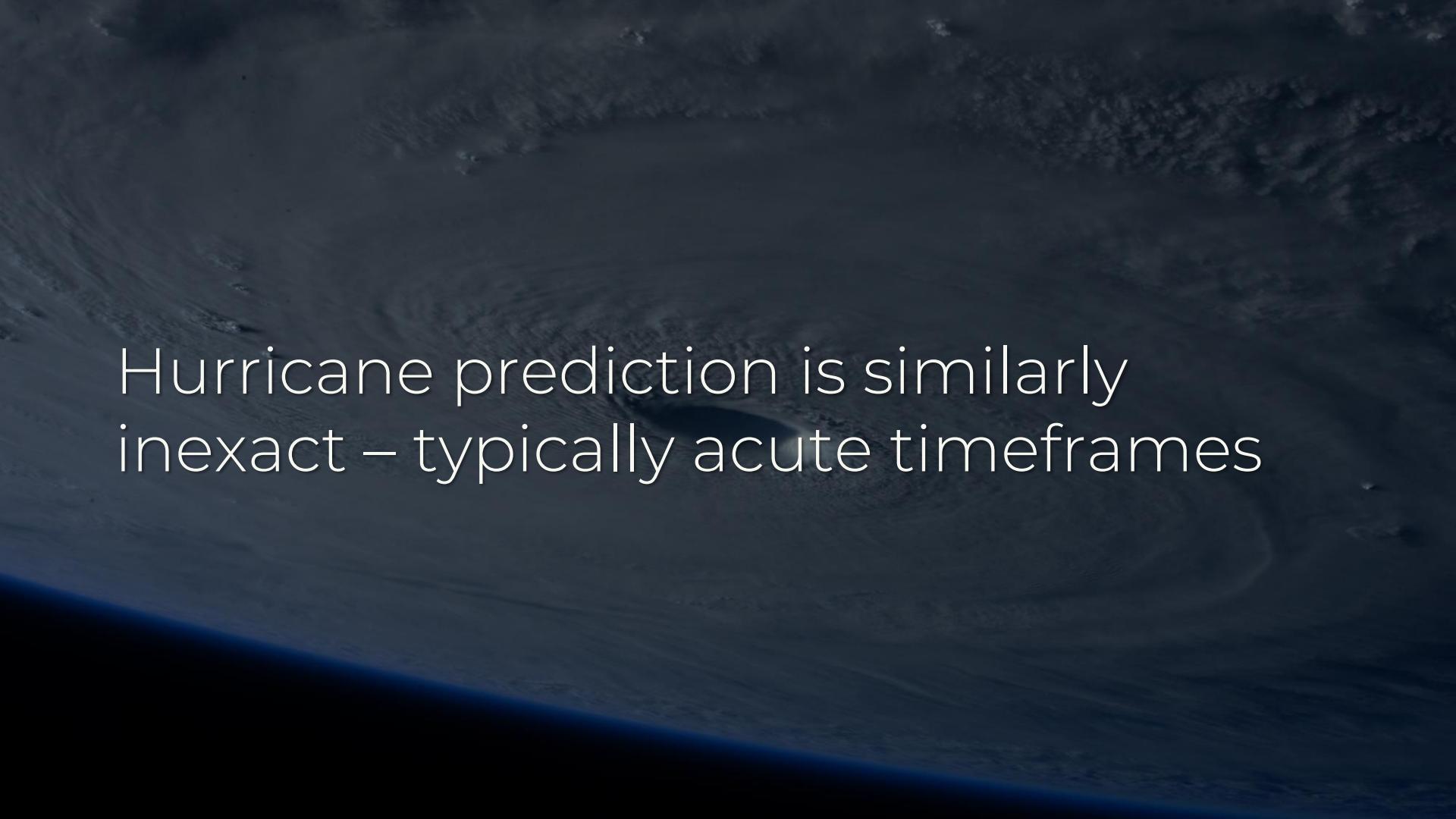
Building codes: withstand effects & incur acceptable level of damage

A dark, grainy photograph showing the aftermath of a disaster, likely an earthquake. In the foreground, a building's roof has completely collapsed, with large amounts of rubble and debris scattered across the ground. Other buildings in the background are partially visible, also showing signs of significant damage. The overall atmosphere is somber and desolate.

“A building doesn’t care if an earthquake or shaking was predicted or not; it will withstand the shaking, or it won’t.”

