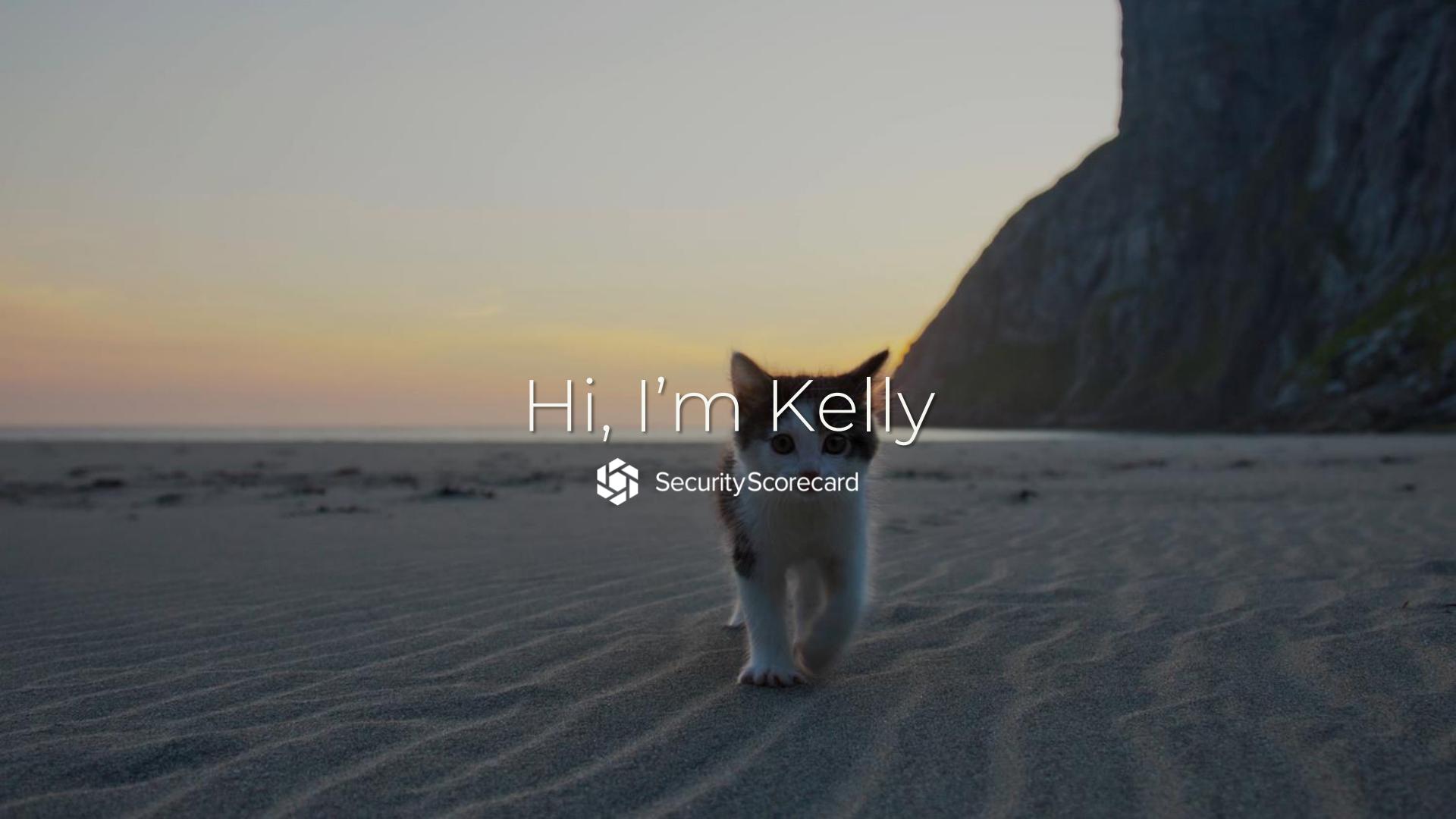


Threat Prioritization: Freeing the White Whale

A dramatic black and white photograph of a large white whale, possibly a humpback or whale shark, breaching the ocean surface. The whale's massive body is angled upwards, with its white underbelly and dark mottled skin clearly visible against the dark, textured water. The spray from its breach creates a sharp, white V-shape against the darker background.

