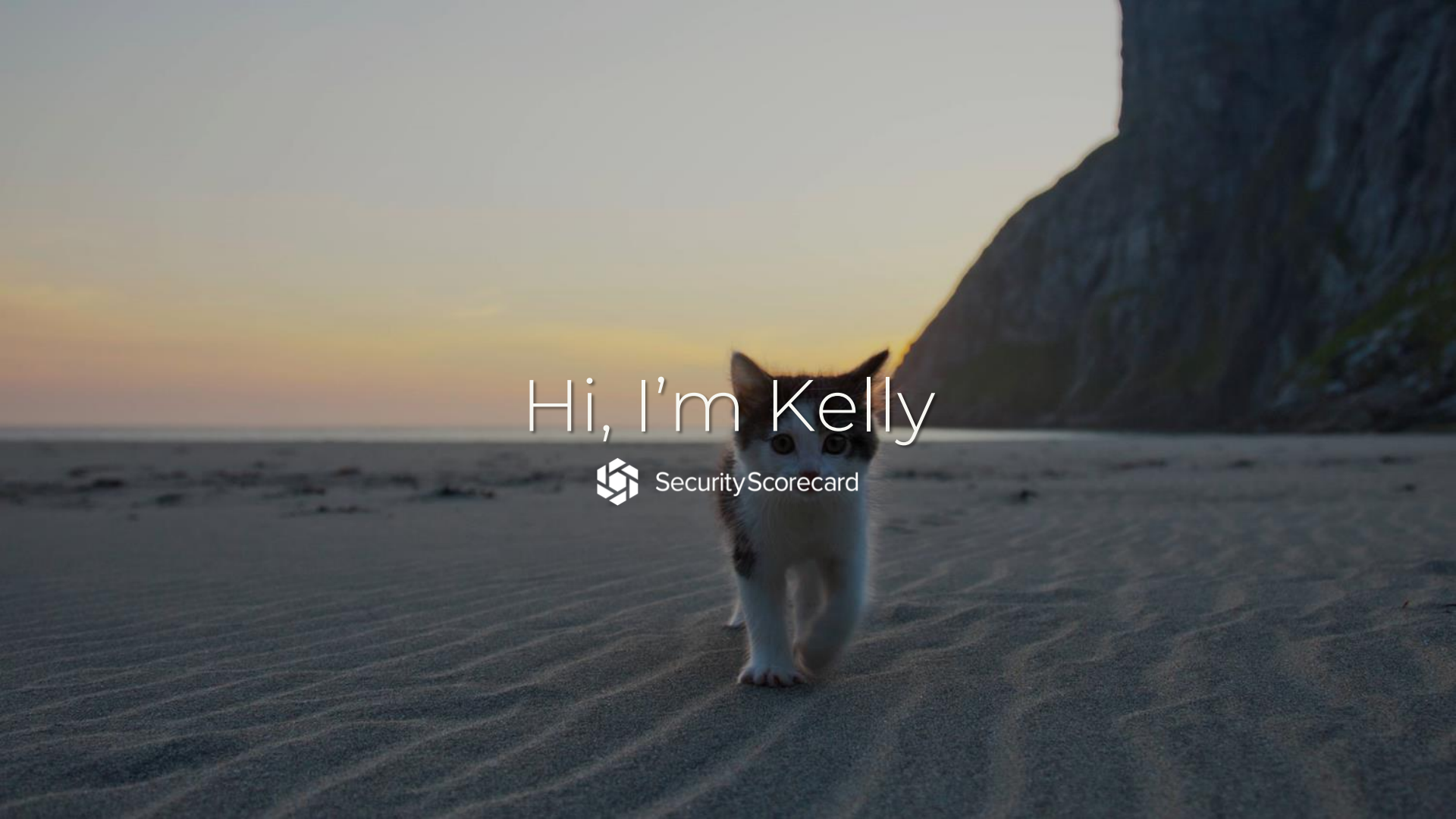
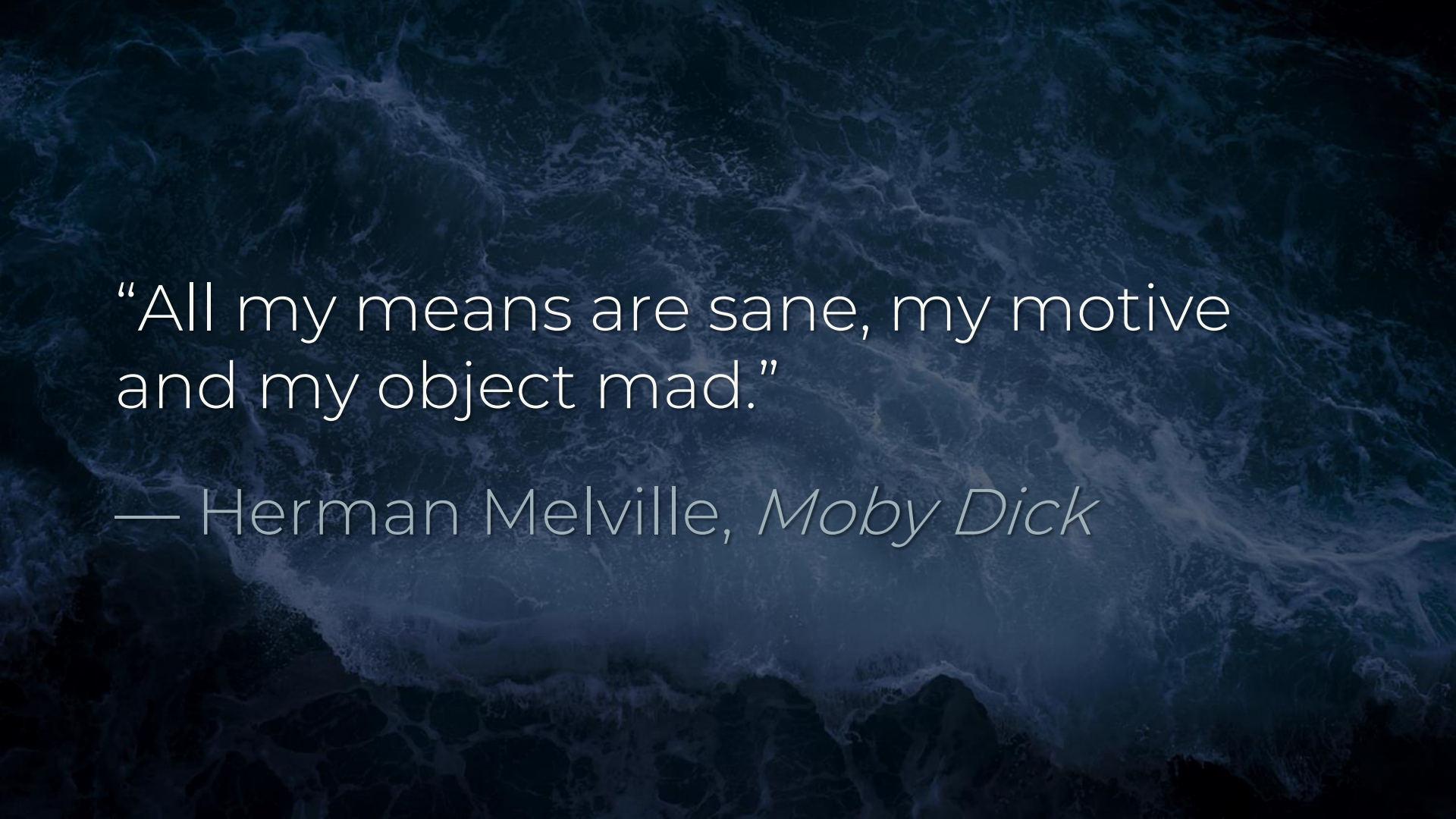
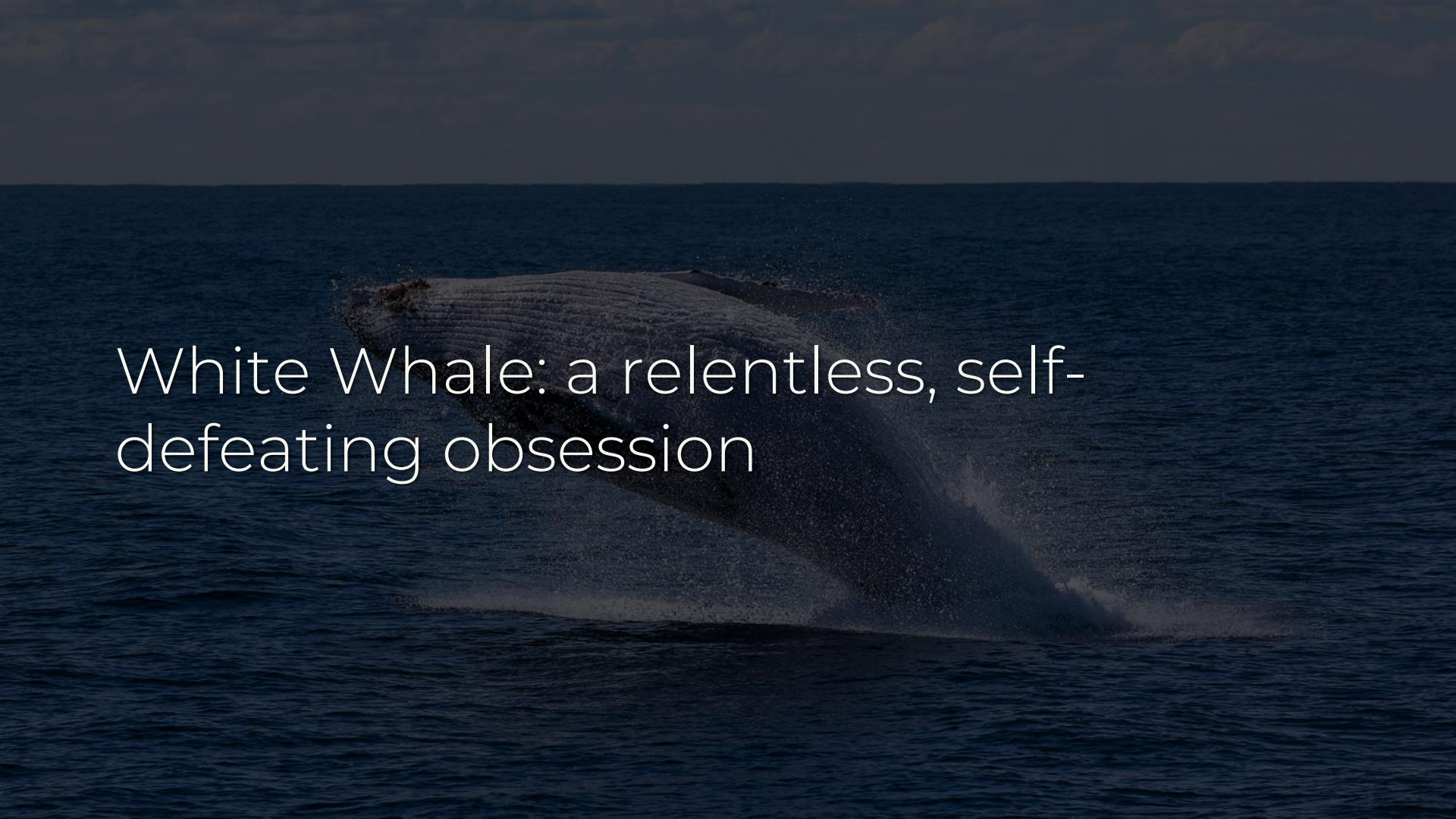
Threat Prioritization: Freeing the White Whale

Kelly Shortridge (@swagitda_)

