

A hand is shown using a power tool to cut through a red and white striped barrier. The barrier is being cut into, and there are flames at the bottom of the image. The background is dark and blurry.

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

Kelly Shortridge (@swagitda\_)

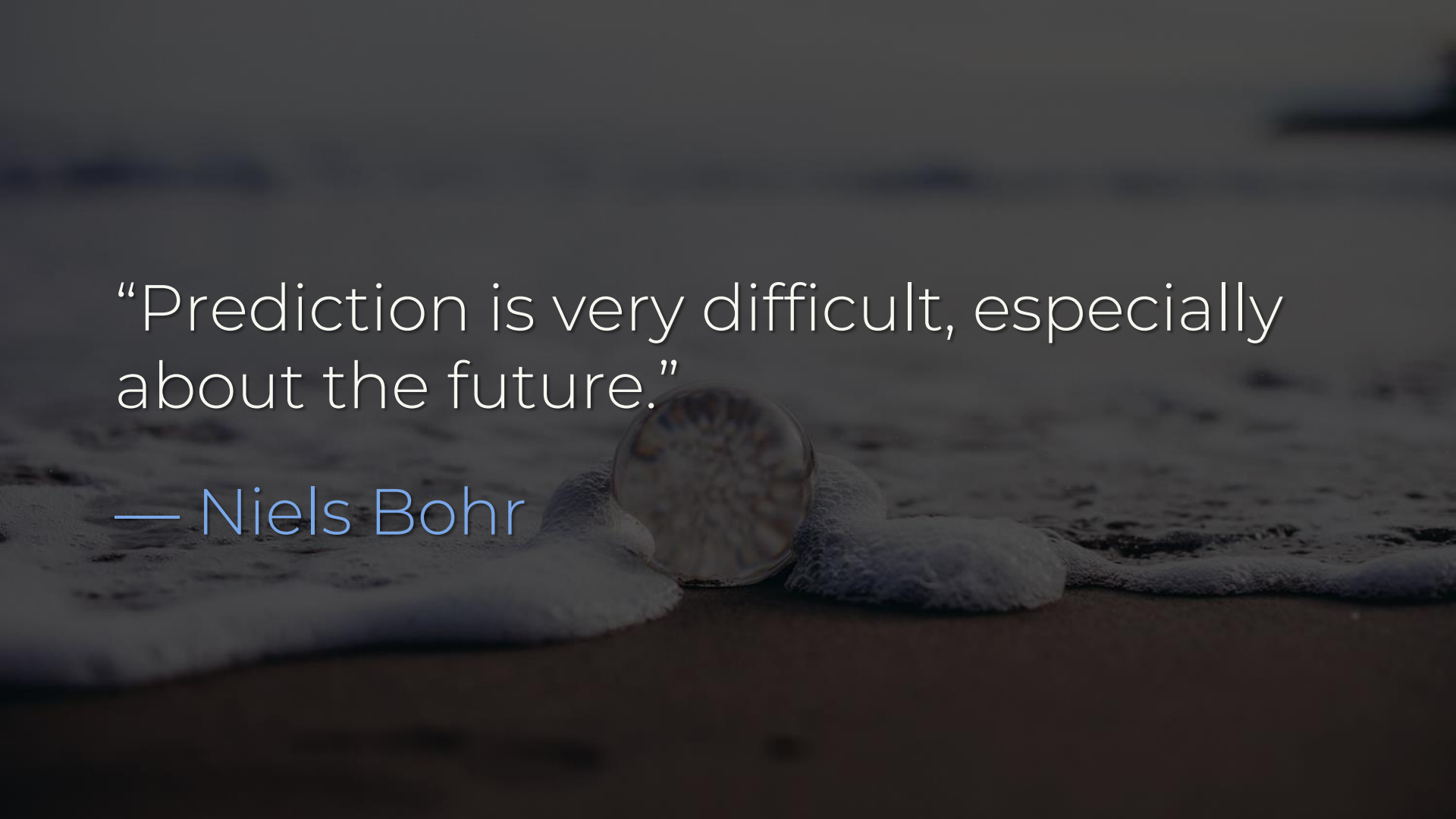
Art into Science 2018



Hi, I'm Kelly



SecurityScorecard

A magnifying glass is placed on a sandy beach, with its handle resting on the sand and its lens reflecting the surrounding environment. In the background, gentle waves are washing onto the shore, creating a soft, white foam. The overall scene is dimly lit, giving it a contemplative and serene atmosphere.

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

— Niels Bohr



Problem: prediction is a sexy problem

A night cityscape with illuminated skyscrapers reflected in water. The scene is dark, with the city lights providing the primary illumination. The buildings are of various heights and architectural styles, some with distinctive features like a pointed top or a blue-lit facade. The water in the foreground is dark, with the lights from the buildings creating a shimmering, blurred reflection. The overall mood is serene and modern.