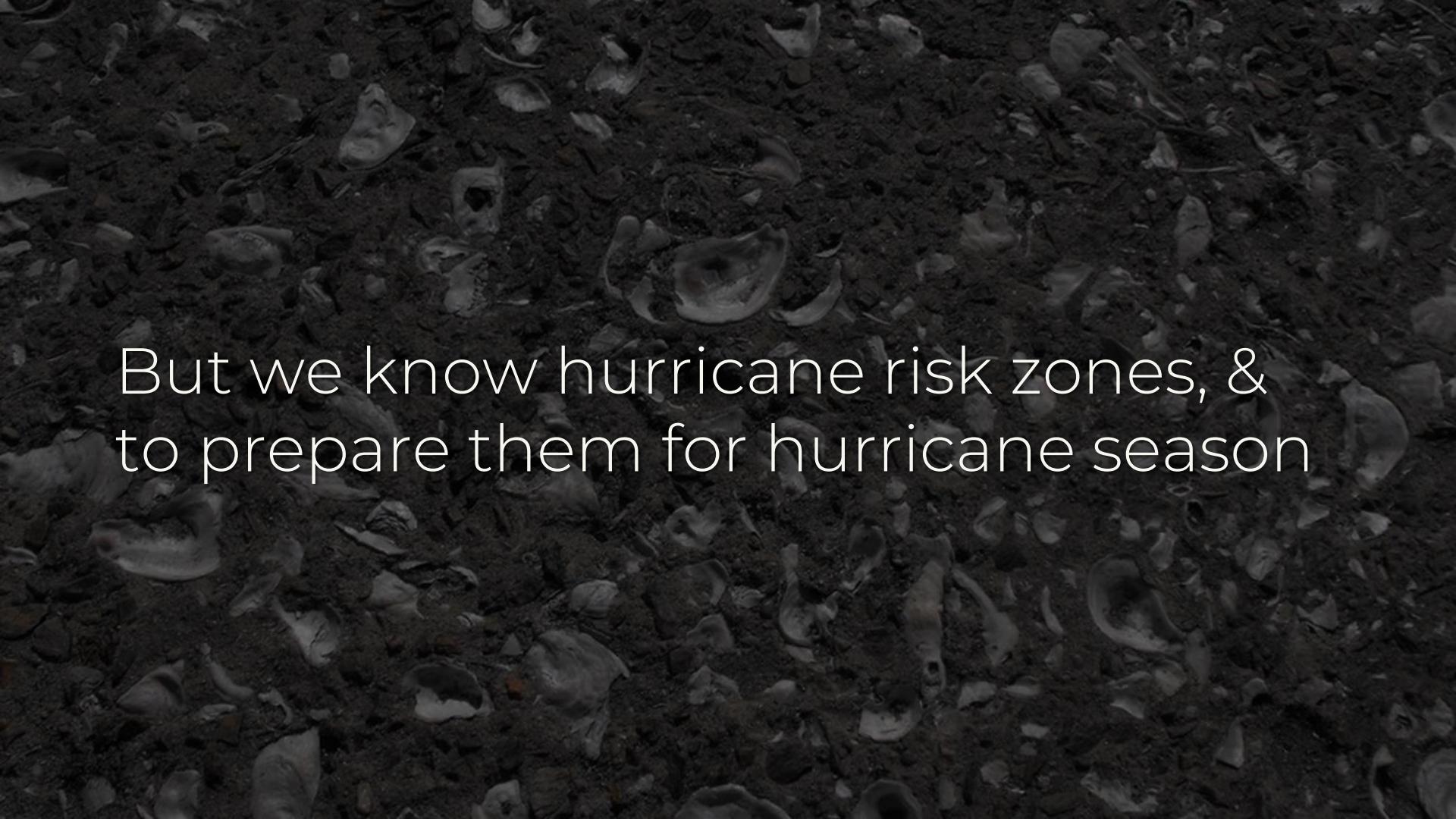
– Susan Elizabeth Hough

More valuable: reducing vulns, risk assessment, understanding impacts



Hurricane prediction is similarly
inexact – typically acute timeframes

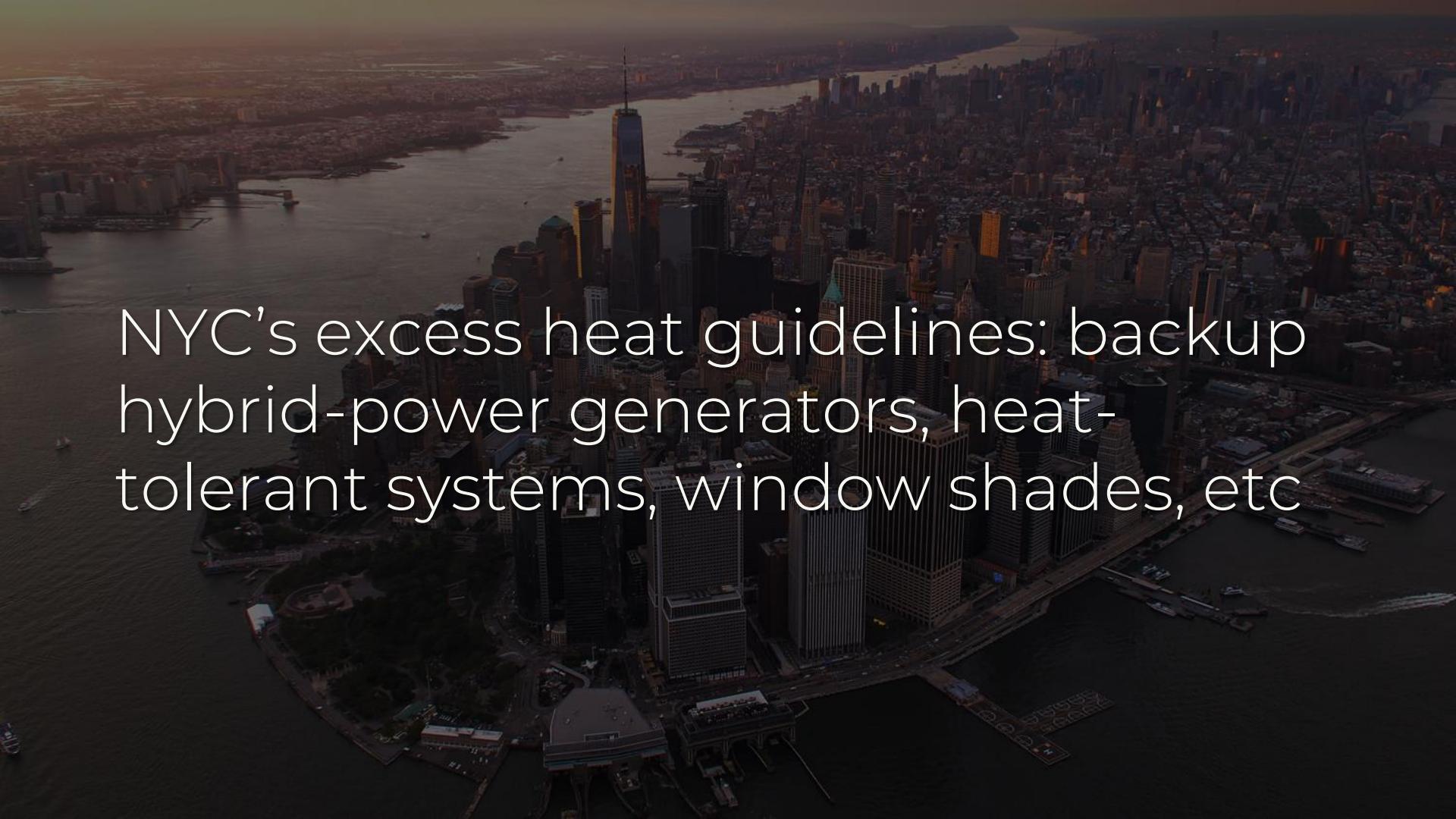
e.g. Hurricane Irma's exact course was incorrectly predicted only days before