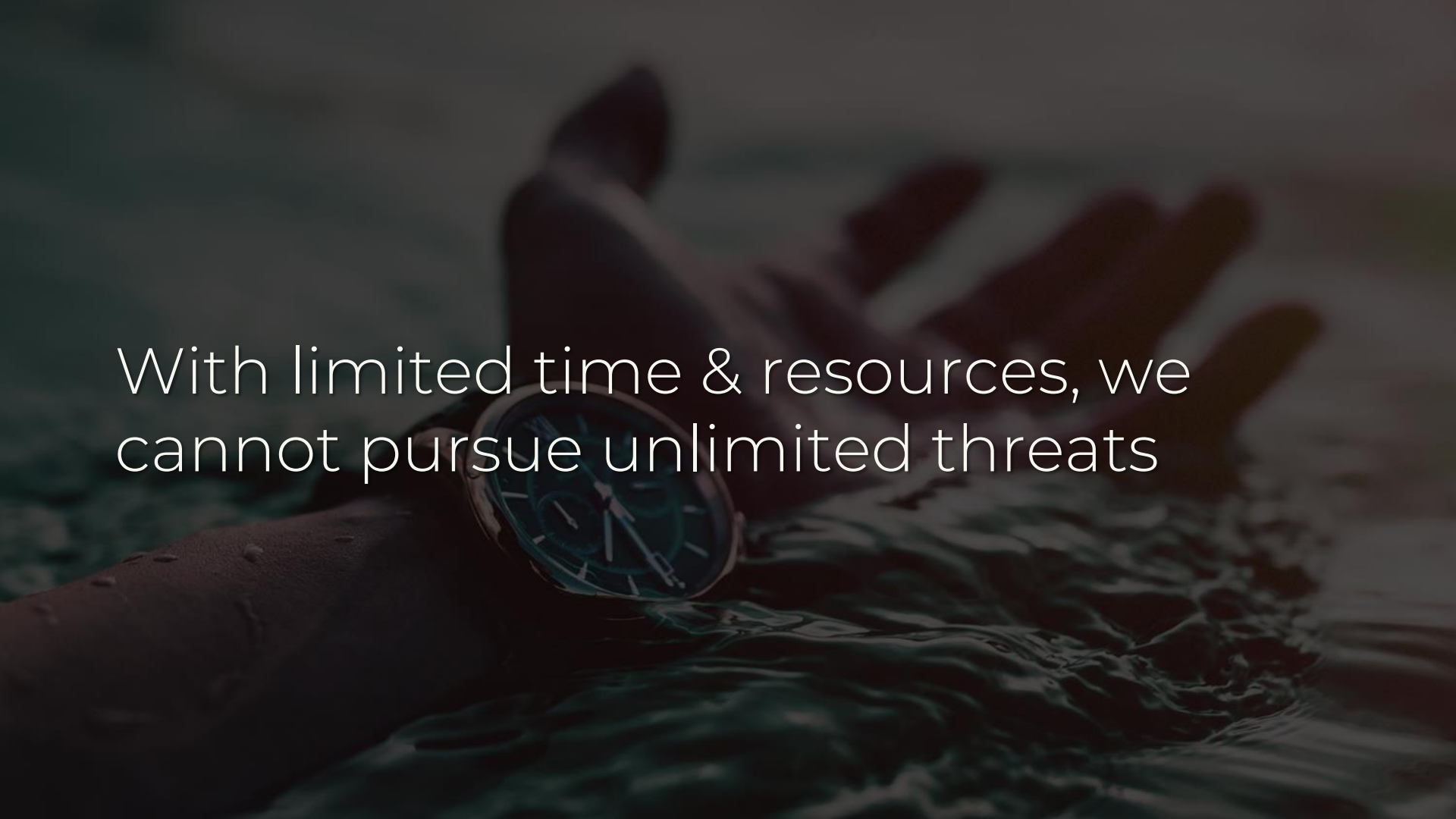
HackNYC 2018


Hi, I'm Kelly
SecurityScorecard

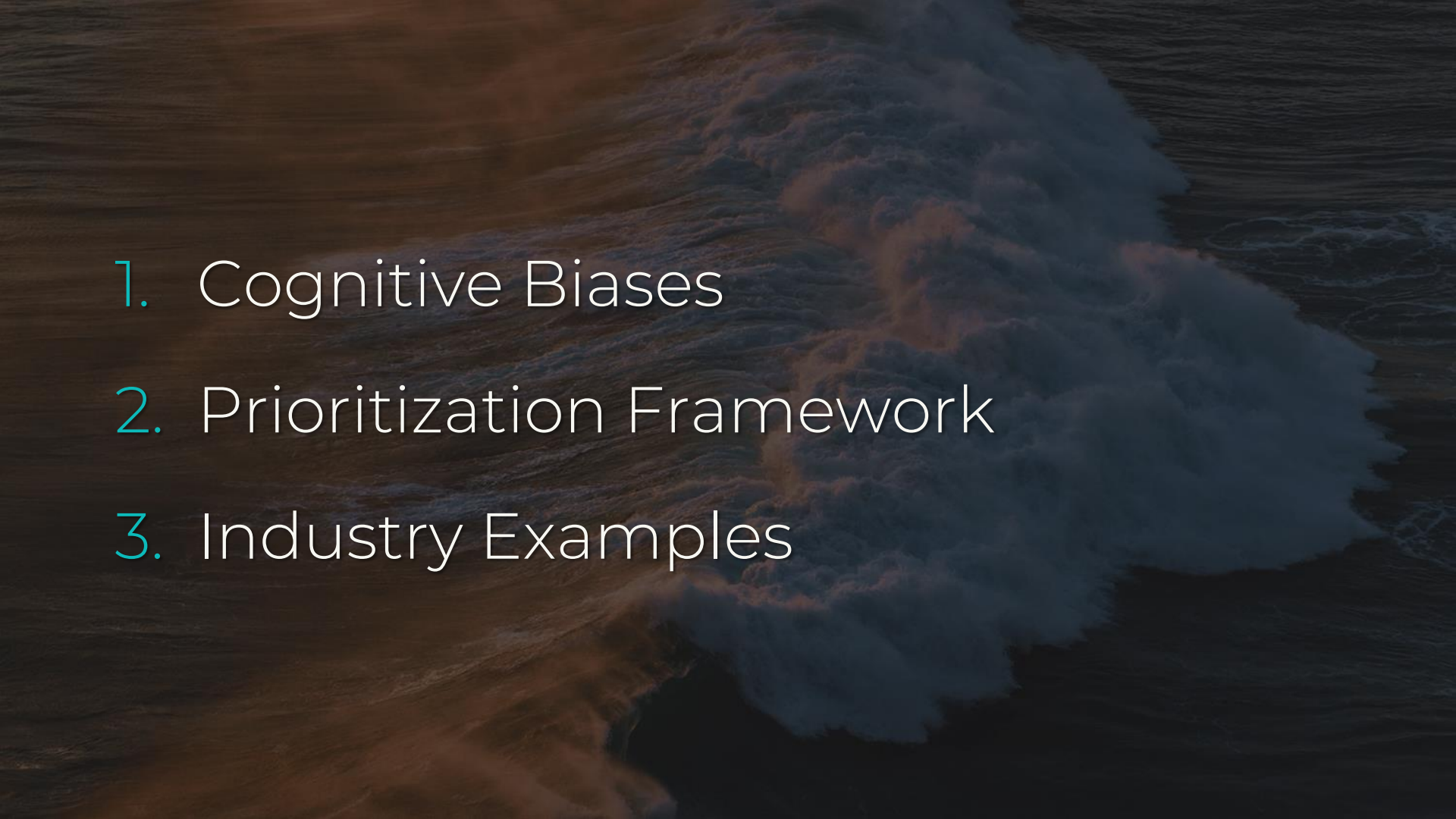

“All my means are sane, my motive and my object mad.”
— Herman Melville, *Moby Dick*



White Whale: a relentless, self-defeating obsession


With limited time & resources, we
cannot pursue unlimited threats

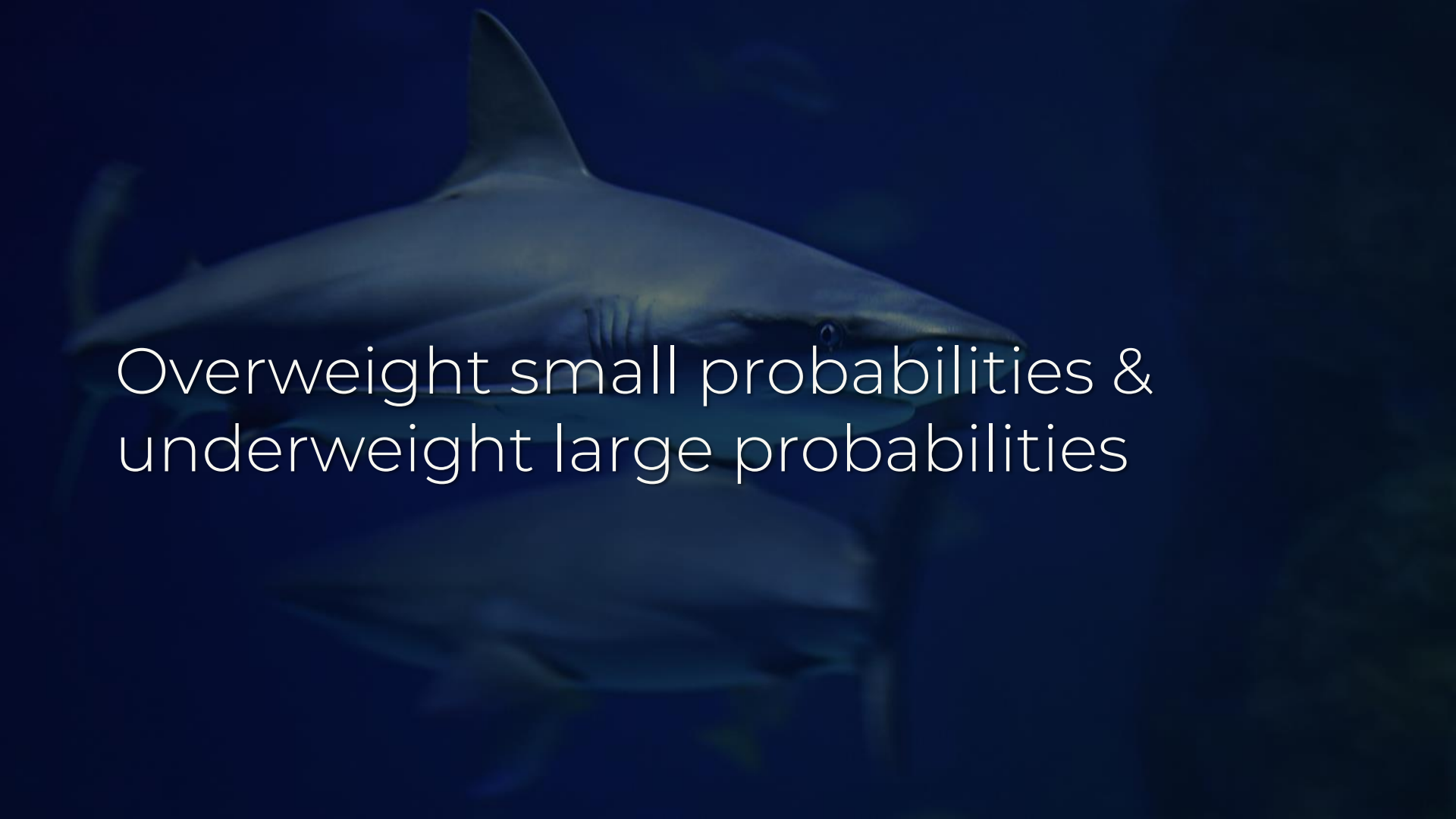

Hunting the White Whale will leave
you vulnerable – or even destroy you


1. Cognitive Biases
2. Prioritization Framework
3. Industry Examples


Cognitive Biases

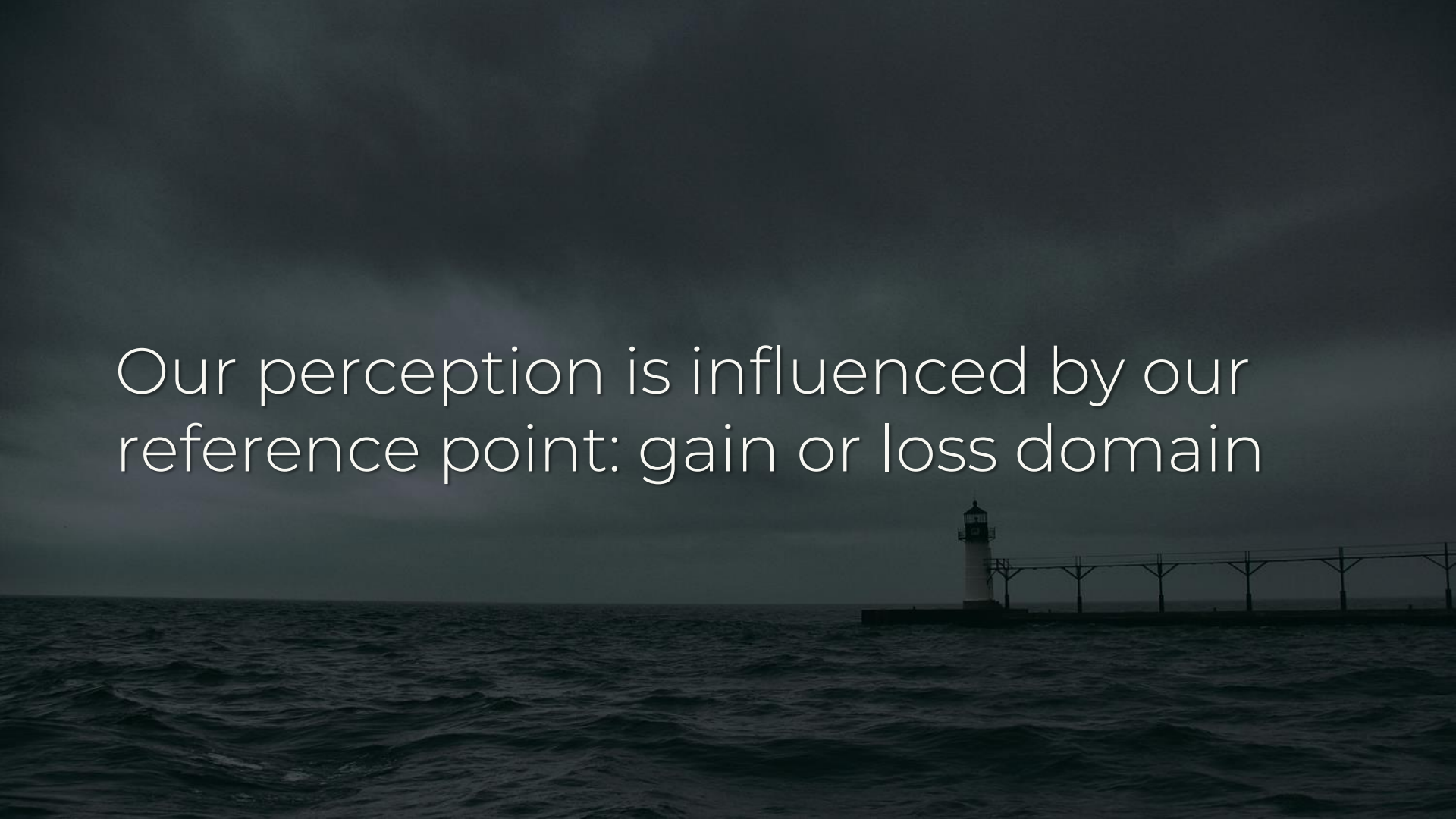
Cognitive biases: we use subjective perceptions of inputs for decisions