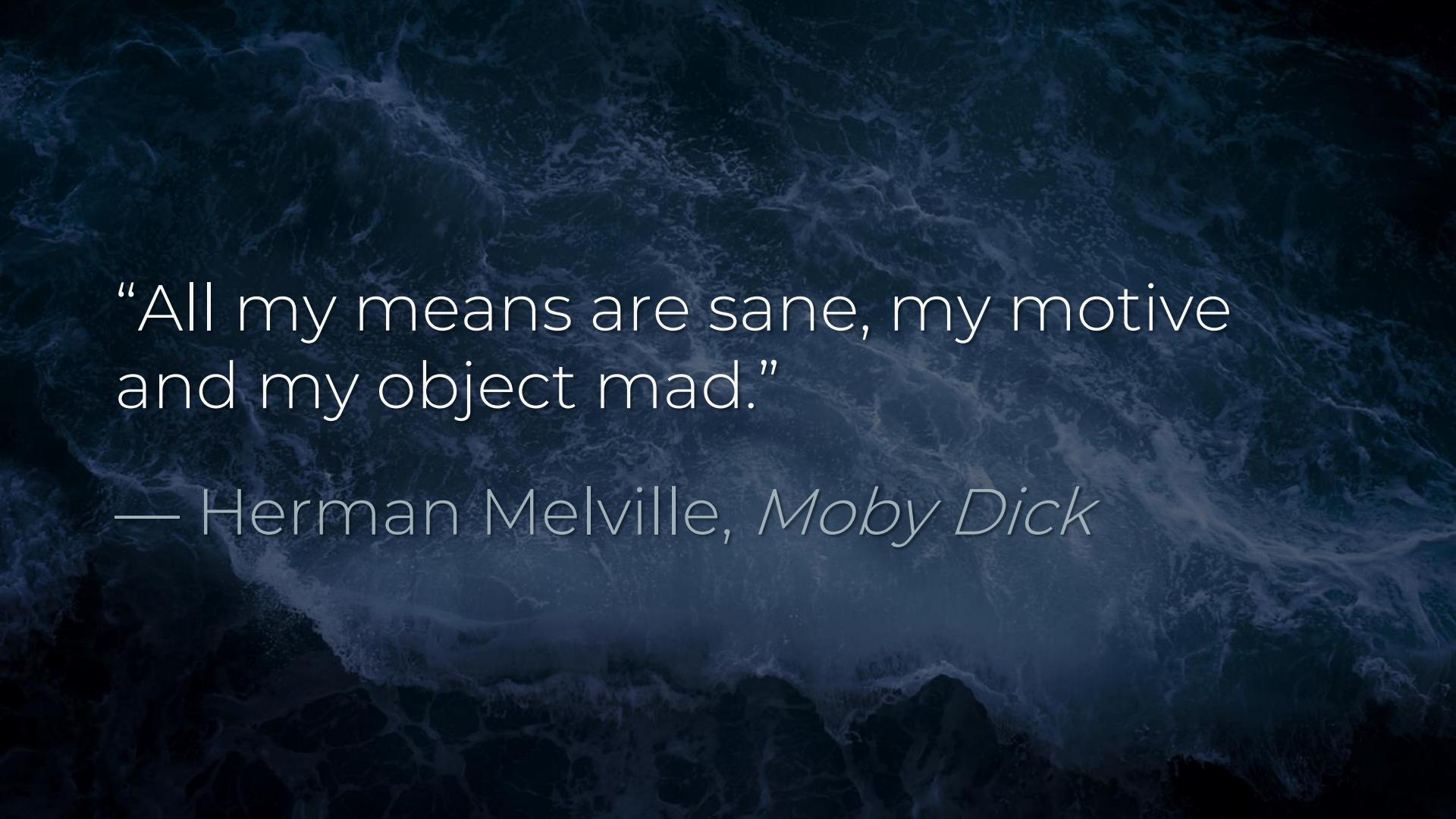
Kelly Shortridge (@swagitda_)
HackNYC 2018

A photograph of a white and brown cat sitting on a sandy beach. The cat is facing towards the left of the frame. In the background, there's a large, dark rock formation on the right and a sunset or sunrise sky with warm orange and yellow hues.