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





Act 1

Why the interest in attack prediction?



Fundamentally, uncertainty feels bad



Ambiguity of potential future threats  
fuels stress & anxiety

Predictable negative events are less stressful than uncertainty

A dark, atmospheric photograph of a nest made of sticks with two large, pale hands resting on it, set against a background of a body of water and a 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 photograph of a person's face and shoulder, illuminated by a dark blue light. The skin is covered in numerous small, glowing particles, primarily in shades of blue and green, creating a starry or bioluminescent effect. The person's eyes are closed, and their expression is serene. The background is completely black, making the glowing particles stand out prominently.

Tacit reason: precogs are cool

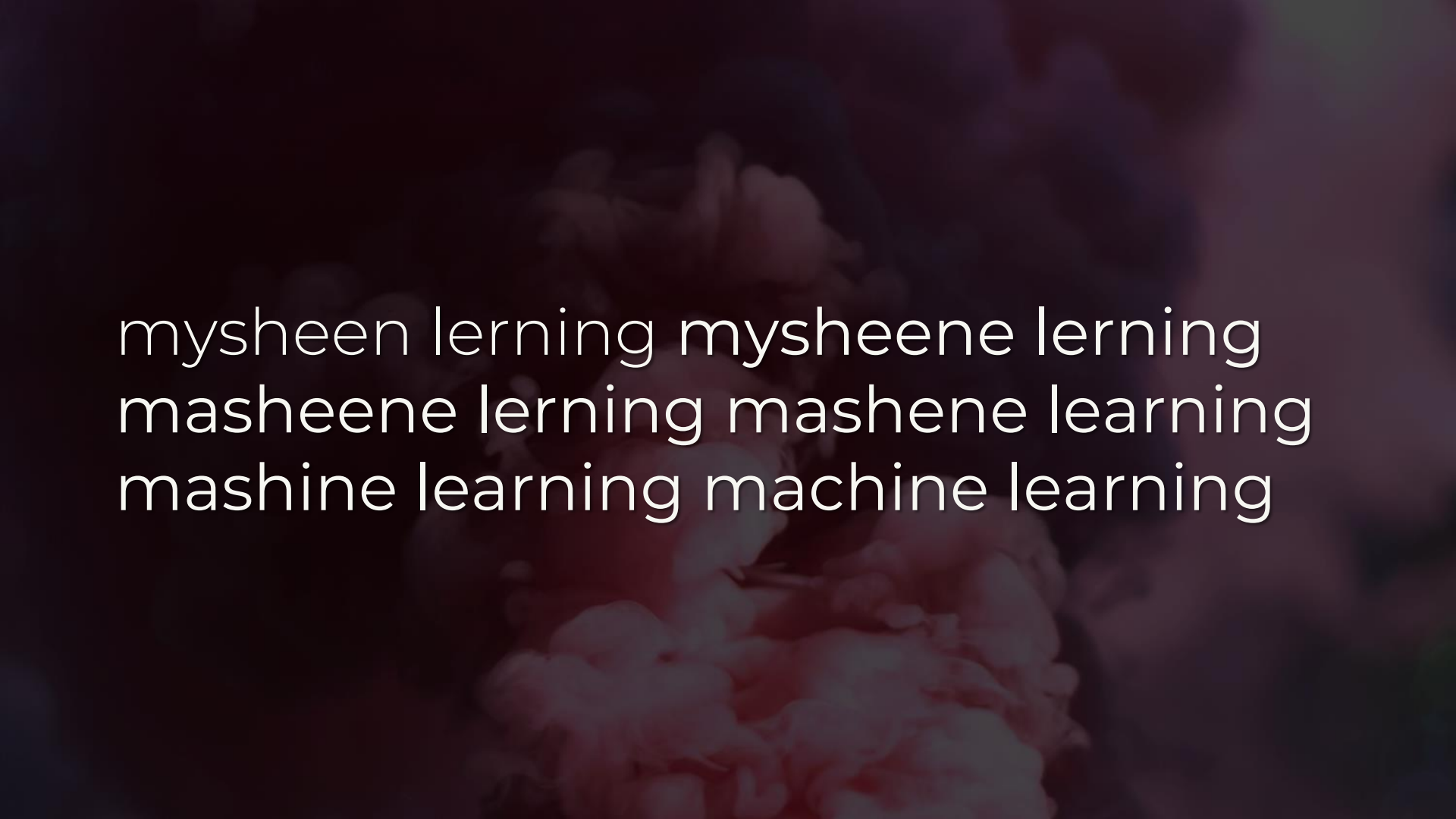
But do the goals align with the methods actually being proposed?