The background of the slide is a dark, textured surface covered in numerous crushed oyster shells. The shells are irregularly shaped and vary in size, creating a mottled, earthy texture. The lighting is low, emphasizing the organic shapes of the broken shells.

But we know hurricane risk zones, &
to prepare them for hurricane season

Climate change: we don't know the exact time & sequence of events

But, we know enough to begin
preparing for the most likely risks

An aerial photograph of the New York City skyline at sunset. The Hudson River runs through the center, with the One World Trade Center (Freedom Tower) standing prominently on the West Side. The Manhattan Bridge is visible on the left, and the Brooklyn Bridge is on the right. The city lights begin to glow against the darkening sky.

NYC's excess heat guidelines: backup
hybrid-power generators, heat-
tolerant systems, window shades, etc



Financial crisis: ignoring systemic risk
leads to cascading failures

Must consider common attributes
that could undergo a collective shock

New Q: what is the minimum level of prediction to justify preparedness?

A close-up photograph of a roll of yellow hazard warning tape. The tape features a repeating pattern of red diagonal stripes. In the center, the word "PELIGRO" is printed in large, bold, red capital letters. The background is dark, making the yellow tape stand out.

IMO: exact prediction is largely irrelevant – focus on hazard reduction

A close-up photograph of a lit incandescent lightbulb against a dark, neutral background. The bulb is oriented diagonally, with its glass housing and metal base visible. The filament is glowing brightly, casting a warm, orange-red light that illuminates the surrounding area of the bulb.

What should we be doing
instead?

Given finite resources, it's better to research hazard assessment & reduction vs. attack prediction

WWWH&W for one attack is less valuable than knowing most probable scenario & prepping for max impact

An analogy based on a true story, via
Alvaro Videla (@old_sound):

Uruguay had a brand new, fancy
radar & detected their airspace was
being used for drug smuggling

...but they can't do anything because
they don't have planes fast enough to
catch the bad guys

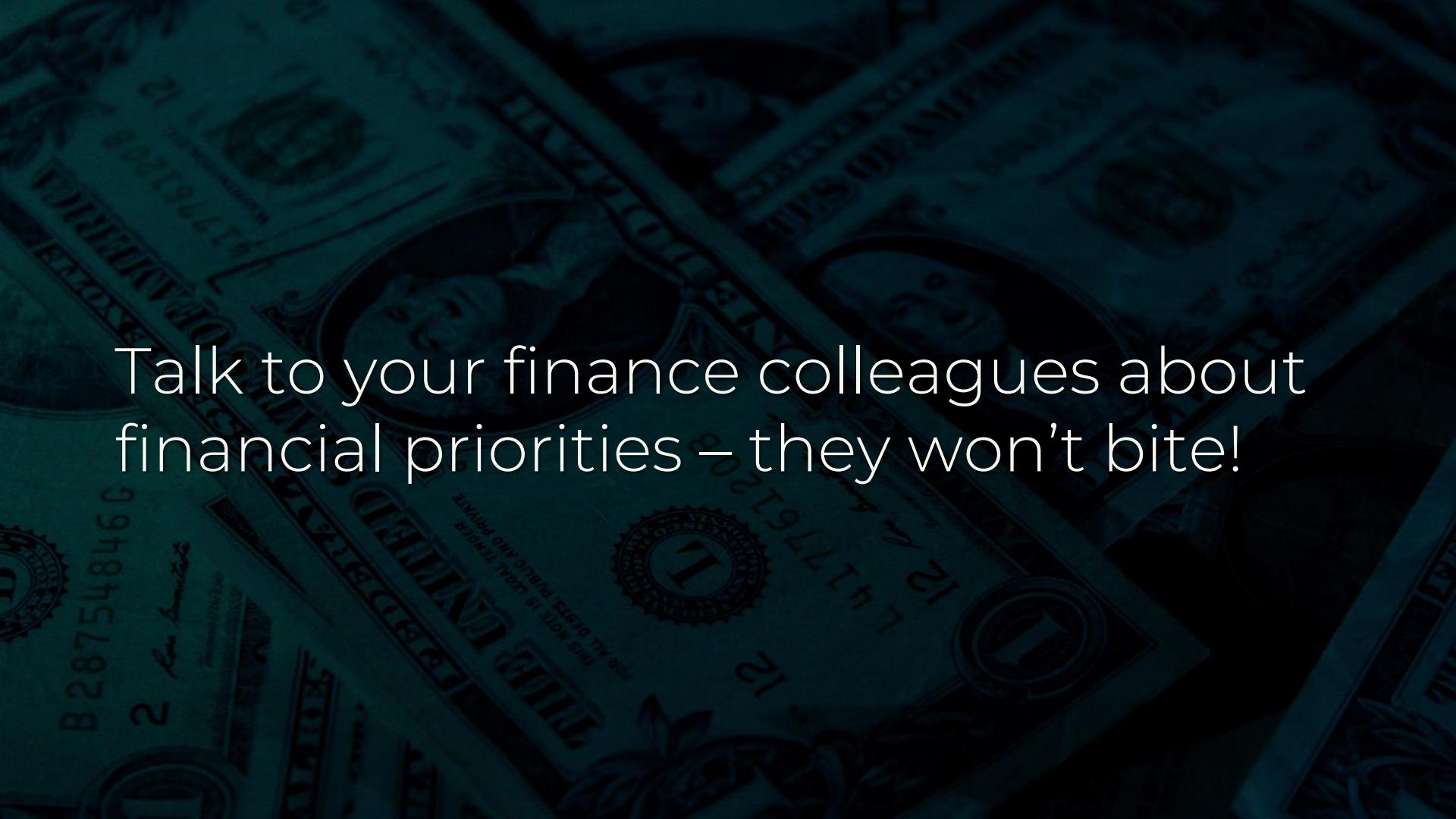
You can predict something, so what?
Can you do anything about it?