Hi, I'm Kelly

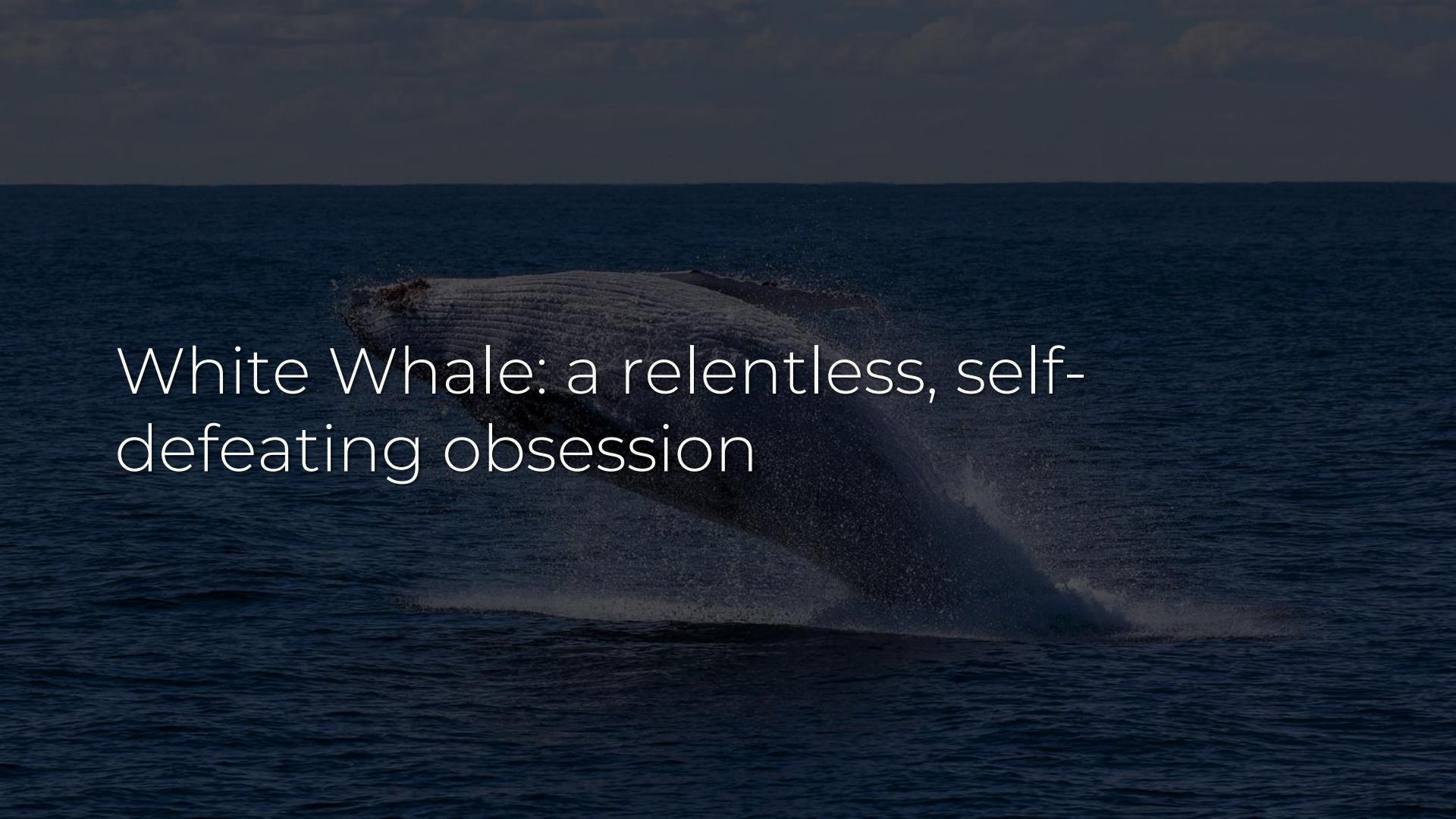


SecurityScorecard

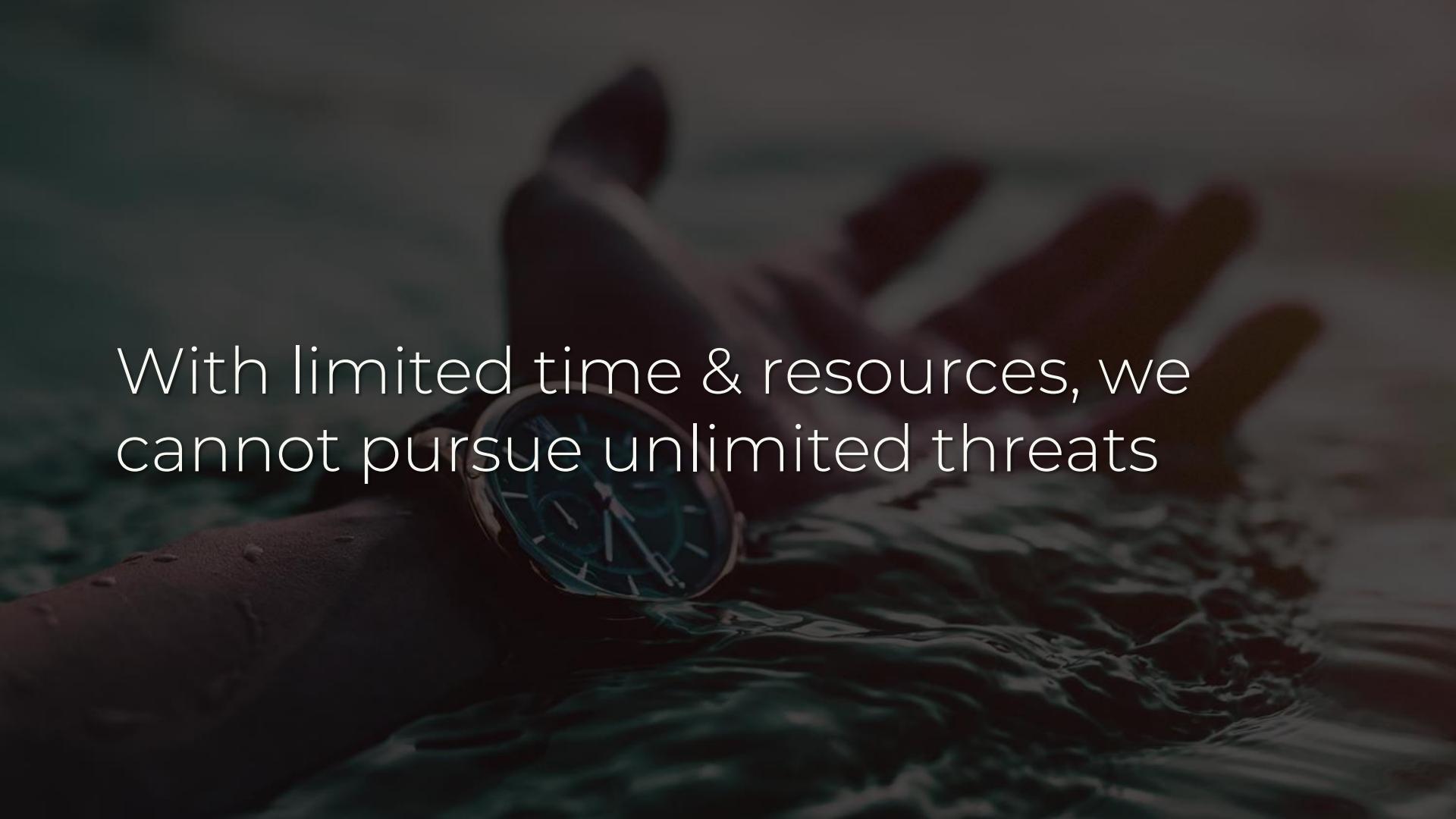
The background of the slide features a dark, textured image of ocean waves, with deep blues and blacks dominating the scene. The waves are highly detailed, showing white foam and spray at their crests, creating a sense of movement and depth.

“All my means are sane, my motive
and my object mad.”

— Herman Melville, *Moby Dick*

A dramatic photograph of a large white whale, possibly a humpback or sperm whale, breaching the dark blue ocean. The whale's body is arched high out of the water, with its white skin contrasting sharply against the deep sea. A massive, powerful splash of white foam and water erupts from its side, trailing off to the right. The background shows a dark, cloudy sky and the vast expanse of the ocean stretching to the horizon.

White Whale: a relentless, self-defeating obsession



With limited time & resources, we
cannot pursue unlimited threats

The background of the slide is a dark, moody photograph of the ocean. A shark is visible, swimming towards the right side of the frame. The water is a deep, translucent blue, with darker shadows at the bottom left and lighter, textured areas representing sunlight filtering through the water at the top right.