A hand-drawn map on a textured surface, possibly a piece of bark or parchment. The map features several dashed lines forming paths or boundaries. There are various symbols: a red 'X' at the top, a red star-like symbol in the center, and several 'A' characters. The background is dark and textured.

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  
maschine learning machine learning



Common idea: unsupervised machine learning to avoid false negatives

A close-up photograph of a hand holding a glowing dandelion seed head. The background is dark, and the light from the seed head creates a soft, ethereal glow. The text is overlaid on the image in a clean, white, sans-serif font.

AI – i.e. a magic black box of math

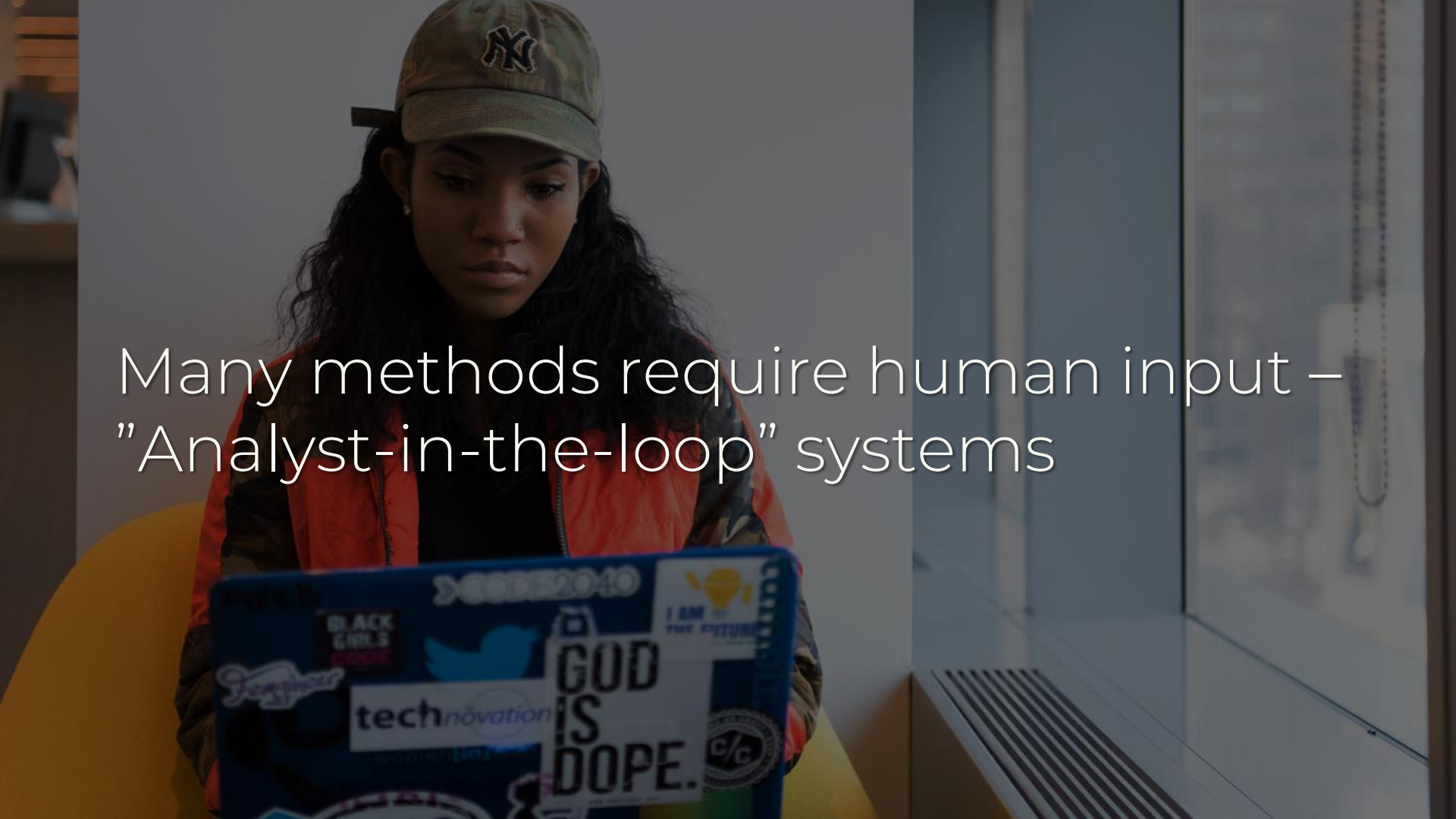
Deep learning threat prediction using  
actionable behavioral analytics...