Conduct attack **forecasting** to determine general, probabilistic risk



Minimize potential impact based on business context, not security context

Step 1: Which threats actually impact business performance?

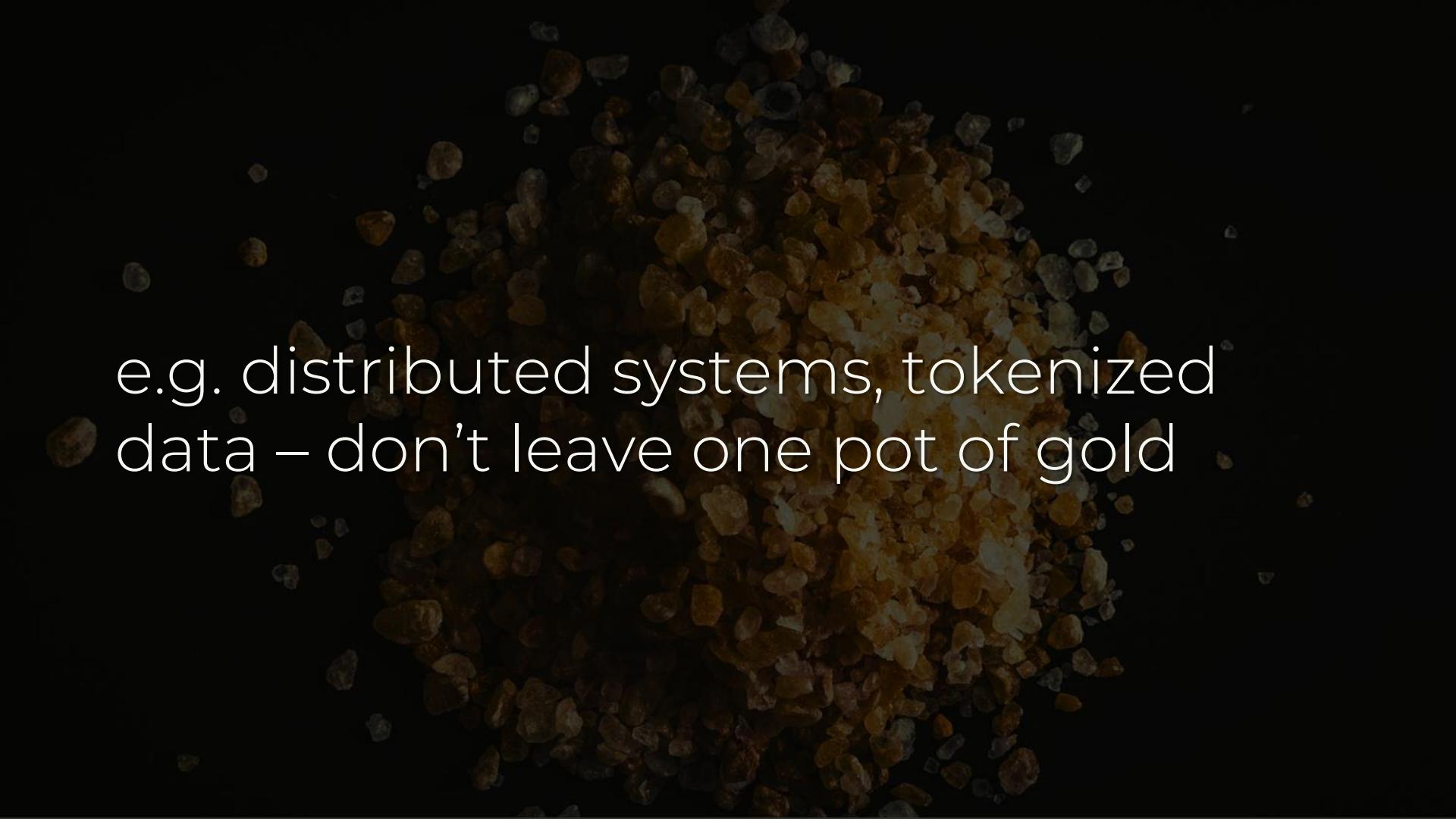


Talk to your finance colleagues about financial priorities – they won't bite!