Heuristics – mental short cuts that allow us to make faster decisions


Overweight small probabilities &
underweight large probabilities

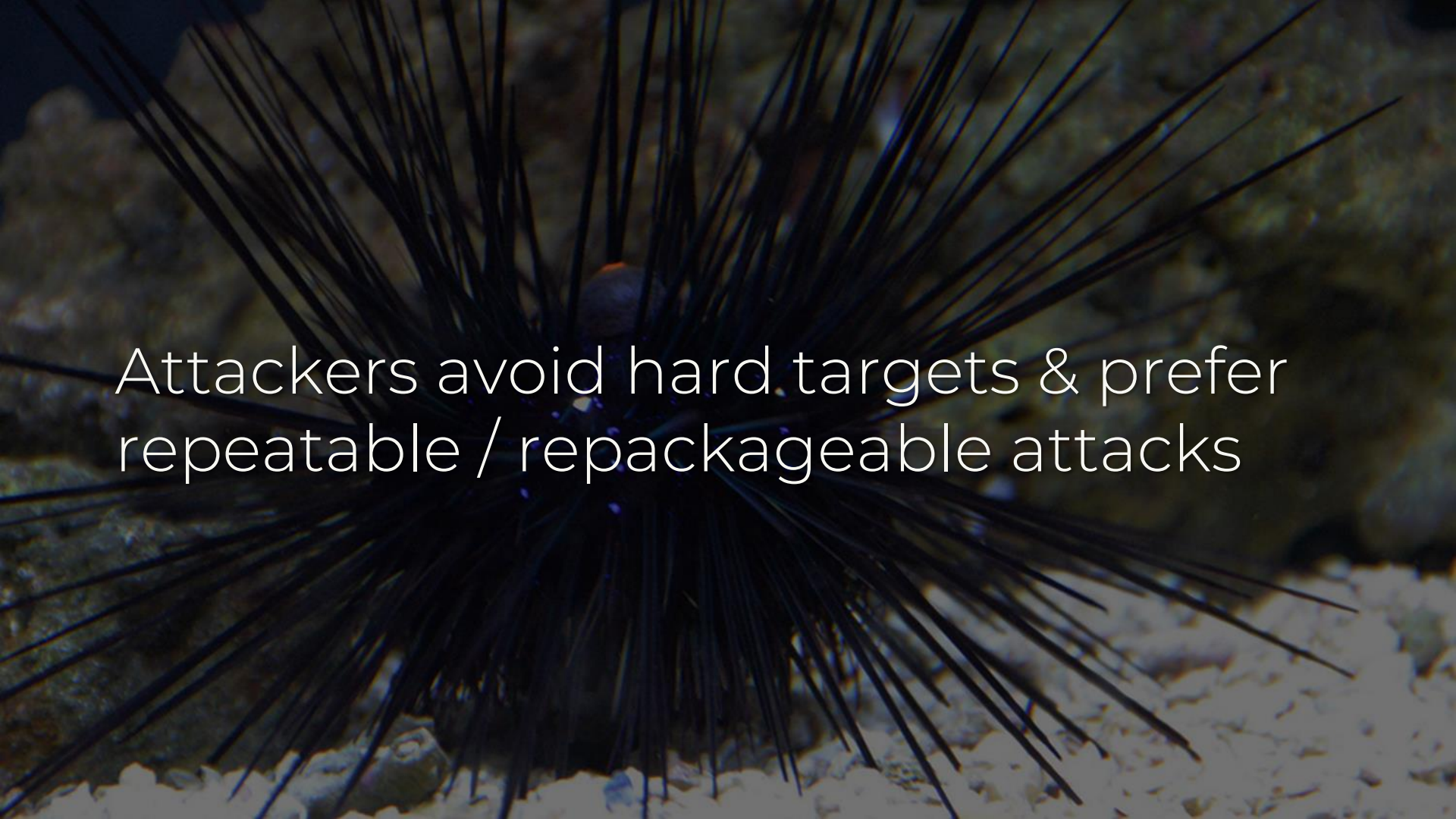
Specifically, ~35% likelihood is when we begin underweighting events


Super elite 0day (overweighted) vs.
phishing (underweighted)


Our perception is influenced by our reference point: gain or loss domain

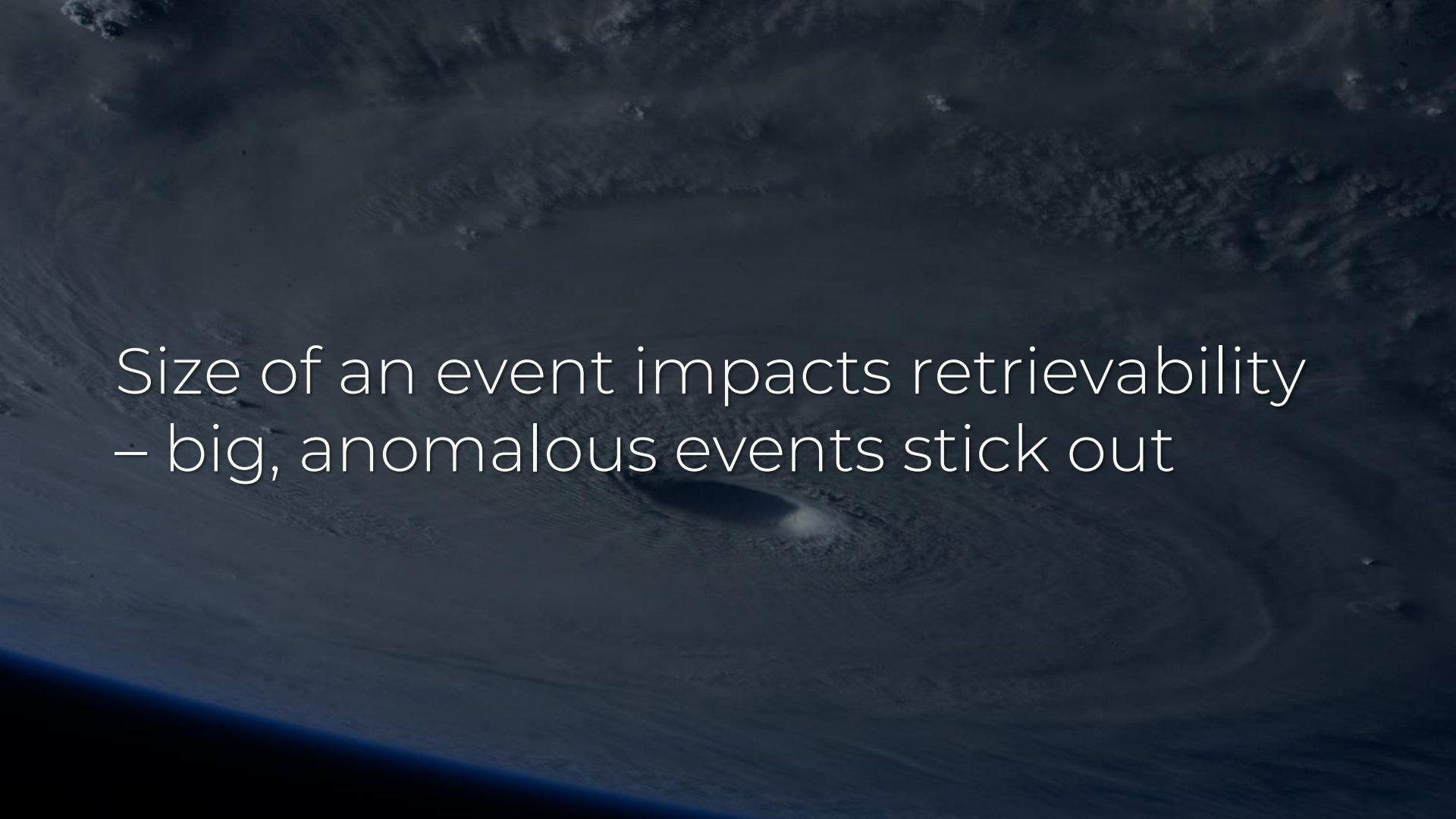
Attackers are risk-averse

Defenders are risk-seeking

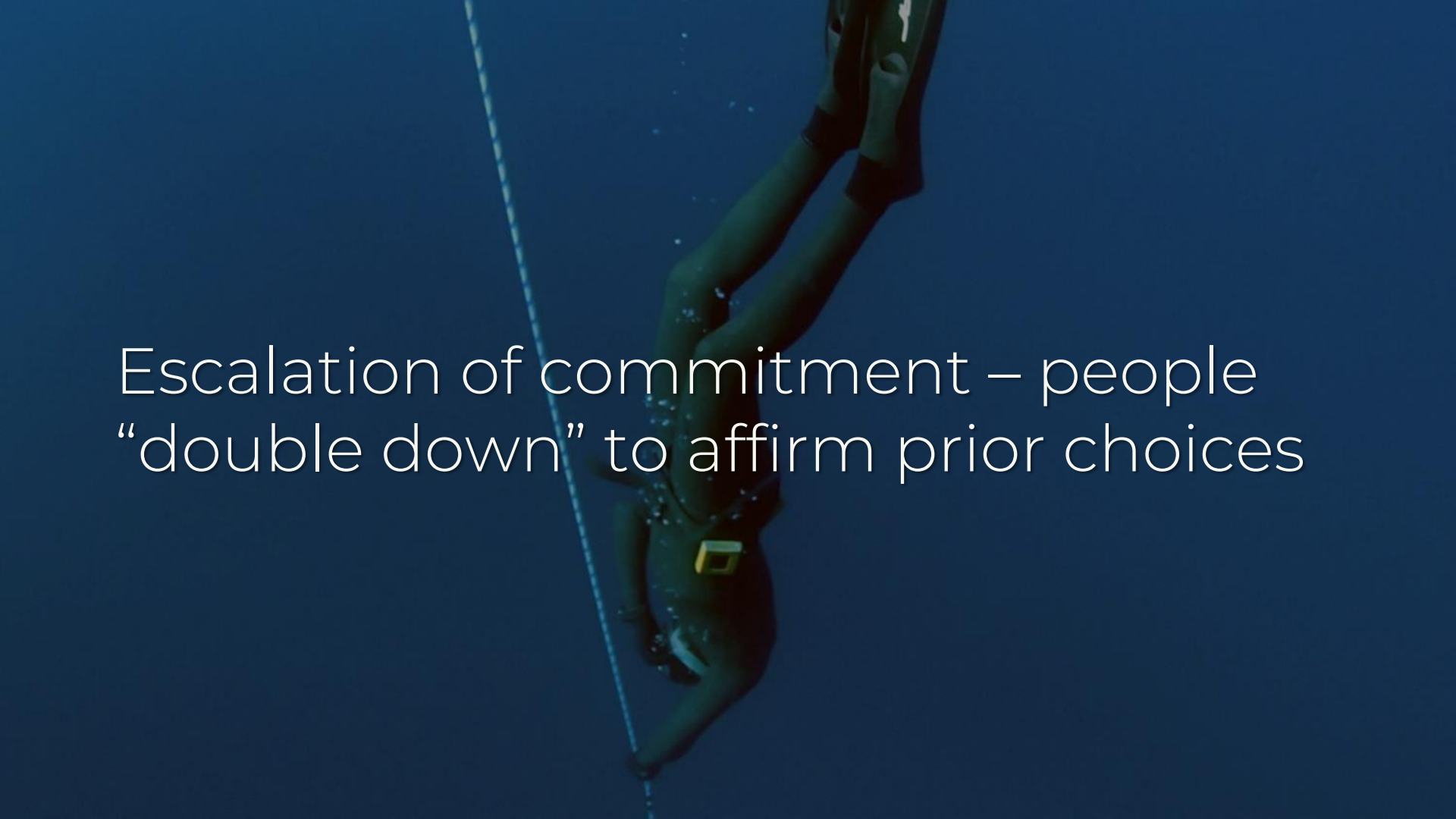

Attackers avoid hard targets & prefer
repeatable / repackageable attacks

Defenders prefer a slim chance of a “gain” (stopping a hard attack)


Availability heuristic – those headlines
about “Cybergeddon” influence you


Size of an event impacts retrievability
– big, anomalous events stick out

Your executives will be prone to this – come prepared with actual data



Escalation of commitment – people “double down” to affirm prior choices


Continuing to use strategies or
vendors with limited efficacy or ROSI

Confirmation bias: people try to prove hypotheses vs. disprove (less efficient)


Finding one incident that proves a
threat exists & ignoring improbability

How can we counter these biases & adopt a framework based on realism?

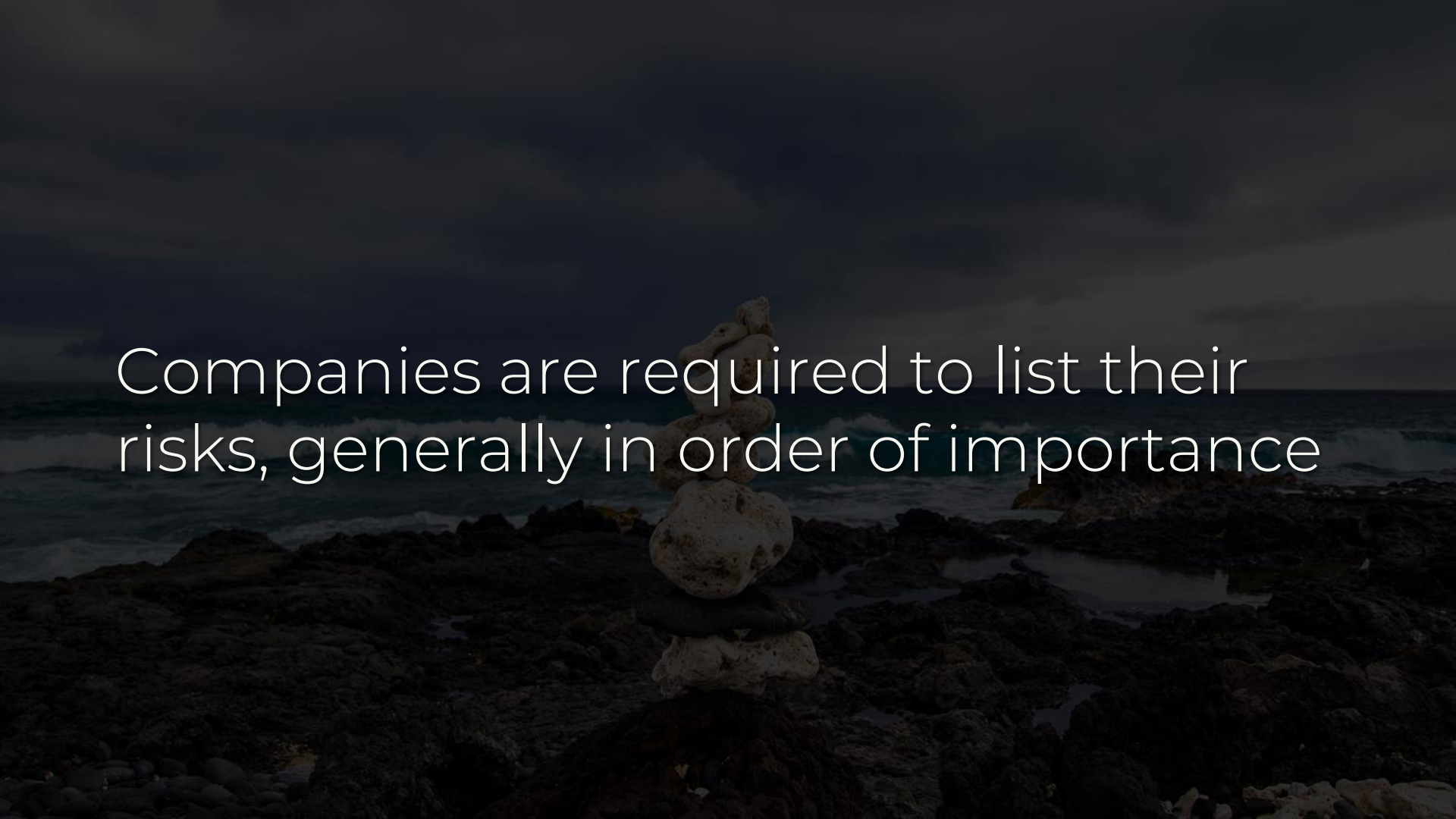

Prioritization Framework


What hurts your business compared to what is valuable to attackers?