“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



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

AI<sup>2</sup> : 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

A photograph of a sandy beach with several footprints scattered across the surface. The footprints are of varying sizes and orientations, suggesting multiple people or animals. The sand is a warm, golden-brown color, and the lighting is soft, creating gentle shadows. The text is overlaid in the center of the image.

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

A wire mesh basket filled with newspapers. The basket is positioned in the foreground, and several newspapers are visible inside. One newspaper prominently displays the title 'The Wall Street Journal'. Other visible headlines include 'Puzder Withdraws As Labor News' and 'From Trump'. The background is dark and out of focus.

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 small bird, likely a finch or sparrow, perched on a dark, textured branch. The bird has bright yellow plumage on its chest and belly, with grey and black streaks on its wings and back. It has a small, dark beak and is looking to the right. A small, cylindrical, silver-colored device is attached to its left leg. The background is a solid, dark blue-grey color.

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



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

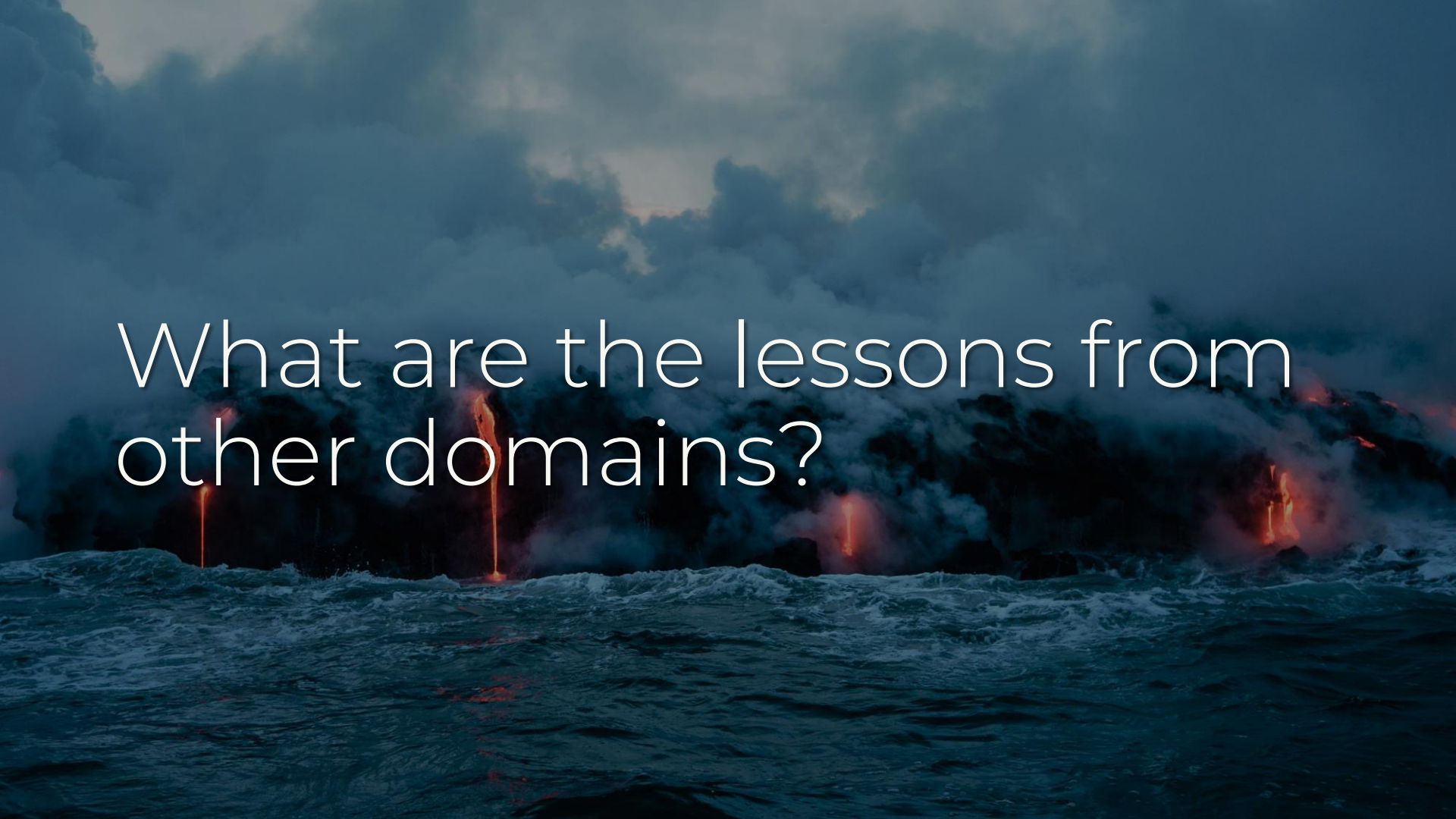
How do you know what to do next?  
Predictive vs. prescriptive

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





# Act 2



What are the lessons from  
other domains?