Anything that doesn't disrupt revenue
directly or erode "differentiation"
probably doesn't matter

e.g. Equifax – revenue isn't actually down, but uncertainty around fines is keeping its stock price depressed

Step 2: Assume they'll actually happen
– how can you reduce the impact?

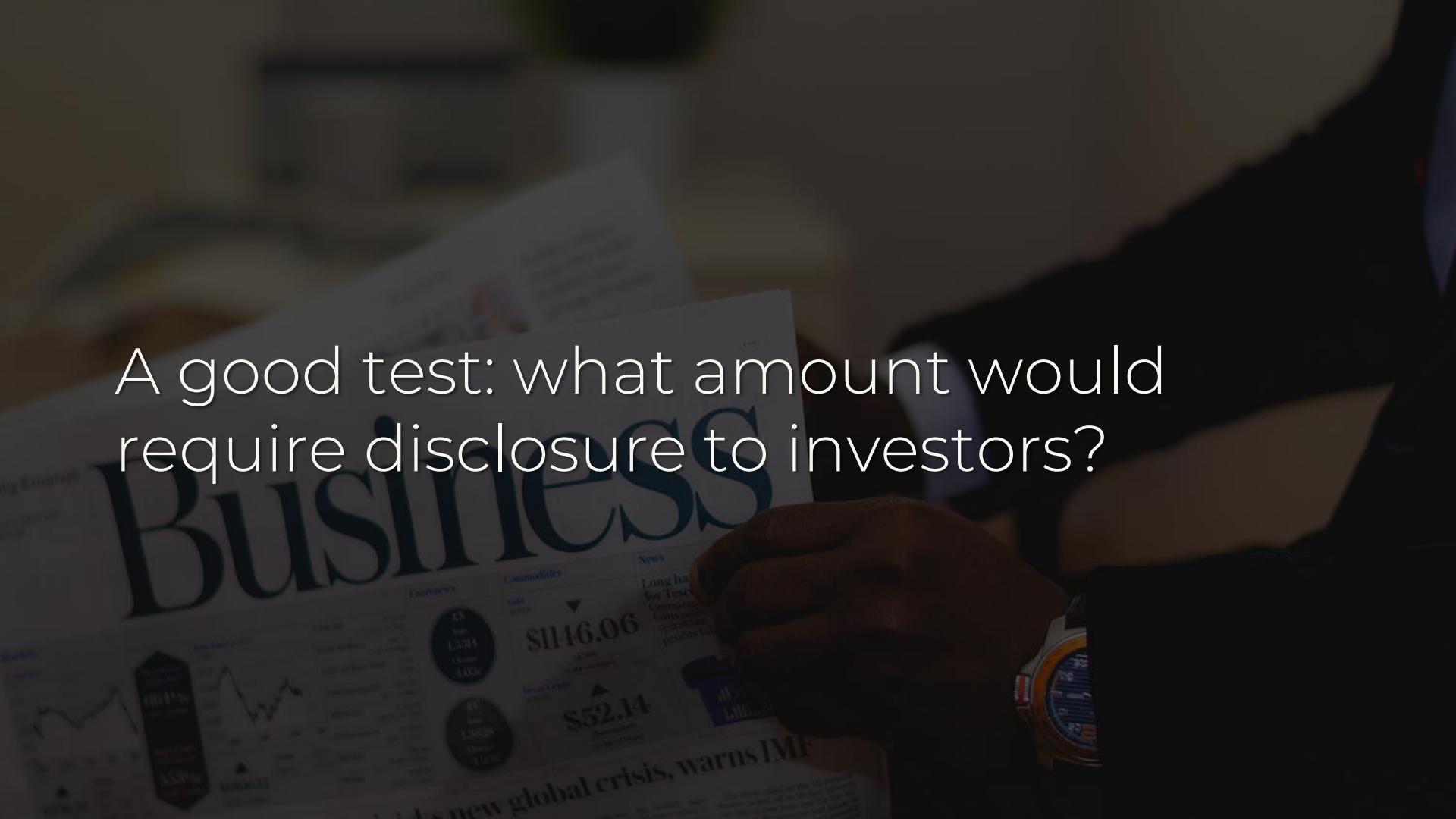


e.g. distributed systems, tokenized
data – don't leave one pot of gold

Step 3: What is an acceptable level of impact your org can tolerate?

What is material to your org? e.g. 10 mins of downtime? 60? 1440?

A good test: what amount would require disclosure to investors?



Exercise: How do impacts translate in \$ terms? (fines, IR costs, lost revenue)