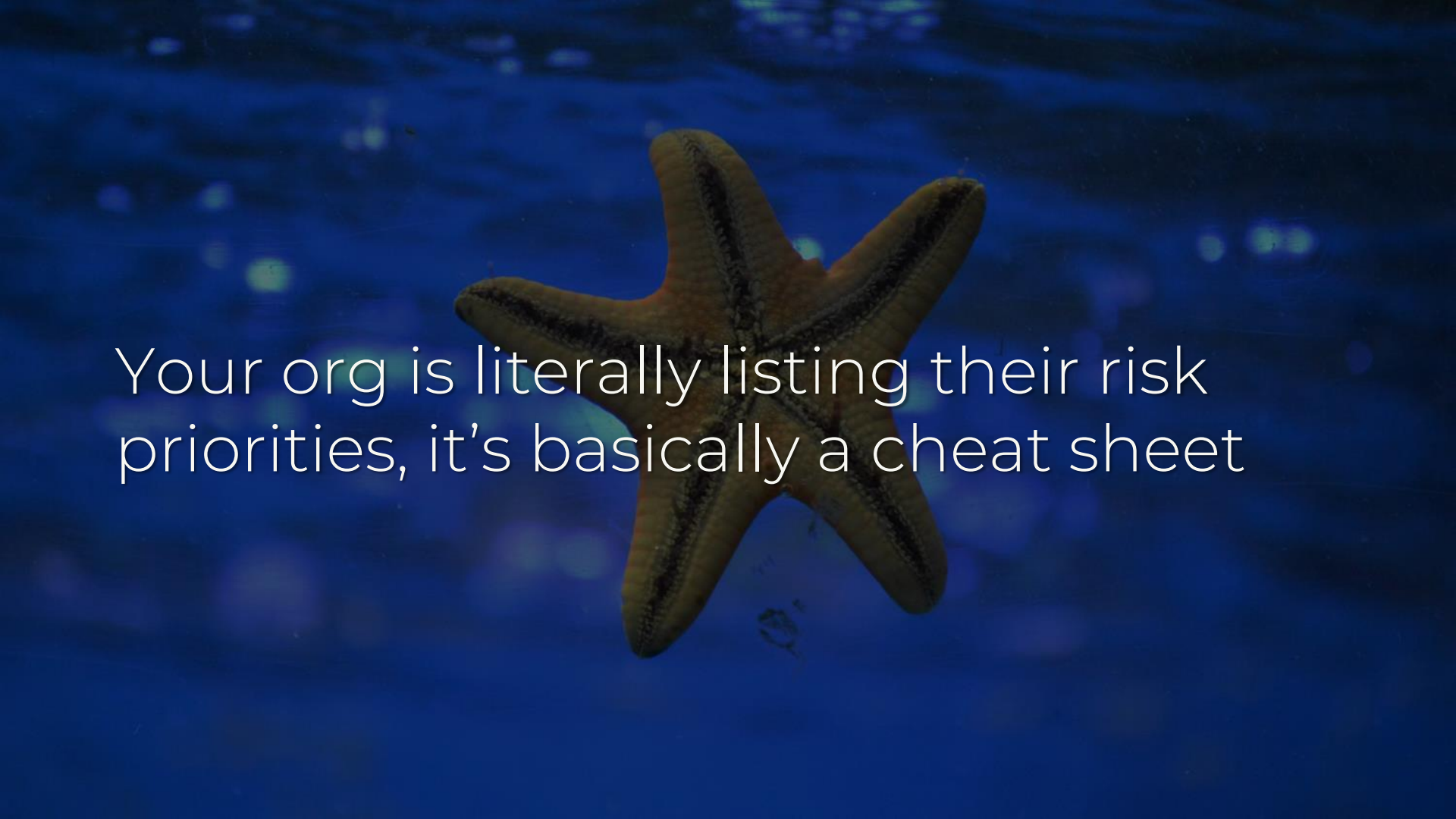

Step 1: How does your business make money? What are risks to that?

Go to your org's / your competitors' Investor Relations website

10-K is an annual report about a business' operations required by SEC


Companies are required to list their risks, generally in order of importance

Read the “Risk Factors” section of your company’s (or competitors’) 10-K


Your org is literally listing their risk priorities, it’s basically a cheat sheet

Reality check: “cyber risk” is usually in the last third of the list

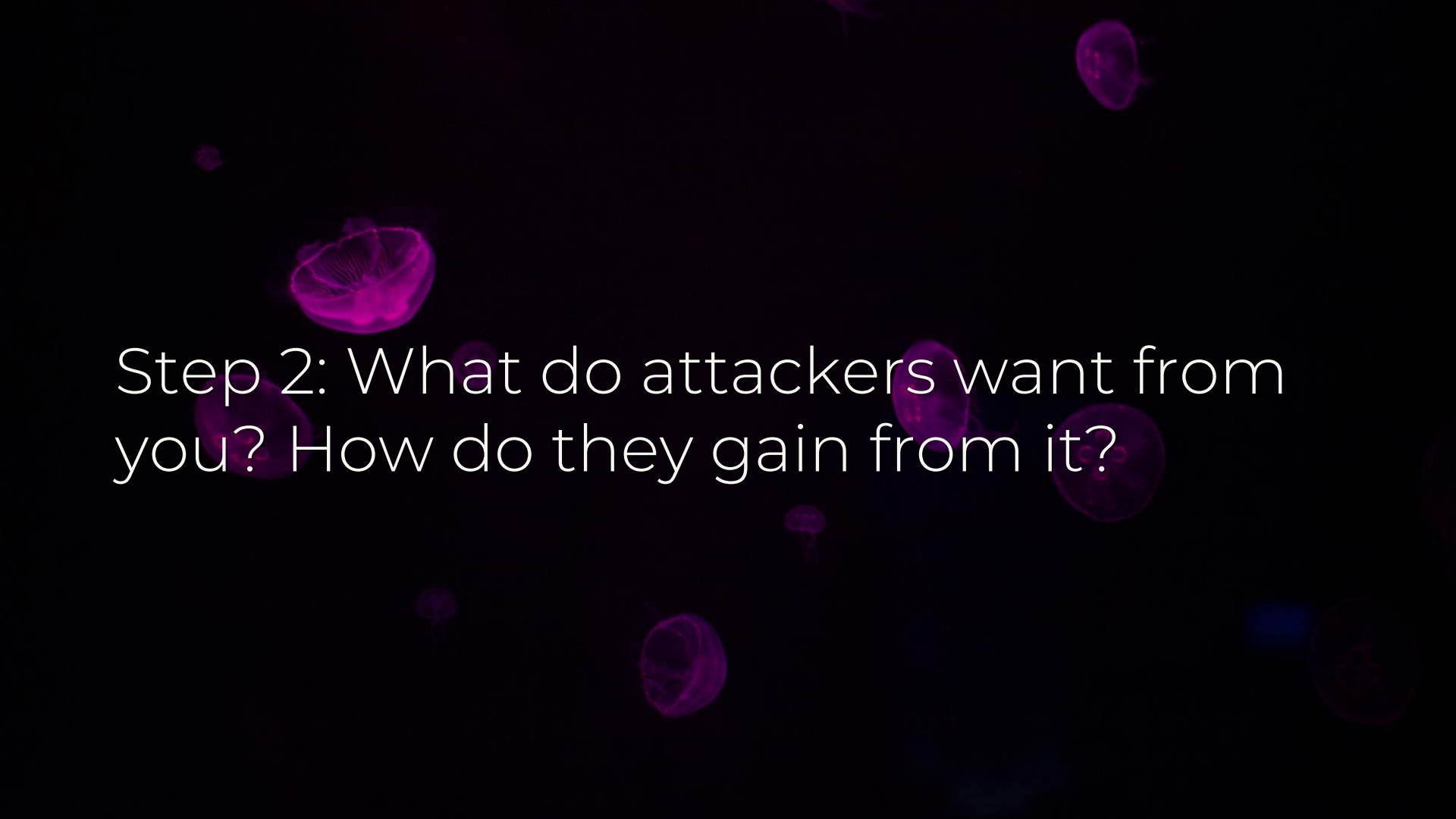
Which business lines make the most money for your company? (Item 6)


The consumer-facing segment isn’t
always the most revenue-generating

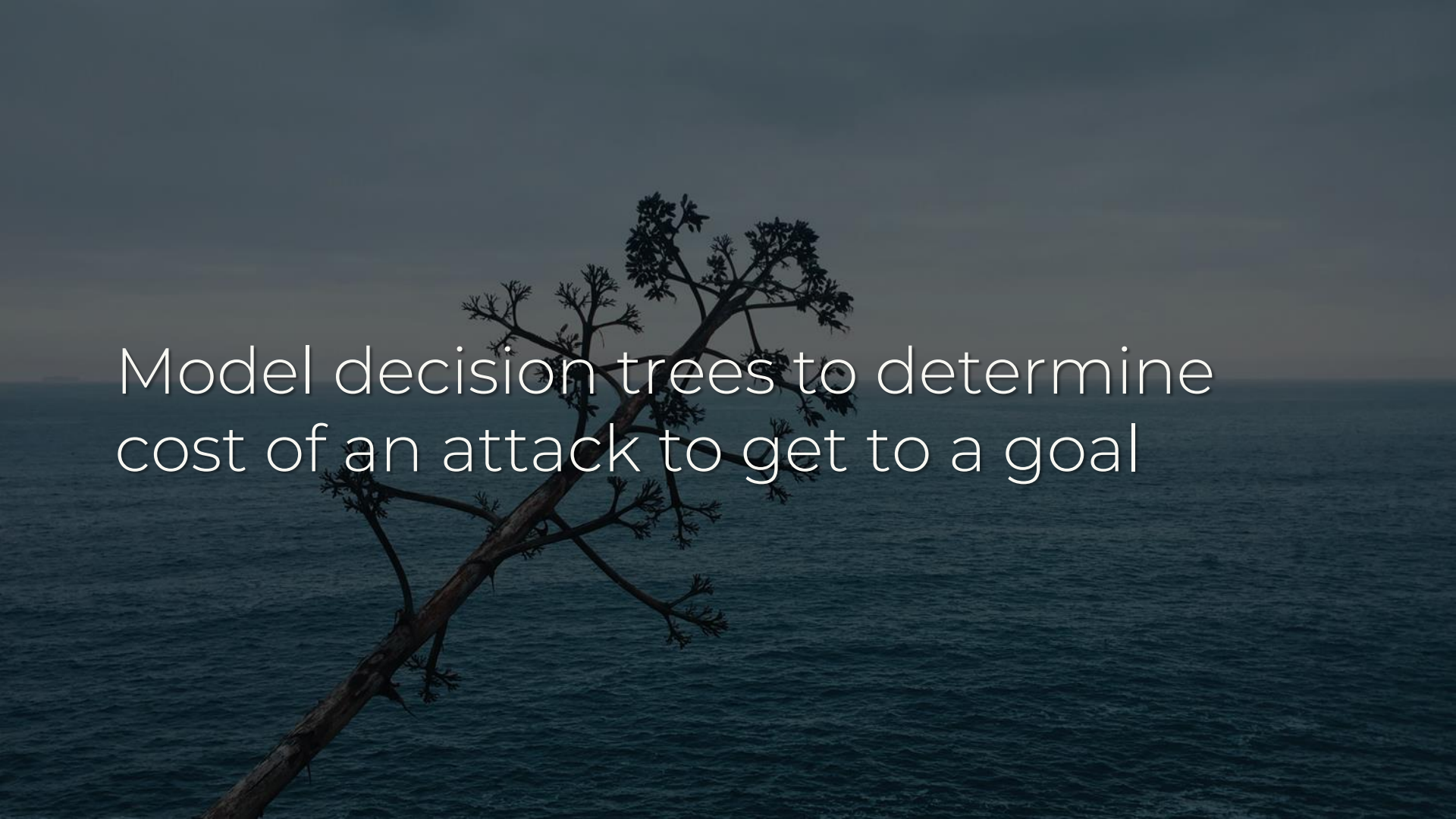
IR resources: cheat-sheets for future priorities, so you can plan ahead

Read cyber insurance coverage for your industry, including exceptions

Ask your local finance / accounting colleague what they think


Step 2: What do attackers want from you? How do they gain from it?