The background is a dark, monochromatic image with a complex, textured surface. It appears to be a close-up of a heavy metal door or a similar industrial structure. A prominent feature is a thick metal chain with several links, which is secured by a large, rectangular padlock. The padlock has the word "COMMERCIAL" embossed on its side. The lighting is dramatic, highlighting the metallic sheen and the intricate details of the chain and lock against the darker, shadowed background. The overall mood is one of strength, security, and complexity.

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

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

A vintage black alarm clock with a white face and Roman numerals, resting on a newspaper. The clock has two bells at the top and is positioned centrally in the frame. The background is a dark, textured surface, possibly a wall or a backdrop. The text is overlaid on the left side of the clock face.

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 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 image is a dense, dark field of oyster shells. The shells are scattered across the entire frame, creating a complex, textured pattern. The lighting is somewhat dim, highlighting the various shapes and sizes of the shells against a dark, almost black background. The overall tone is somber and naturalistic.

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 New York City at dusk, showing the dense skyline of Lower Manhattan. The Freedom Tower is prominent in the center. The Hudson River is visible on the left, and the East River on the right. The sky is a mix of orange and dark blue, indicating sunset. The city lights are beginning to glow.

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?



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



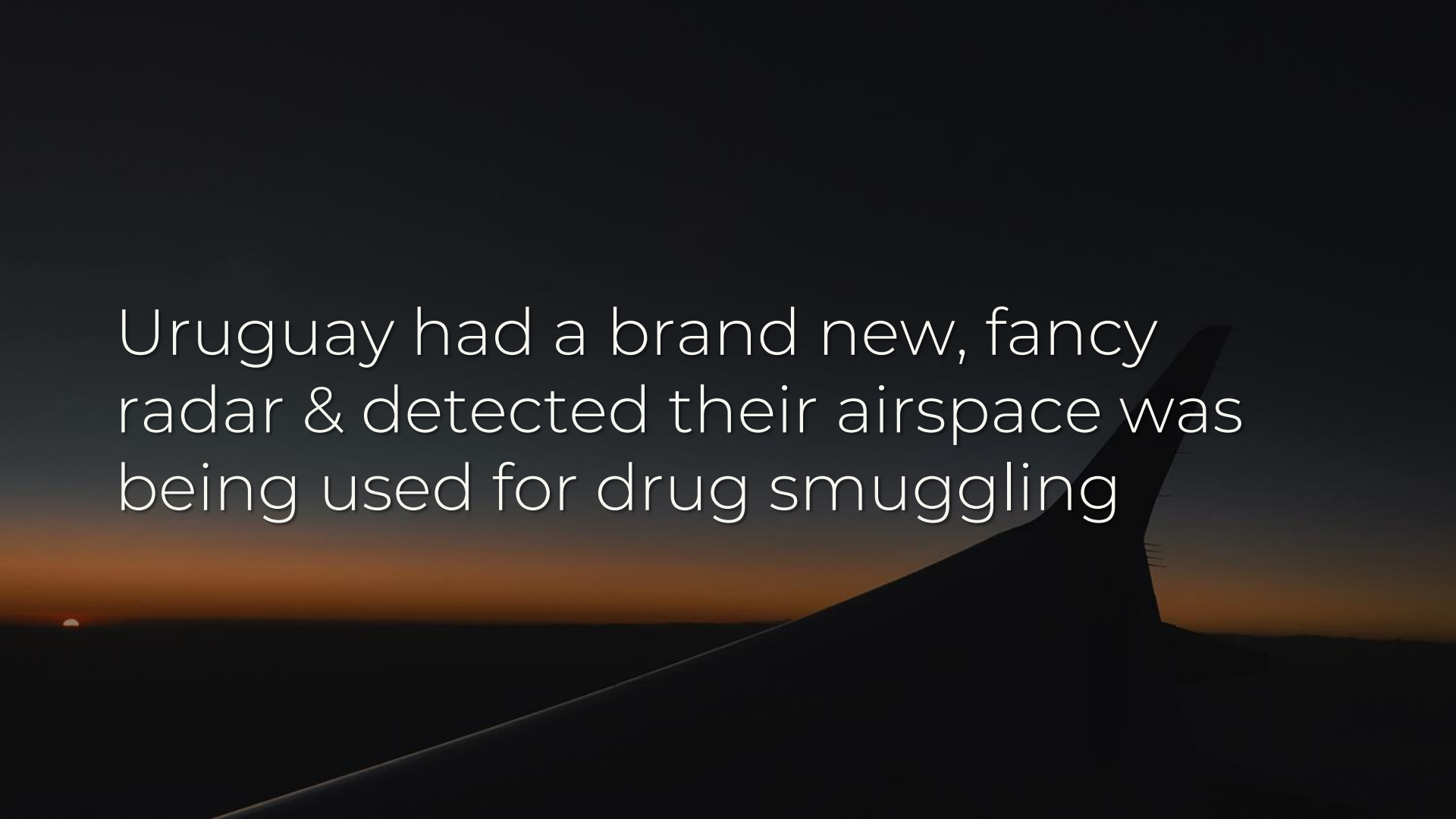
A glowing lightbulb is shown against a dark background. The bulb is lit, with a warm orange glow emanating from the filament. The text "What should we be doing instead?" is overlaid in white, sans-serif font across the middle of the bulb. The bulb is positioned diagonally, with the base at the bottom left and the top at the top right.