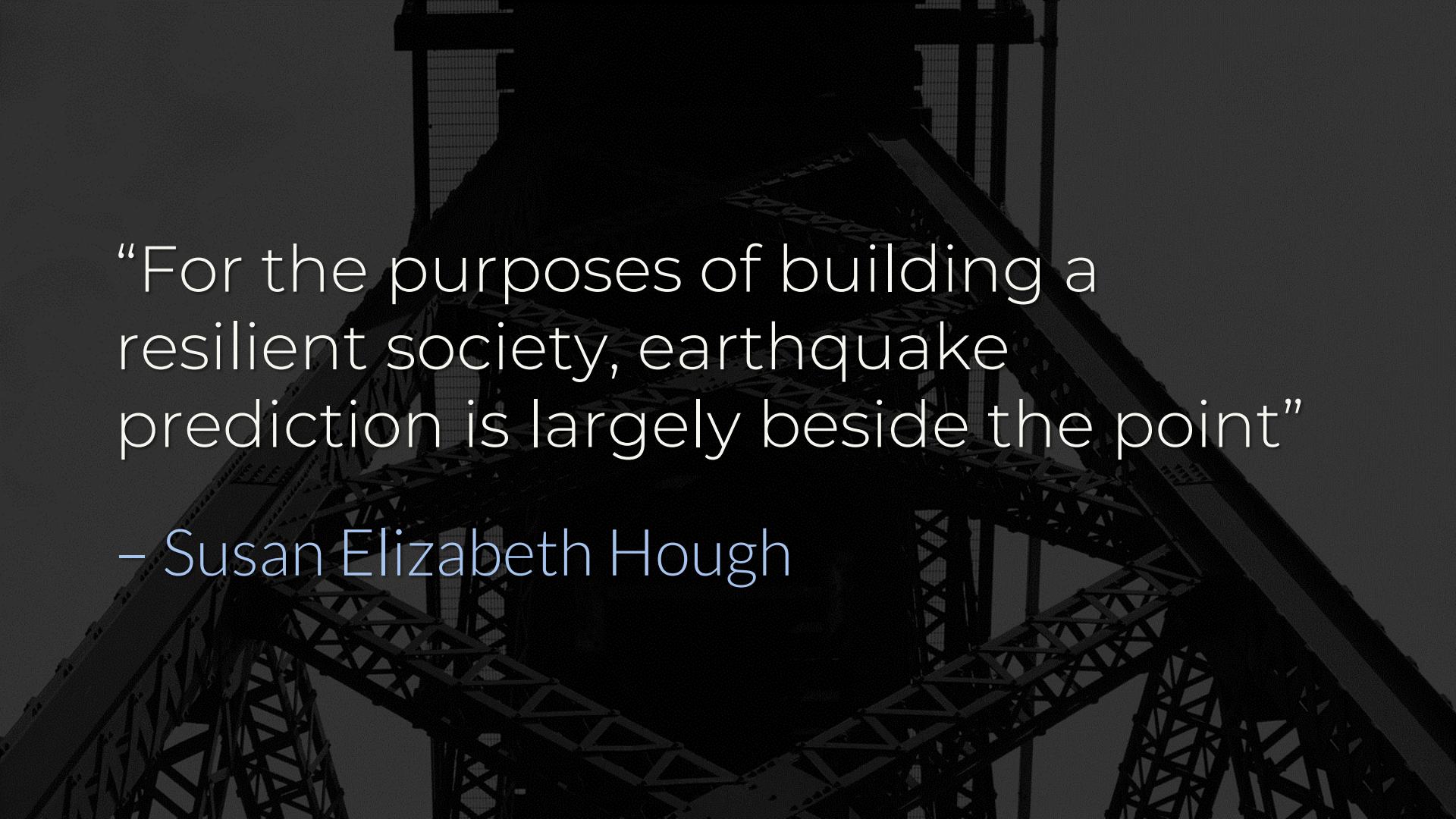
You can't protect everything – accept
some things just aren't as important

Security teams can burn out others & themselves with “everything = critical”

e.g. Critical infrastructure: customer \$
data is less important than uptime

“Resilience in infosec is a flexible system that can absorb an attack and reorganize around the threat”