Criminals need monetization & deeply care about ROI


Model decision trees to determine
cost of an attack to get to a goal


Step 3: Cross-compare results


If you don’t see *your* priority in Risk Factors, challenge your assumptions

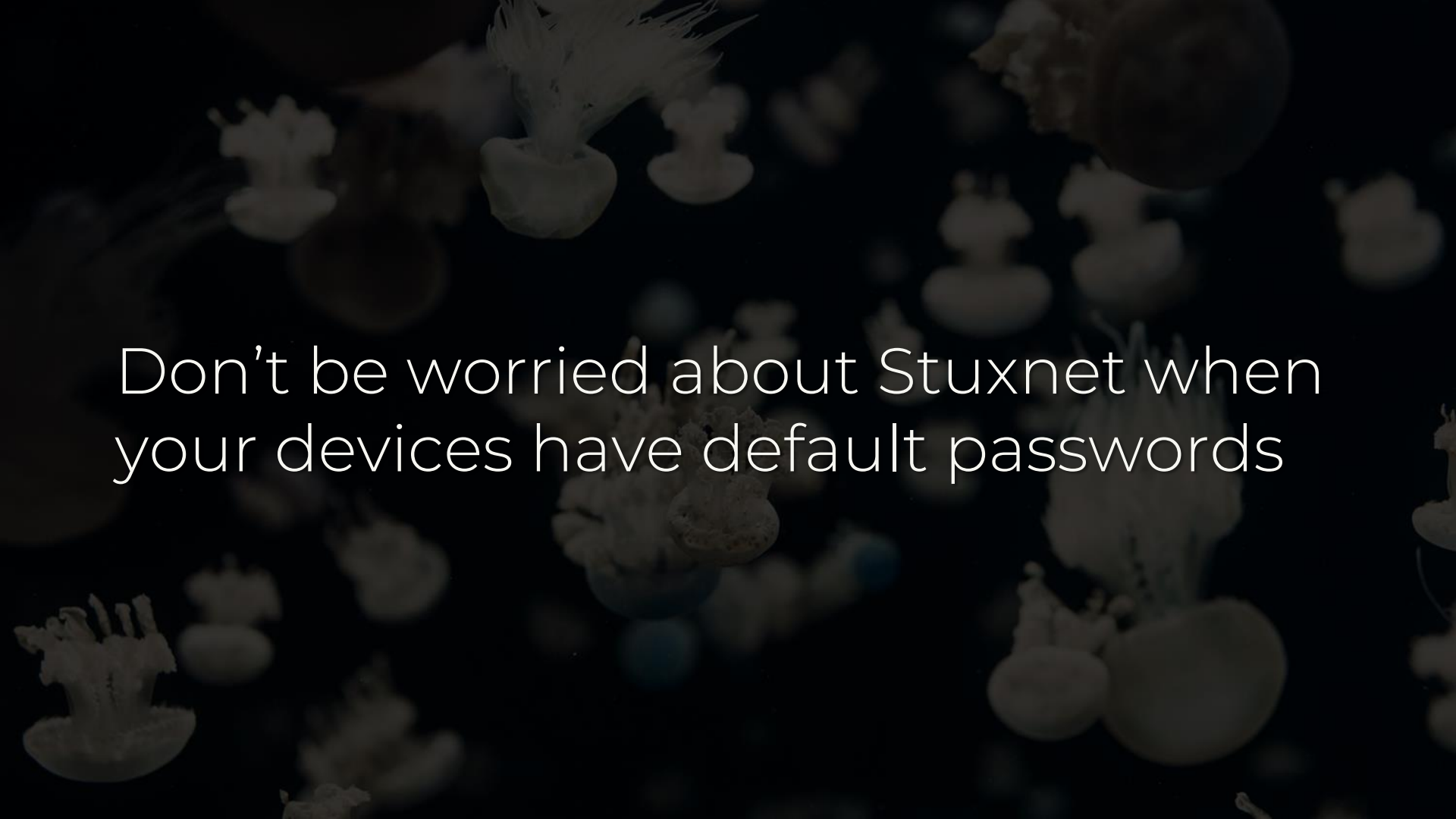
If there’s a Risk Factor that is implausible for attackers, let it go


Hackers are unlikely to remotely crash your satellite into space debris

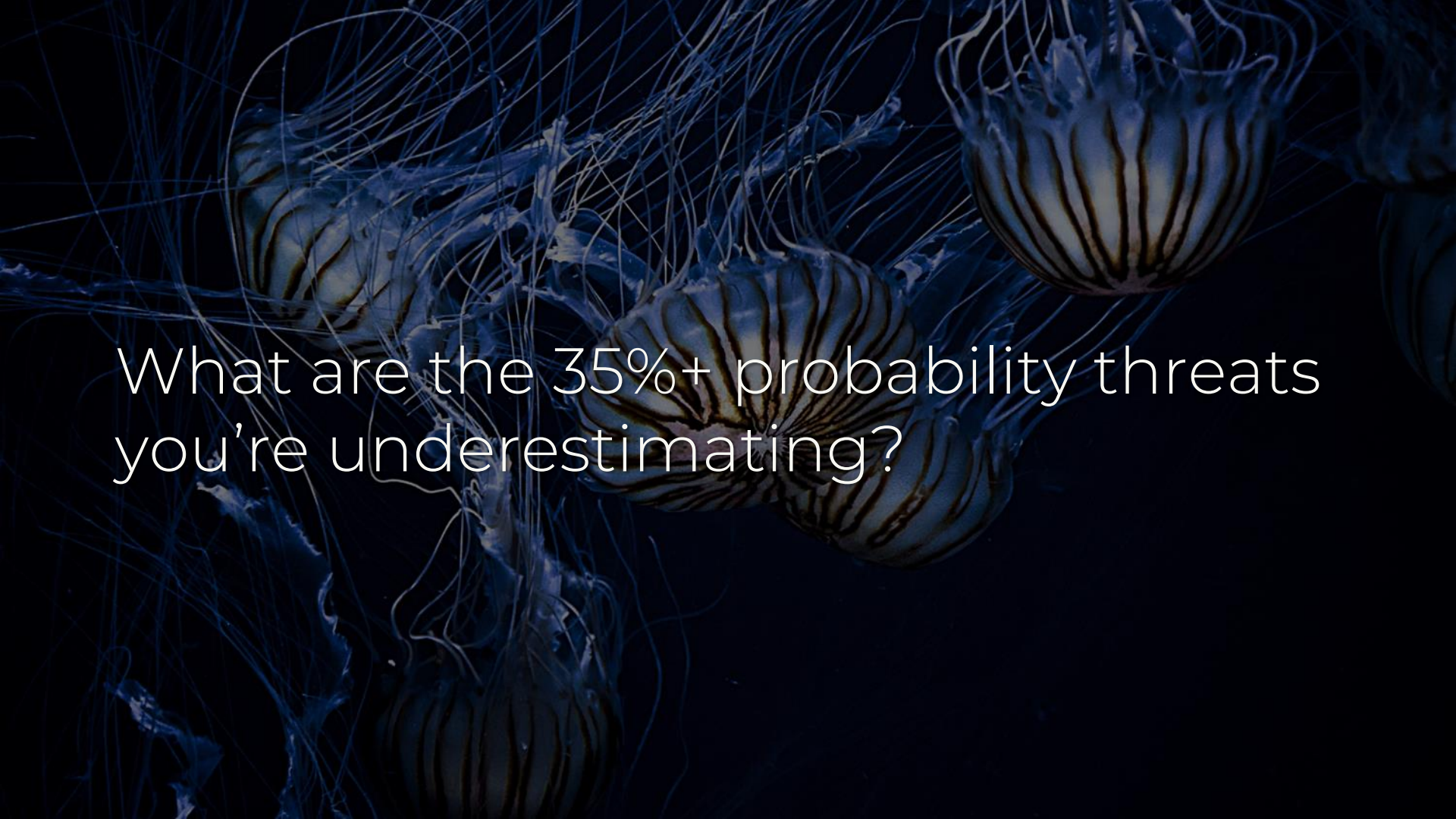
Just because something is possible, doesn’t mean it’s worth defending


Security morals: literally every threat is
the most super duper critical ever


Evolution doesn’t favor those who
don’t prioritize threats accurately

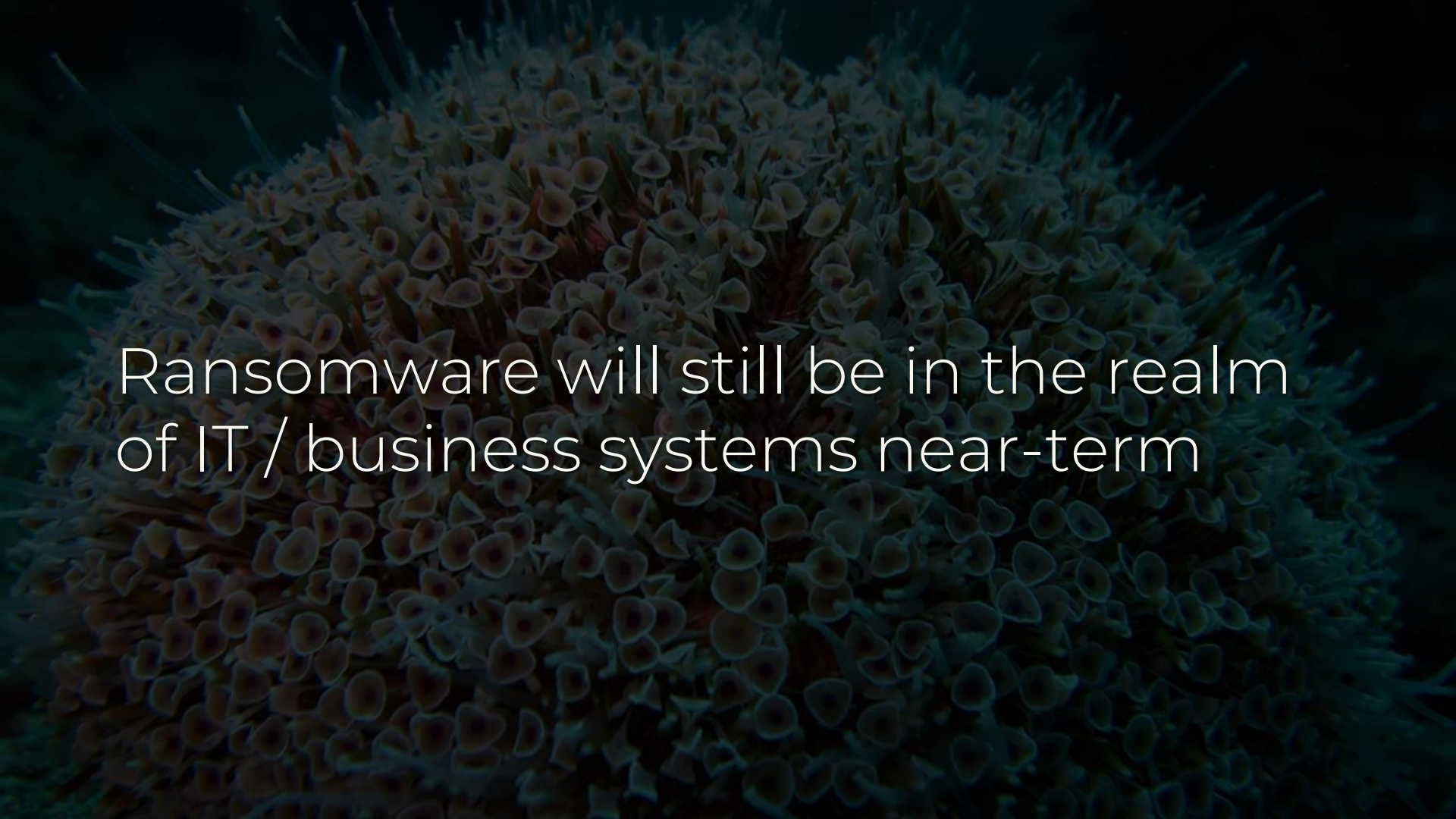

Don’t be worried about Stuxnet when
your devices have default passwords

Financial impact analysis is an essential part of your risk assessments


What are the 35%+ probability threats you’re underestimating?

Spear-phishing & BEC – attackers might as well try it first


DDoS attacks – spam or ransom

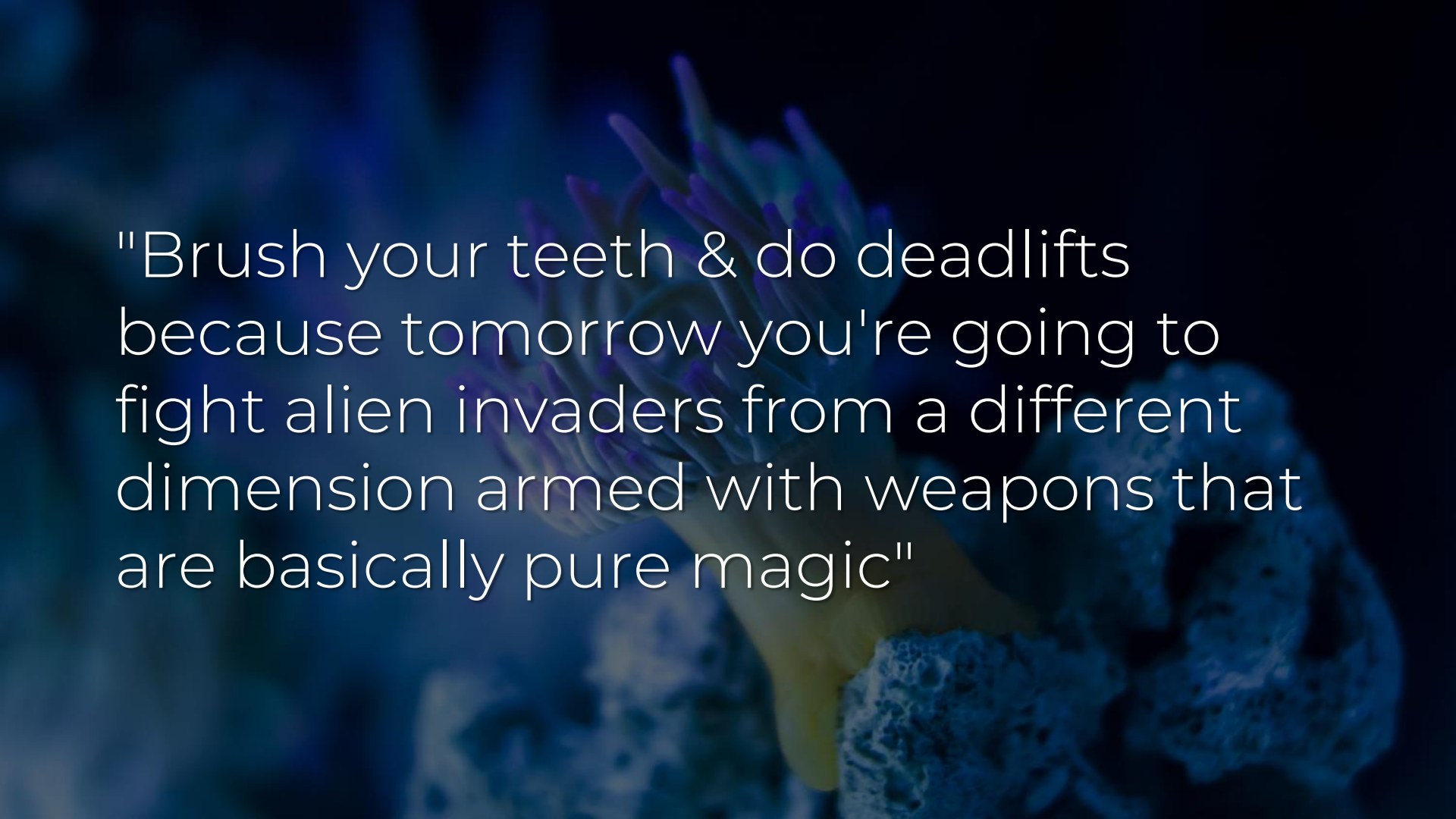

Ransomware will still be in the realm
of IT / business systems near-term

Time & resources required to port ransomware to OT = poor ROI

Mid-level attacks for OT simply don’t have proper economics for attackers


Well-resourced groups, sophisticated techniques – please try to care less

CNI threat model: IT systems security basics + serenity prayer for APT


"Brush your teeth & do deadlifts because tomorrow you're going to fight alien invaders from a different dimension armed with weapons that are basically pure magic"

First $1mm in budget: backups, 2FA, SSO, config management, cloud SIEM

How would this apply to individual industries?