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):

A dark silhouette of an airplane's tail fin is visible on the right side of the image, set against a background of a sunset sky with a gradient from orange to dark blue. The text is overlaid on the left and center of the image.


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?

The background of the image is a dark, teal-tinted collage of US dollar bills. The bills are overlapping and slightly out of focus, creating a textured, financial backdrop. The text is centered over this background.

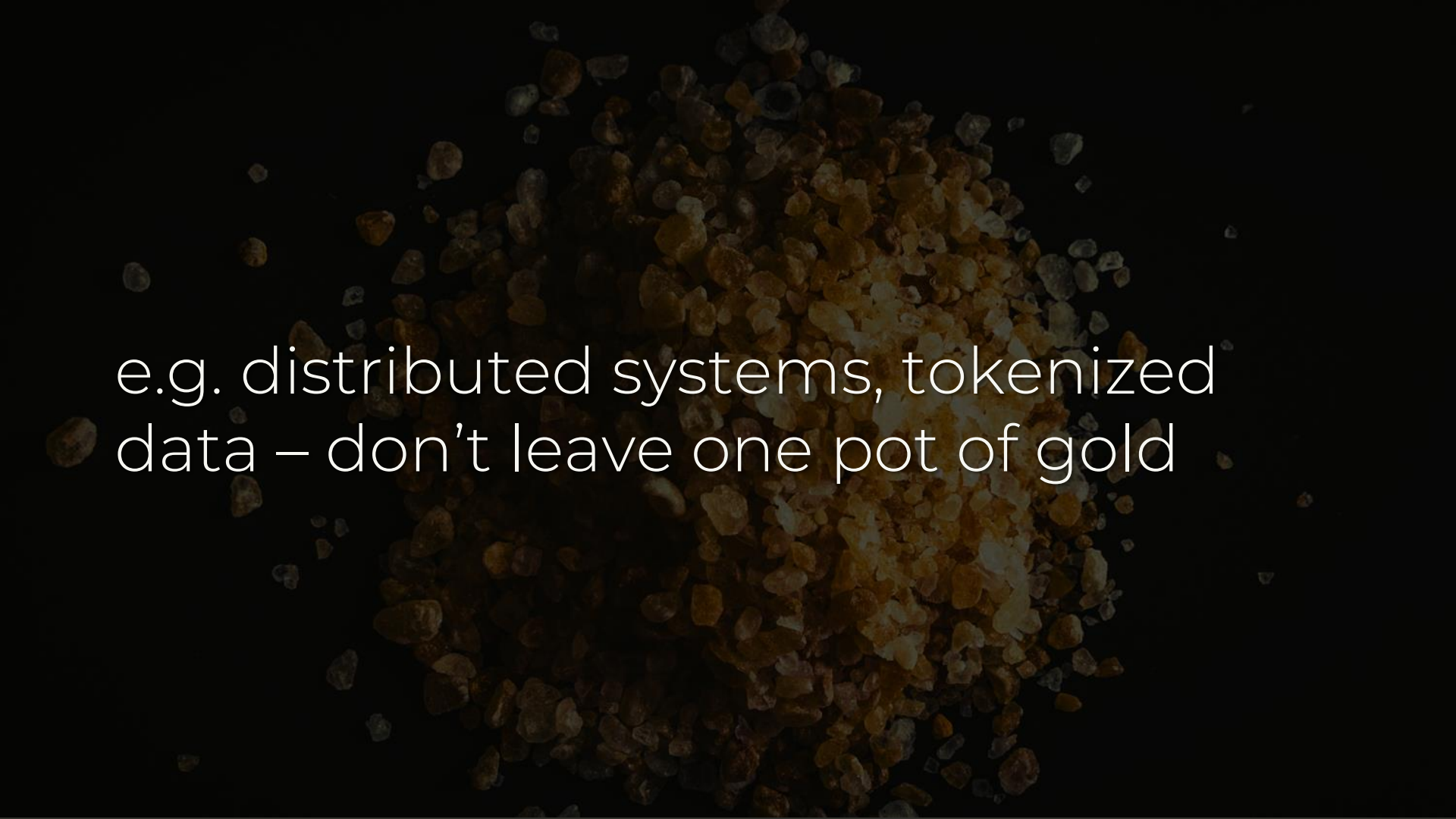
Talk to your finance colleagues about financial priorities – they won't bite!