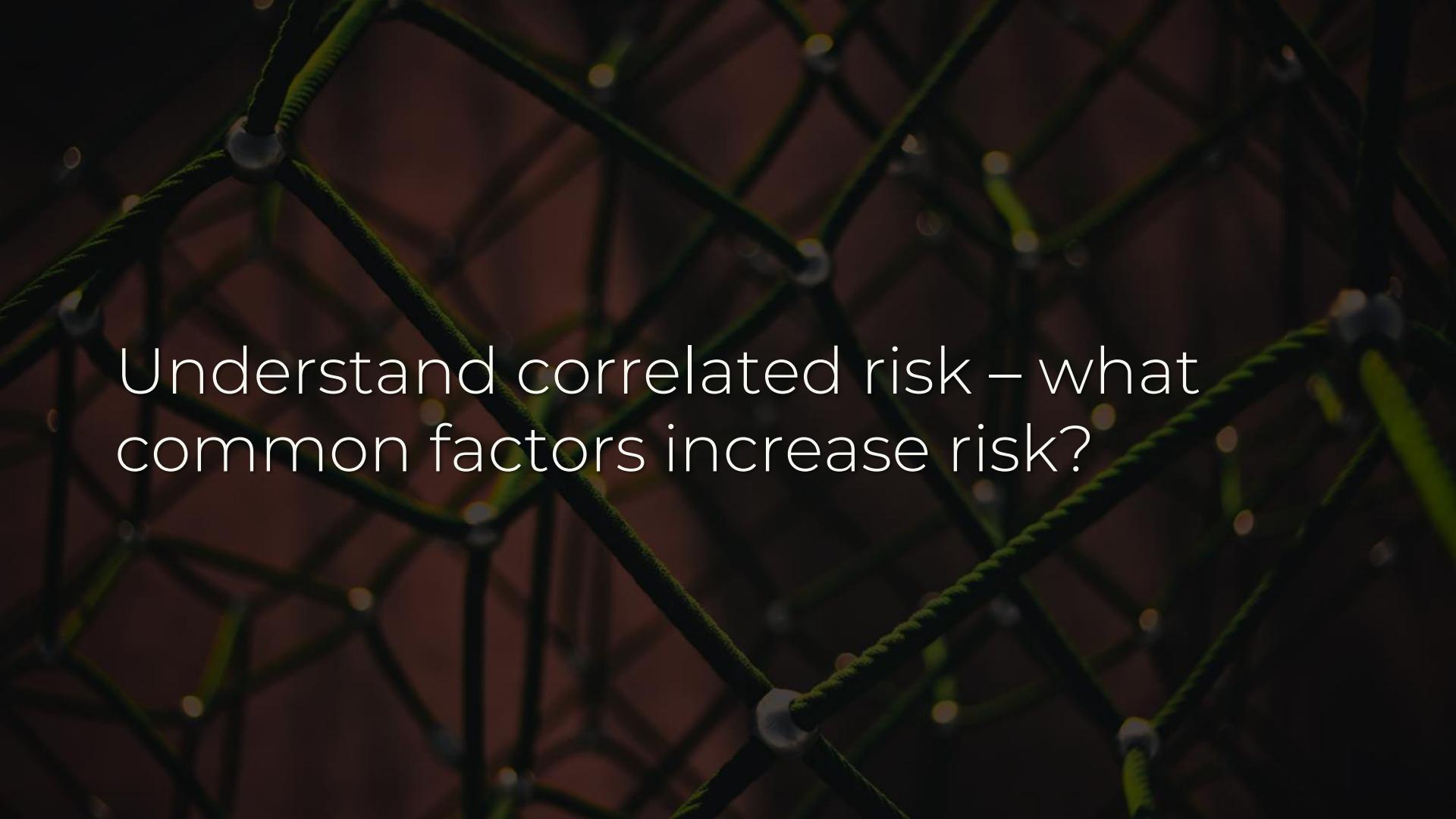
– my attempt at a definition



“For the purposes of building a resilient society, earthquake prediction is largely beside the point”

- Susan Elizabeth Hough

Resilience “radically accepts” an outcome & aims to reduce the hazard

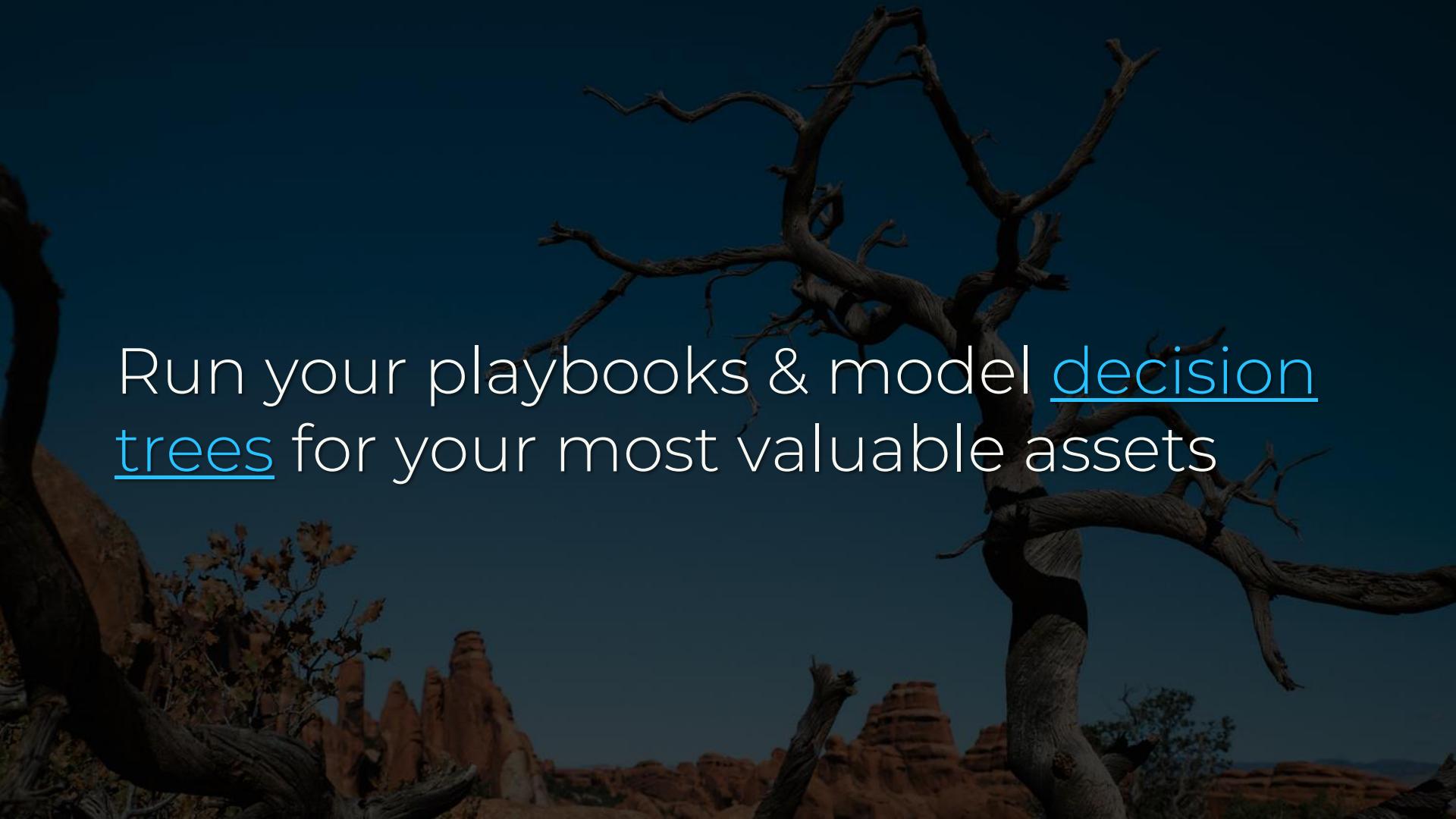


Understand correlated risk – what common factors increase risk?