Energy

Step 1: What are the risks & predominant revenue sources?


Non-tech: changes in oil prices, regulations, cleanup liability, weather


Operational efficiency is seen as a
competitive advantage now

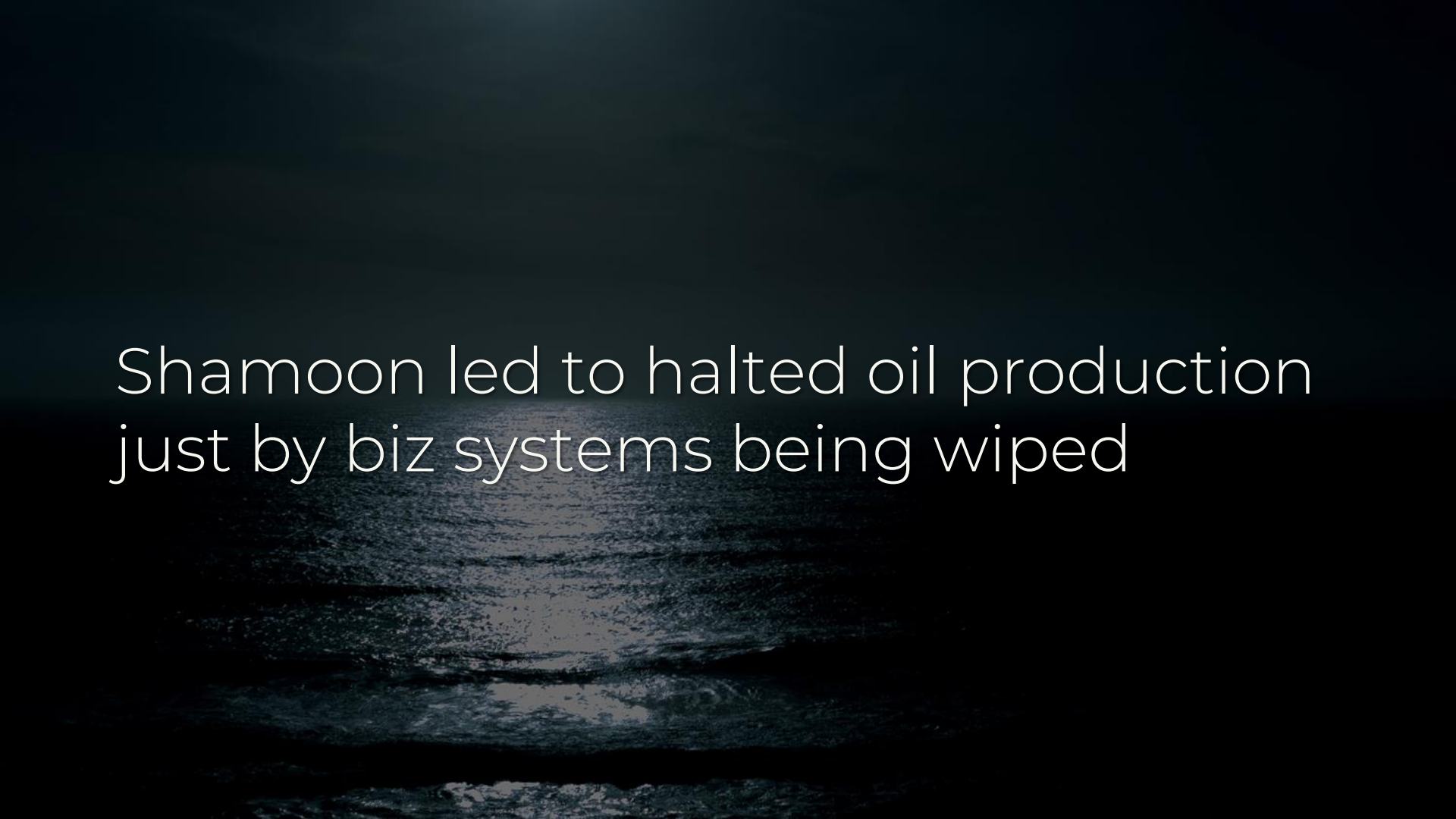
Project management: negotiations, development, optimization

Tech: operational unavailability, inefficiency, or disruption

Infosec: physical harm, asset damage, op disruption, biz system compromise


Oil rig = >$500mm
Refinery = $5bn - $15bn

Disruption of operations: more about the business side, ie IT systems

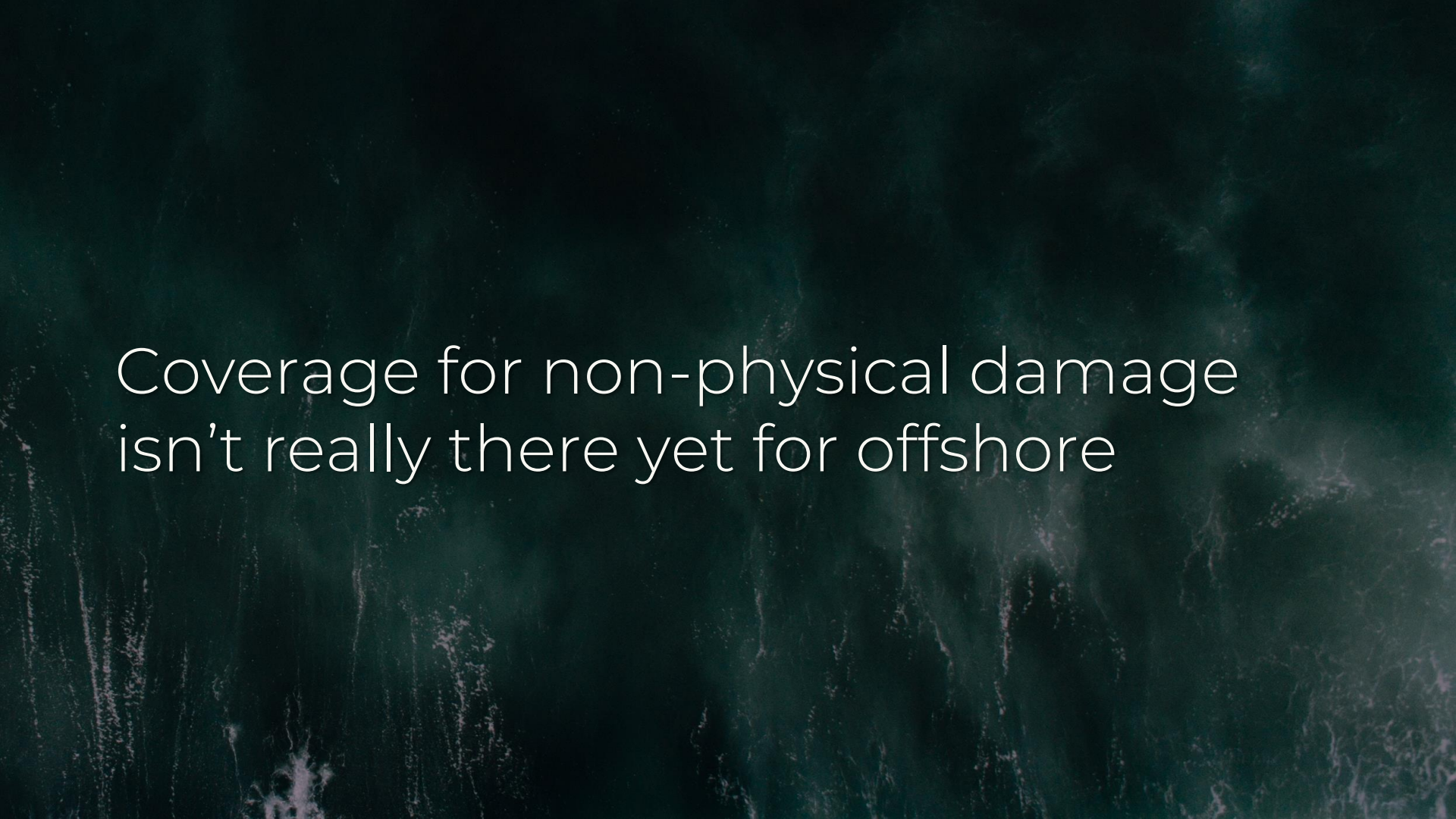

Shamoon led to halted oil production
just by biz systems being wiped

Up next: using big data for predictive maintenance = more connected

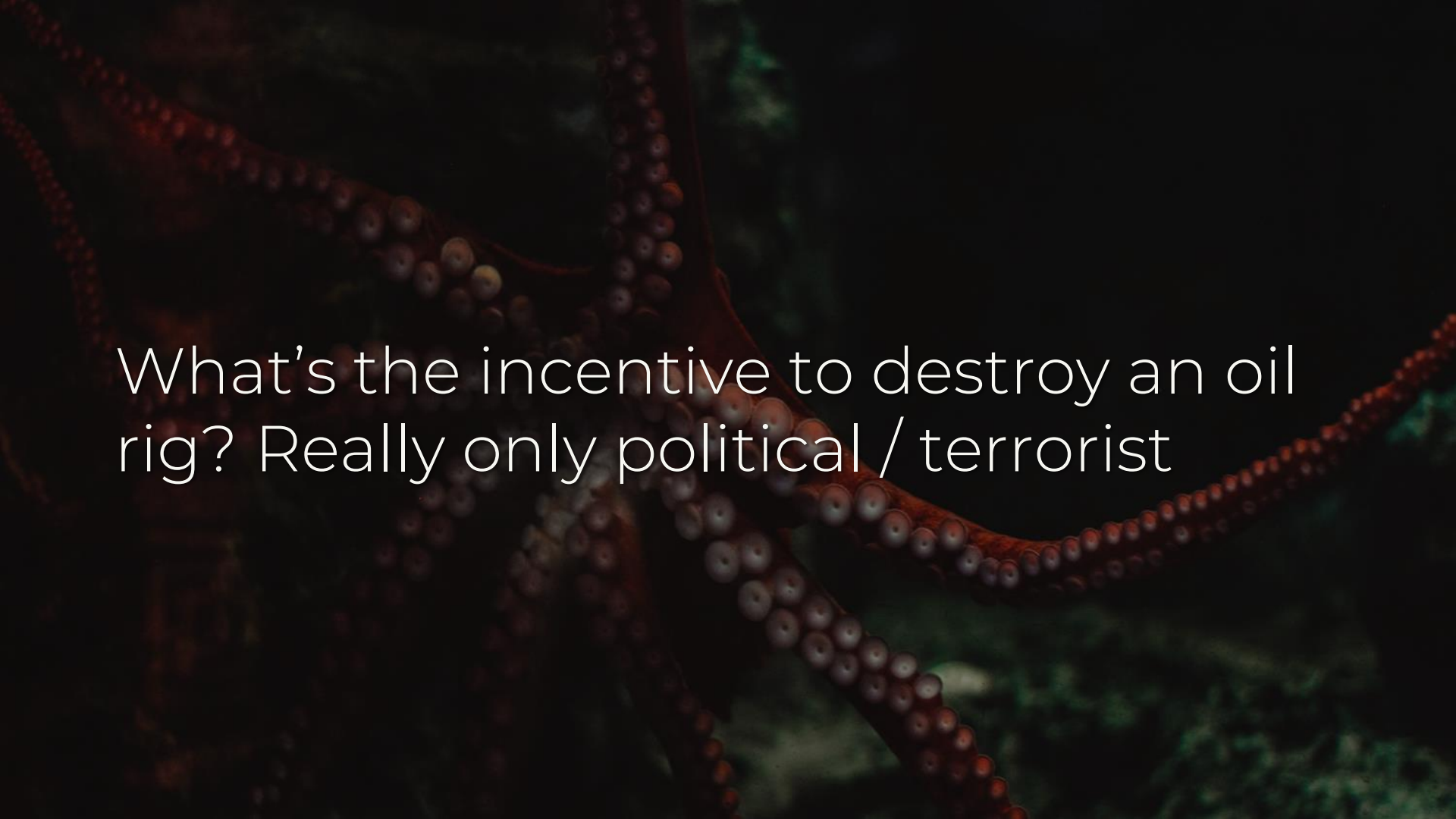
What is being insured by cyber insurance for oil & gas?