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?



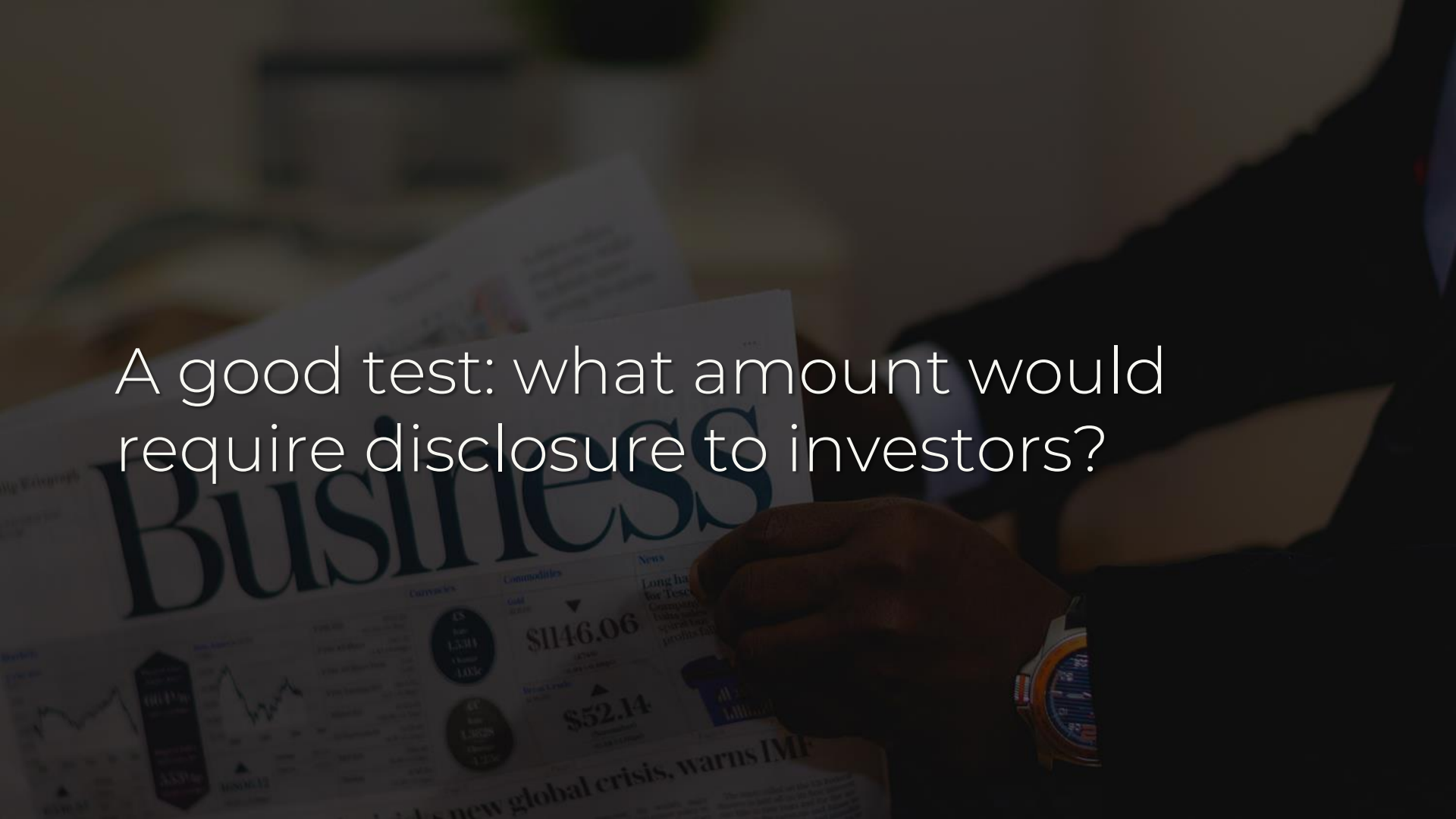
e.g. distributed systems, tokenized  
data – don't leave one pot of gold

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)

A black and white photograph of a person's hands held up, palms facing forward. The word "CARELESS" is written in dark ink across both palms. The person's face is visible in the background, looking directly at the camera. The overall mood is somber and reflective.