Design (biz critical) systems with the assumption of compromise in mind

e.g. NZ designated a “red zone” where land is too vulnerable & where rebuilding is uneconomic post-quake

Identify the red zones within your IT systems (read [this talk](#) for more)

The background of the slide is a dark, moody photograph of a desert landscape. In the foreground, a large, ancient-looking tree with many bare, twisted branches stands prominently. Behind it, several tall, thin rock formations rise against a dark sky, creating a sense of depth and ruggedness.

Run your playbooks & model decision trees for your most valuable assets

No point predicting if you haven't
practiced how to defend against it

Conclusion



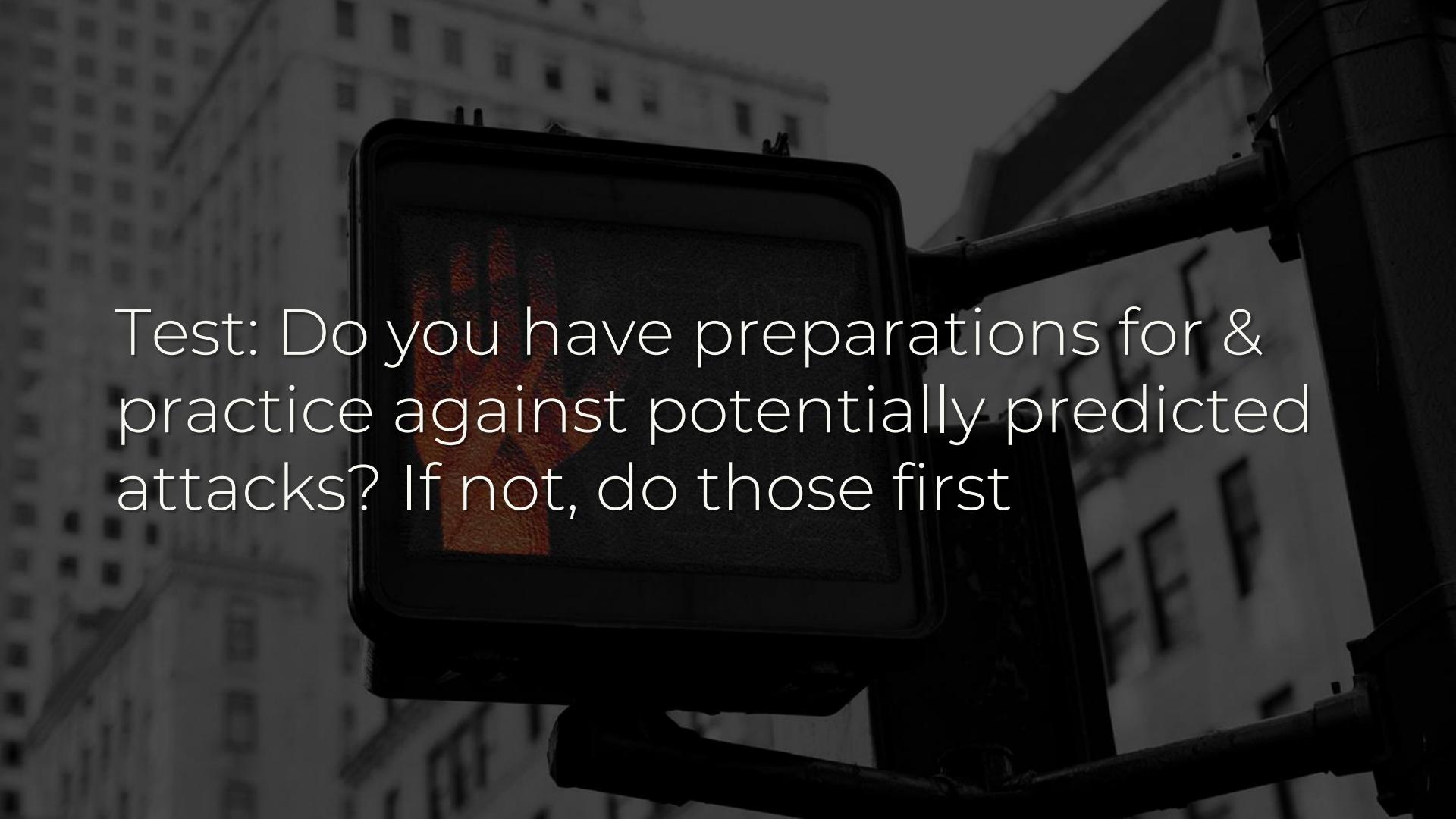
The background of the slide is a dark, moody photograph of a forest floor. In the center, a deer skull with prominent antlers is suspended by a cord. Several large pumpkins of different sizes are scattered around, some with their tops removed and lit from within by tall, thin candles. Smaller, shorter candles are also scattered across the ground. Twigs and branches are visible throughout the scene, creating a sense of a natural, undisturbed environment.

Predicting who, when, where, how,
why about an attack is unrealistic

Prediction about an individual attack
is not that useful (on a relative basis)

Many “attack prediction” methods are
really about detection & too myopic

Requires an inherently reactive approach – even more “things to do”



Test: Do you have preparations for & practice against potentially predicted attacks? If not, do those first

Assume pwnage & architect robust,
adaptable, & transformable systems

Resilient systems support the business against many eventualities

“Hoping for the best, prepared for the worst, and unsurprised by anything in between.”

– Maya Angelou



@swagitda_



/in/kellyshortridge



kelly@greywire.net