Offshore energy insurance often has an exclusion for cyber attacks

Coverage for cyber-physical damage covers up to $150mm - $400mm


Coverage for non-physical damage
isn’t really there yet for offshore

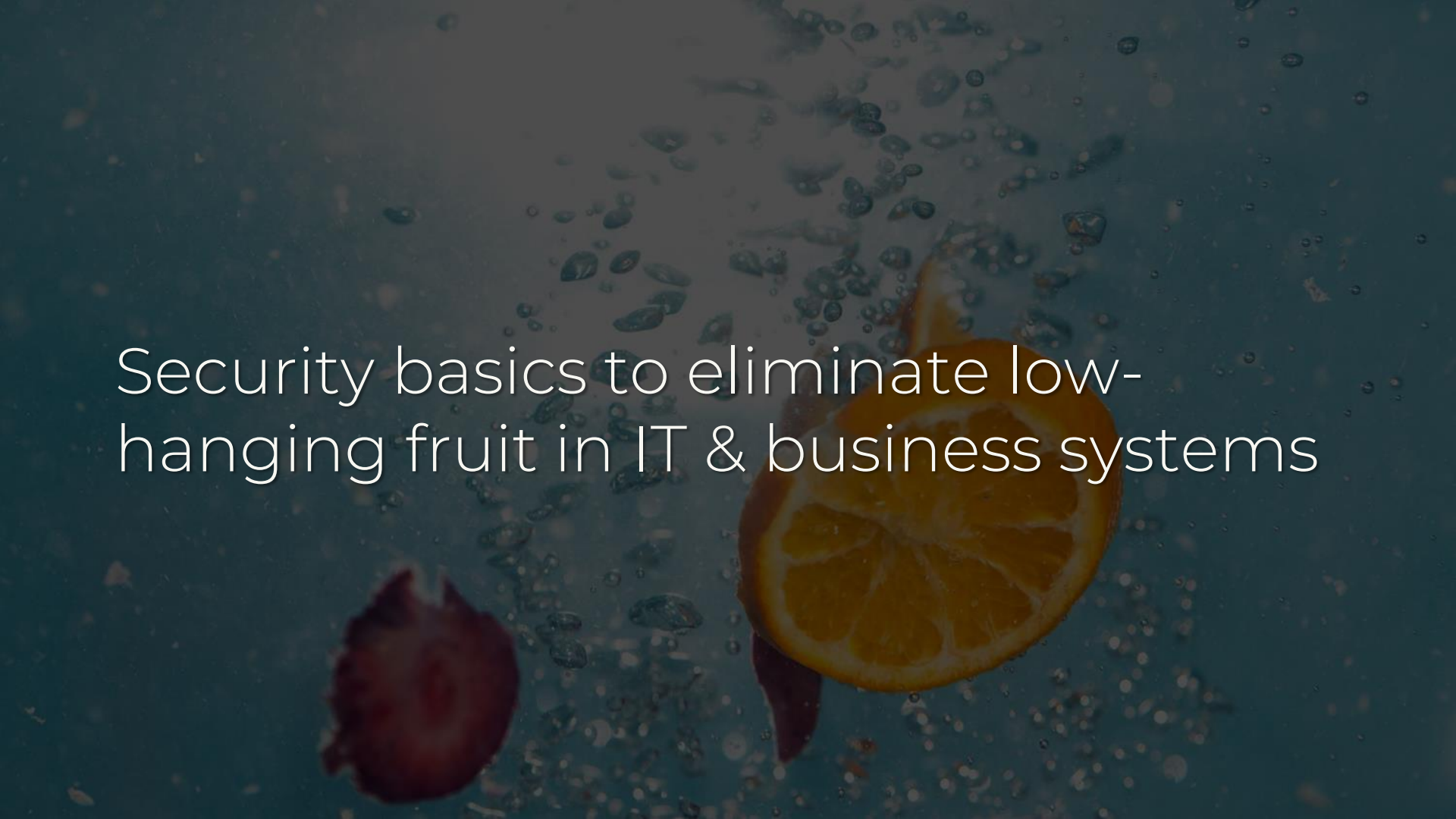
Step 2: What do attackers want?


What’s the incentive to destroy an oil rig? Really only political / terrorist

Nation-states also want leverage in negotiations – business data


BEC (e.g. CEO spam), DDoS (spam, extortion), IT system ransomware

Step 3: Where do Risk Factors & attacker goals align?


Security basics to eliminate low-hanging fruit in IT & business systems

Insurance, redundancy, & serenity prayer for physical assets


Telecom

Step 1: What are the risks & predominant revenue sources?

Uptime requirements, network disruption, service interruptions

Highly competitive envs, inability to role out new tech / modernize


Telecom companies = slow-moving,
curious creatures

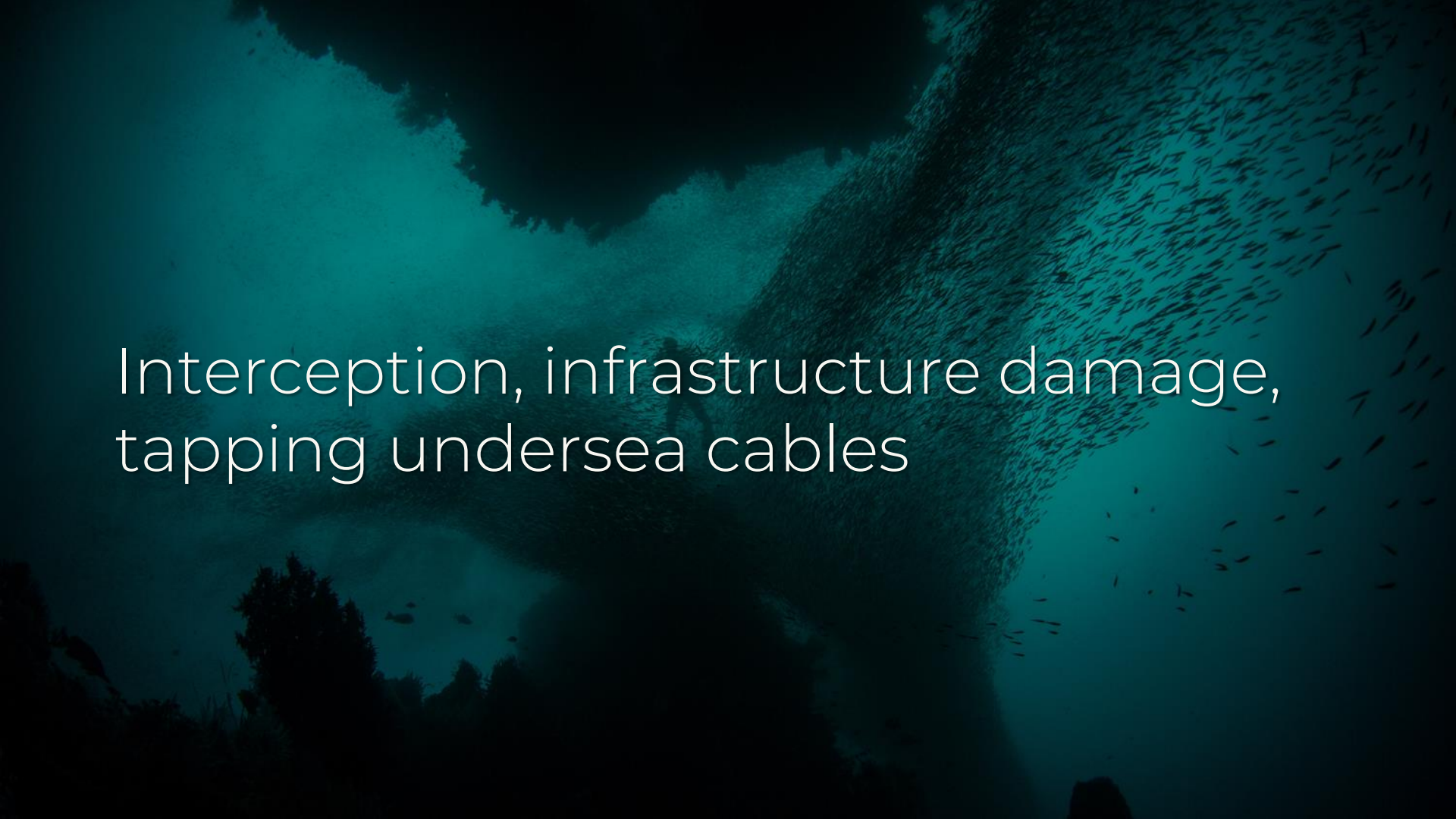
Curious about 5G (XML, JSON, REST), but slow-moving to adapt new tech

GDPR means PII may matter – privacy hasn't been economical before

Region-specific: fraud in developing countries (eg roaming disruption)

Step 2: What do attackers want?

PII, fraud (so much fraud), SS7 to intercept 2FA, spam

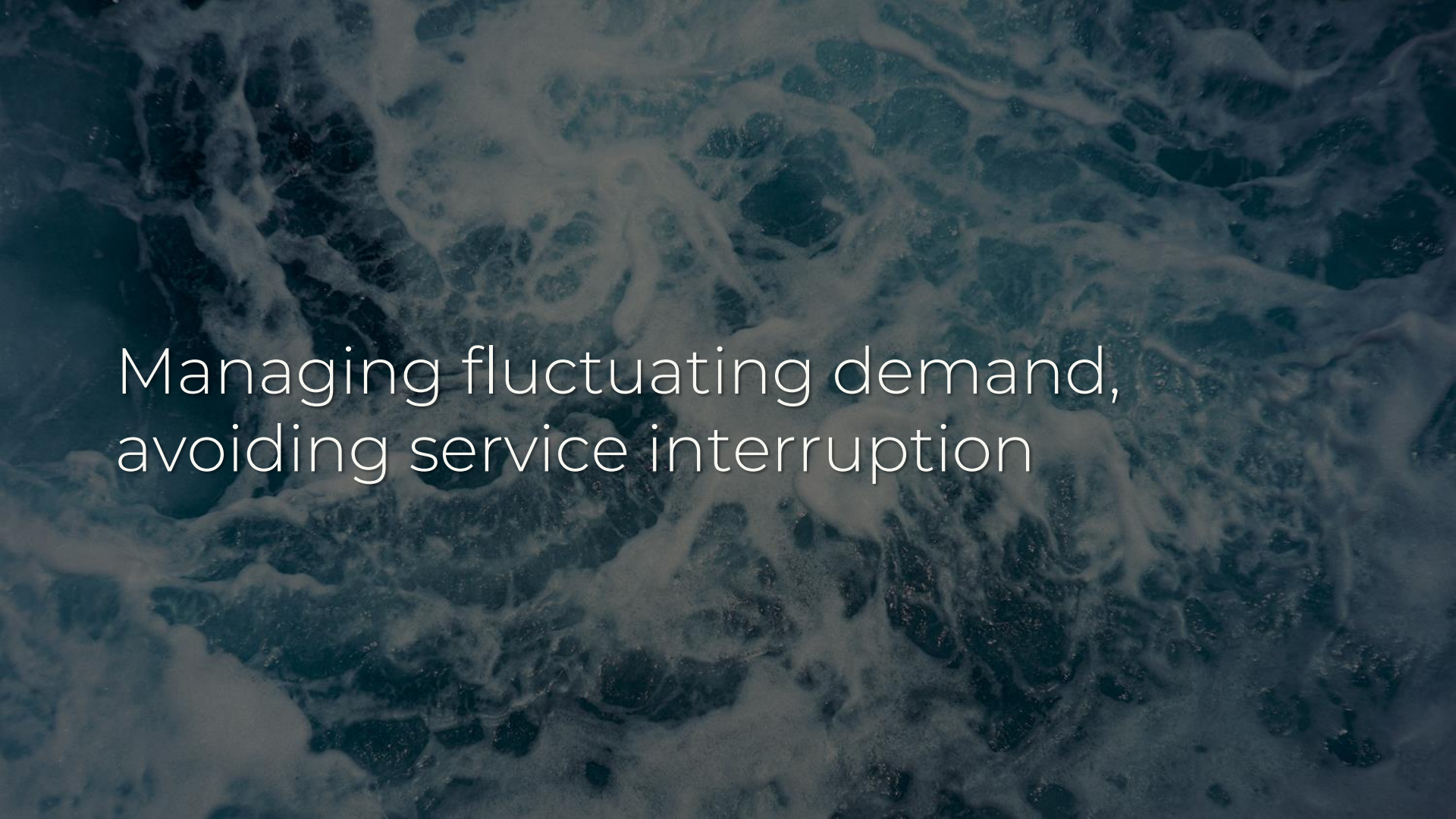

Interception, infrastructure damage,
tapping undersea cables

Step 3: Where do Risk Factors & attacker goals align?

Security basics to protect PII, improve network resiliency, API security

Transportation

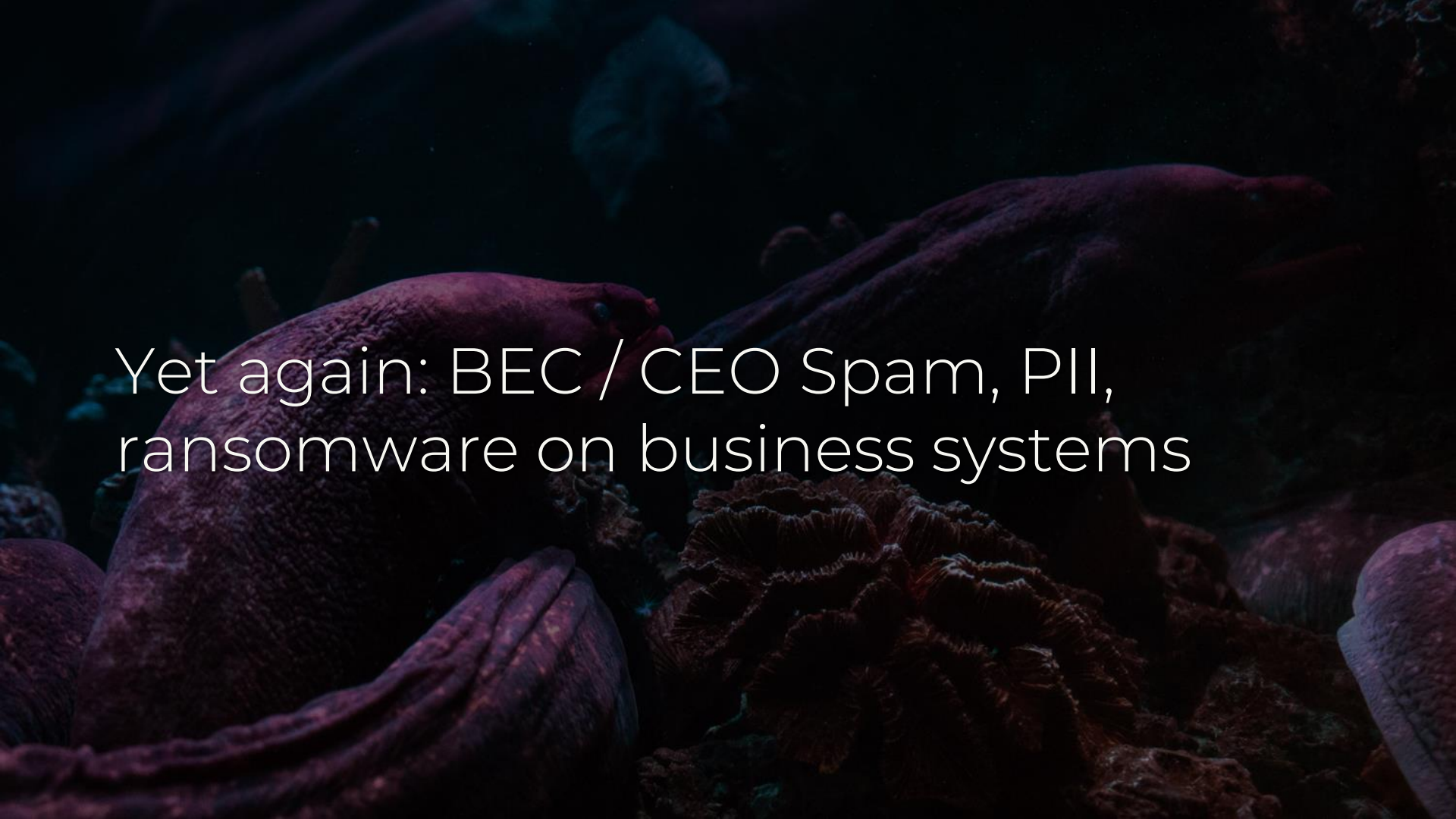
Step 1: What are the risks & predominant revenue sources?