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

CARELESS

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)



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





A dark, atmospheric scene featuring a deer skull with antlers in the center, surrounded by pumpkins, lit candles, and twigs. The text is overlaid in the center.

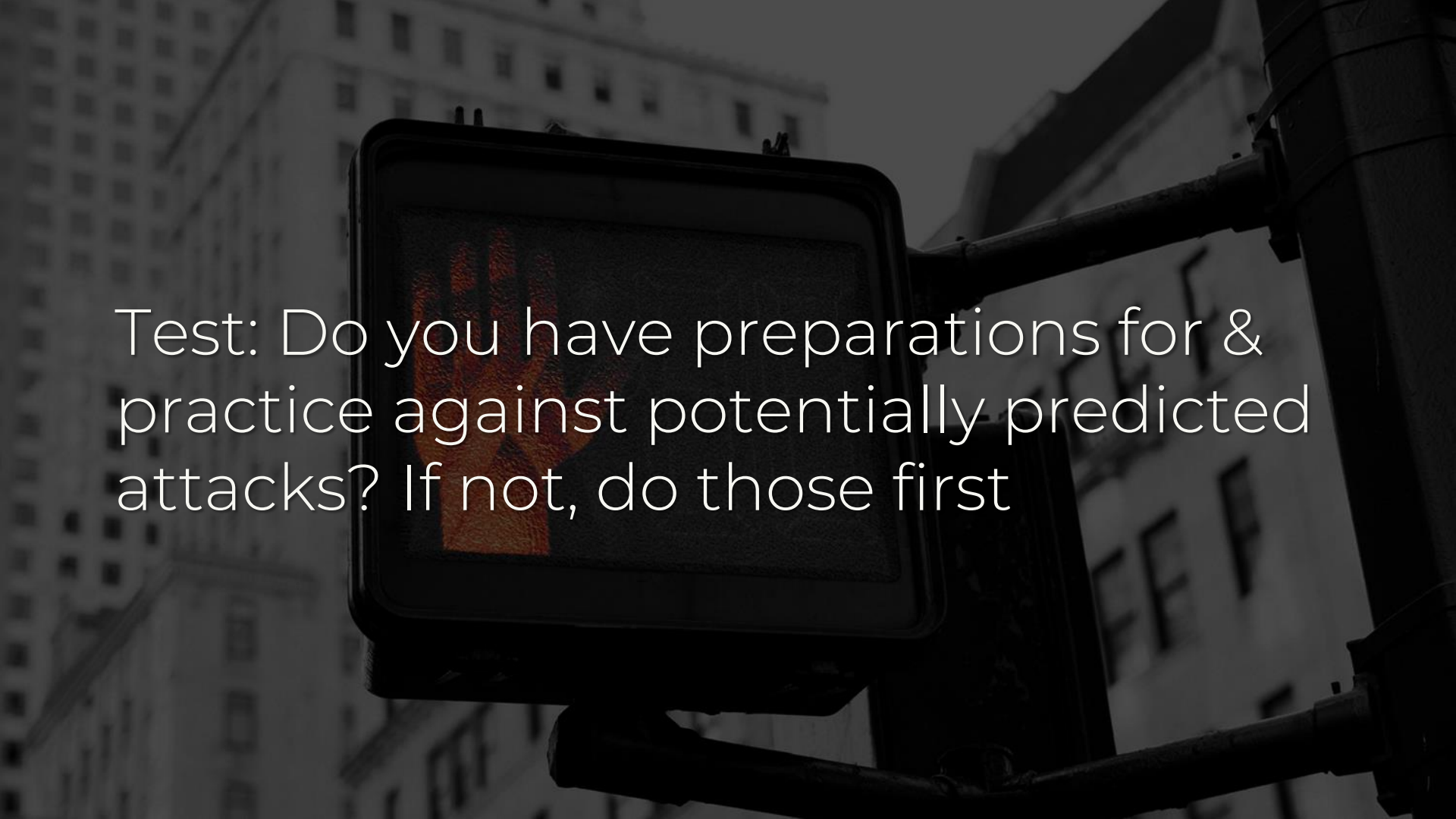
Predicting who, when, where, how,  
why about an attack is unrealistic

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”

A dark, low-angle photograph of a pedestrian crossing signal. The signal is a square box with a red hand icon in the center, mounted on a metal pole. The background is a blurred city street with buildings and a street sign that partially reads 'E F'. The overall tone is somber and urgent.

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