Managing fluctuating demand,
avoiding service interruption


Hazardous materials, accidents, bad
weather, piracy, public health threats

Reliance on tech improvements to operations & biz operations

Step 2: What do attackers want?


Yet again: BEC / CEO Spam, PII,
ransomware on business systems

Transportation schedules can be used for theft or hijacking... but non-trivial

Drug orgs have redirected ships to gain containers for smuggling

Bridge systems: IBS or AIS theft, ECDIS misdirect… but non-trivial

Future opportunities: autonomous ships & ports, PTC, other automation


PTC is a security tire-fire – but you still must consider attacker ROI

Step 3: Where do Risk Factors & attacker goals align?

Security basics: email security, backups, network / comms resilience

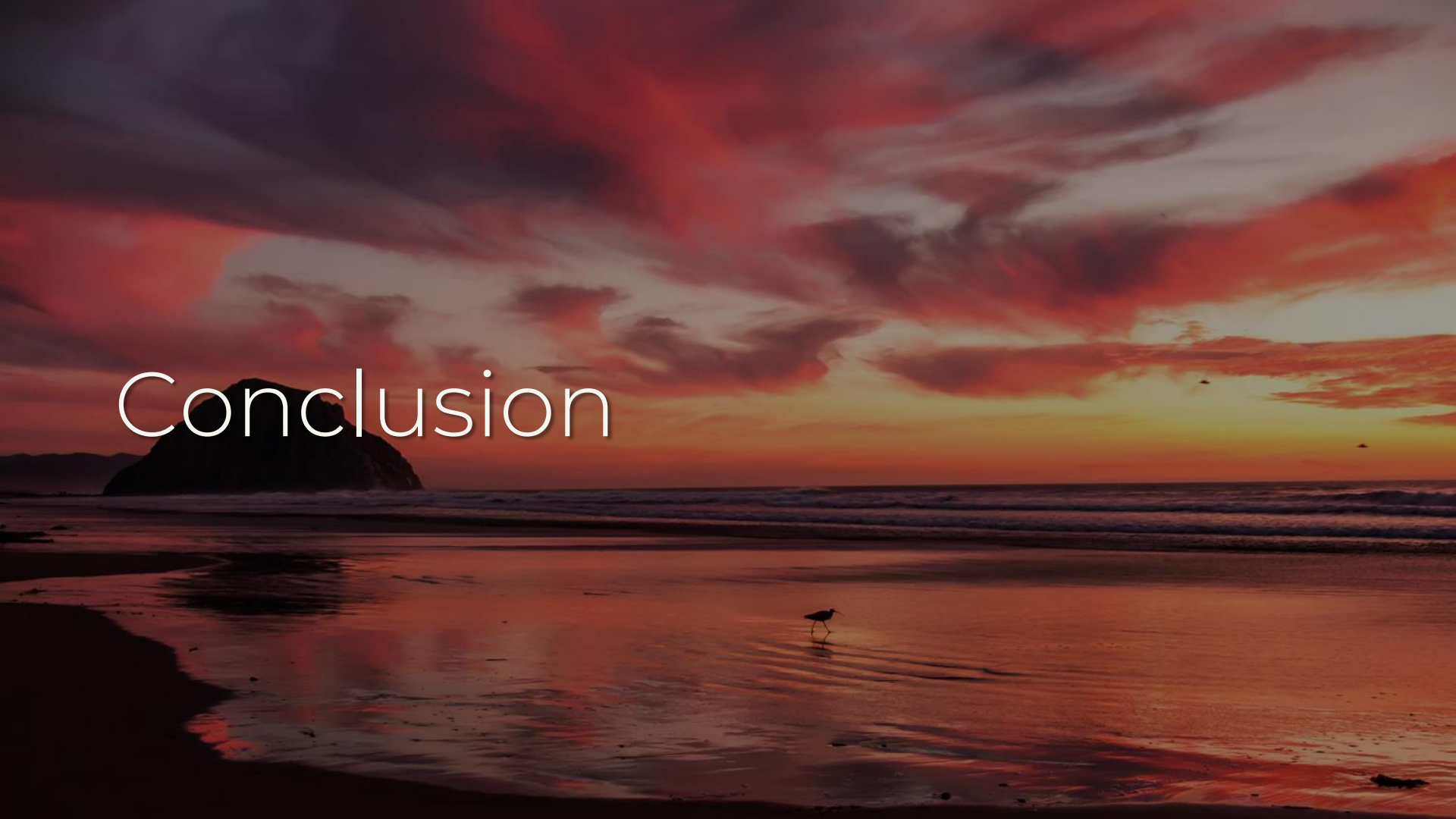
What is being insured by cyber insurance for transportation?


Physical damage is covered, except
sometimes in “war risks” (terrorism)

Time element expense, eg systems failure, without physical damage


Cargo coverage includes damage,
theft, misdirection, interruptions

Most data breaches involving PII are excluded, along with ransomware


Conclusion

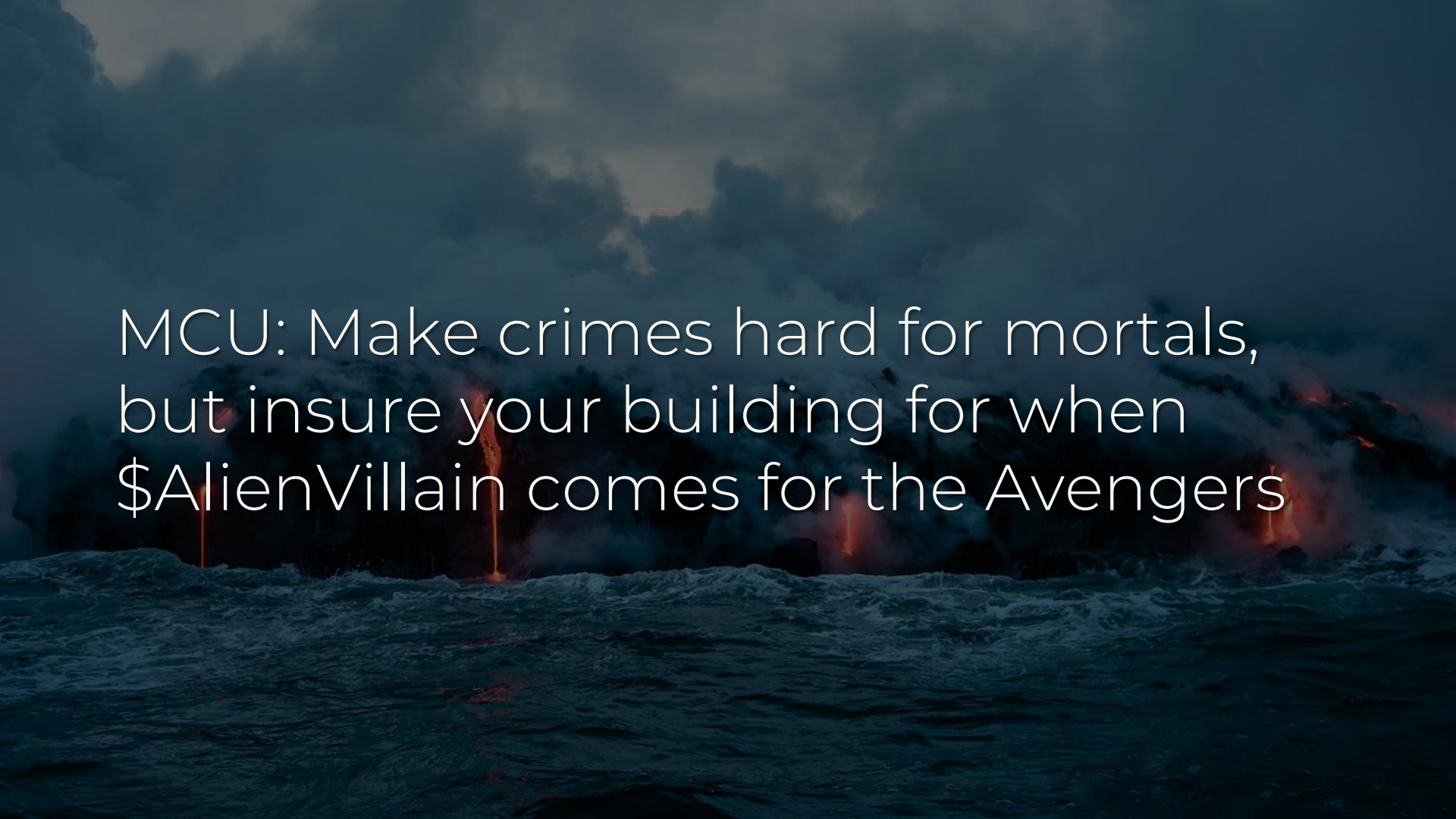

You don’t know better than your org
on what business risks exist

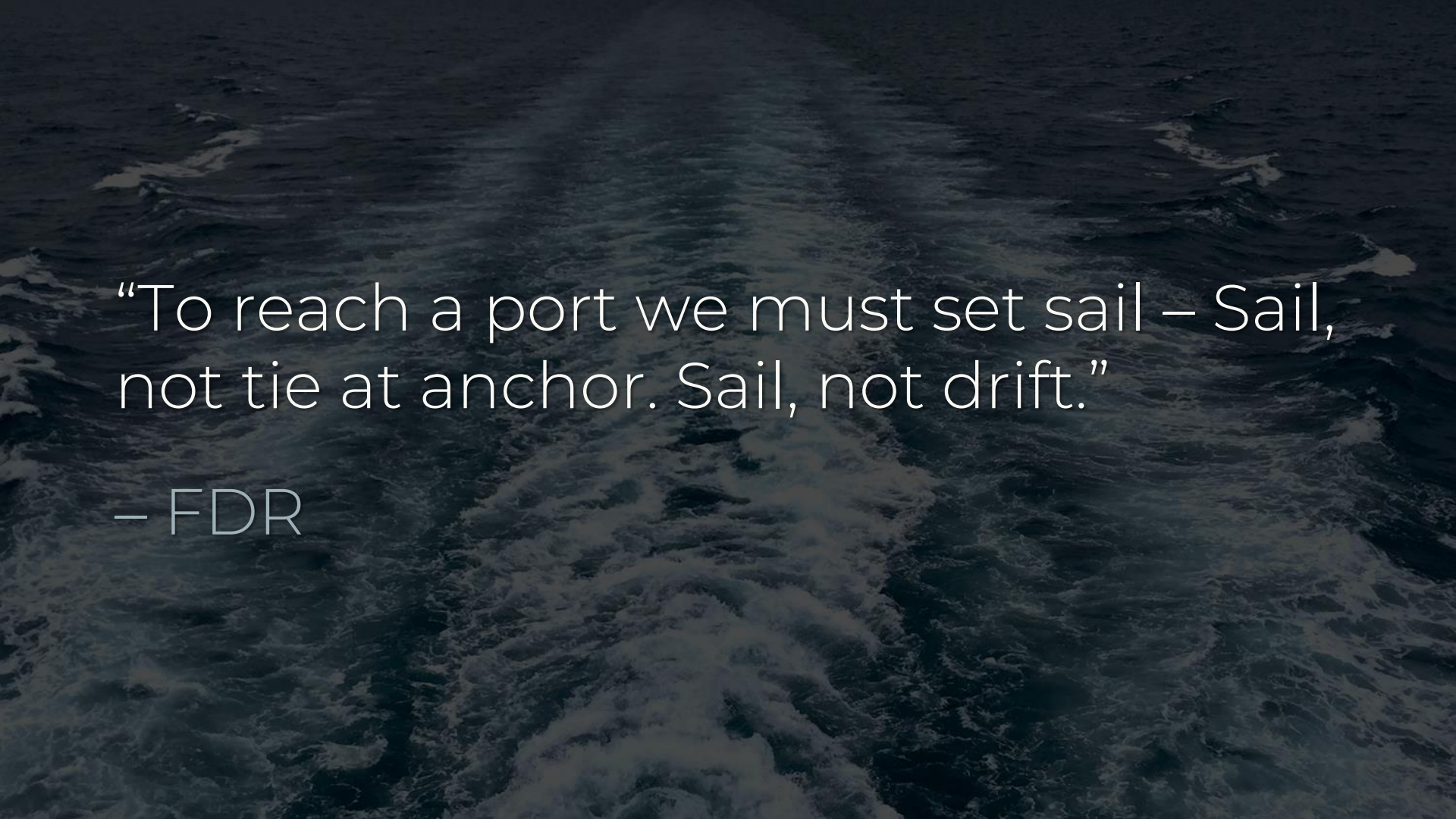

Free yourself from the burden of
defending against all threats


Where you can excel: how digital risks
can connect to your business risks


Identify where your org’s risks meet
what attackers actually want


Model how attackers most easily
reach their goals & make it harder


MCU: Make crimes hard for mortals, but insure your building for when $AlienVillain comes for the Avengers


“To reach a port we must set sail – Sail, not tie at anchor. Sail, not drift.”
– FDR

@swagitda_

/in/kellyshortridge

kelly@greywire.net