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

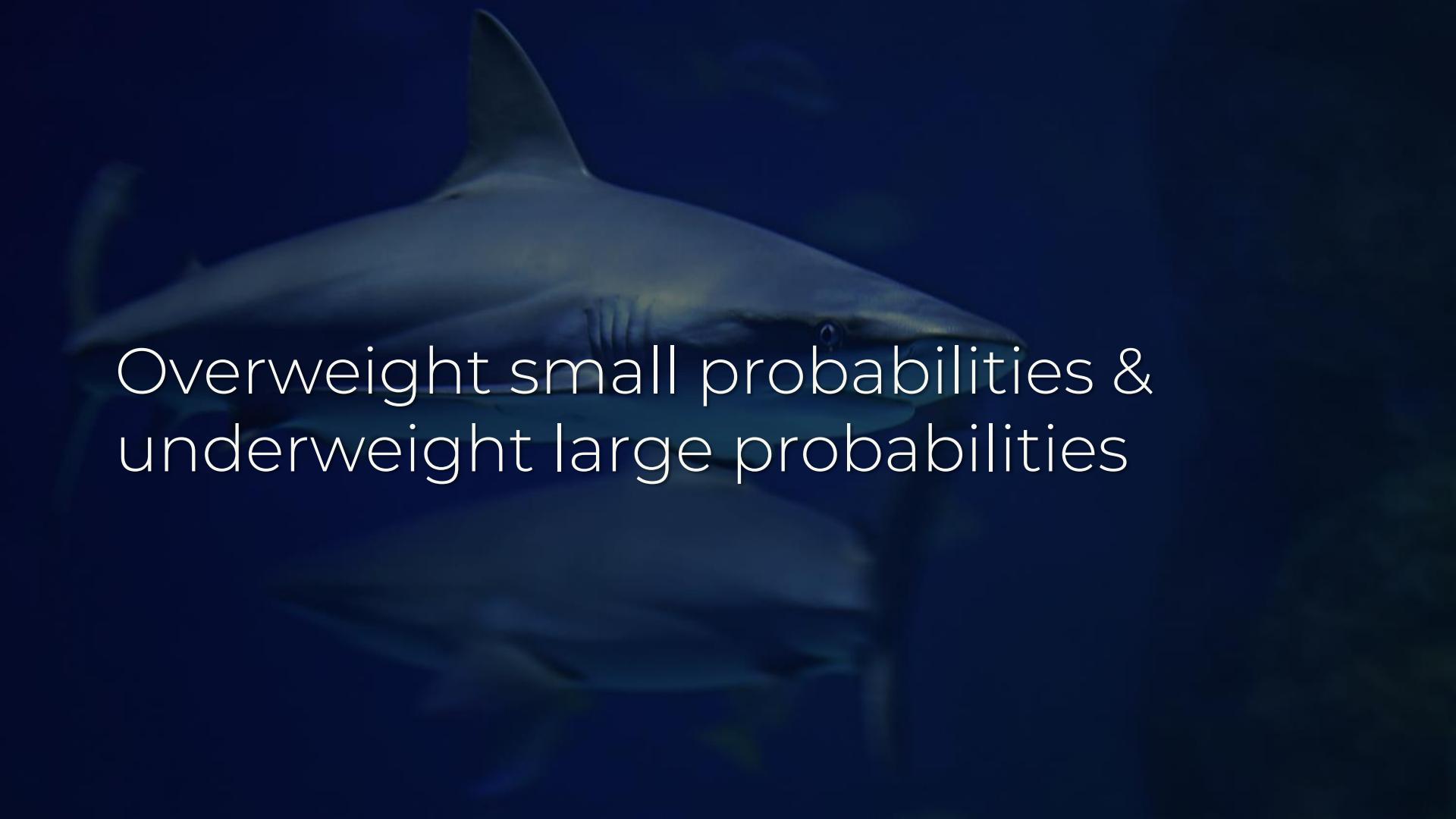
- 
1. Cognitive Biases
 2. Prioritization Framework
 3. Industry Examples



Cognitive Biases

Cognitive biases: we use subjective perceptions of inputs for decisions

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

A close-up photograph of a shark's head and upper body, swimming through dark blue, slightly rippled water. The shark's skin is a mottled grey-blue, and its eye is clearly visible. The lighting is low, creating a mysterious and somewhat foreboding atmosphere.

Overweight small probabilities &
underweight large probabilities

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

The background of the slide is a close-up photograph of a large school of fish, likely jacks or tuna, swimming in a dark, blue-green ocean. The fish are densely packed, filling most of the frame. They have silvery bodies with dark fins and tails. Their eyes are clearly visible, looking towards the camera. The lighting is somewhat dim, suggesting a deep sea environment.

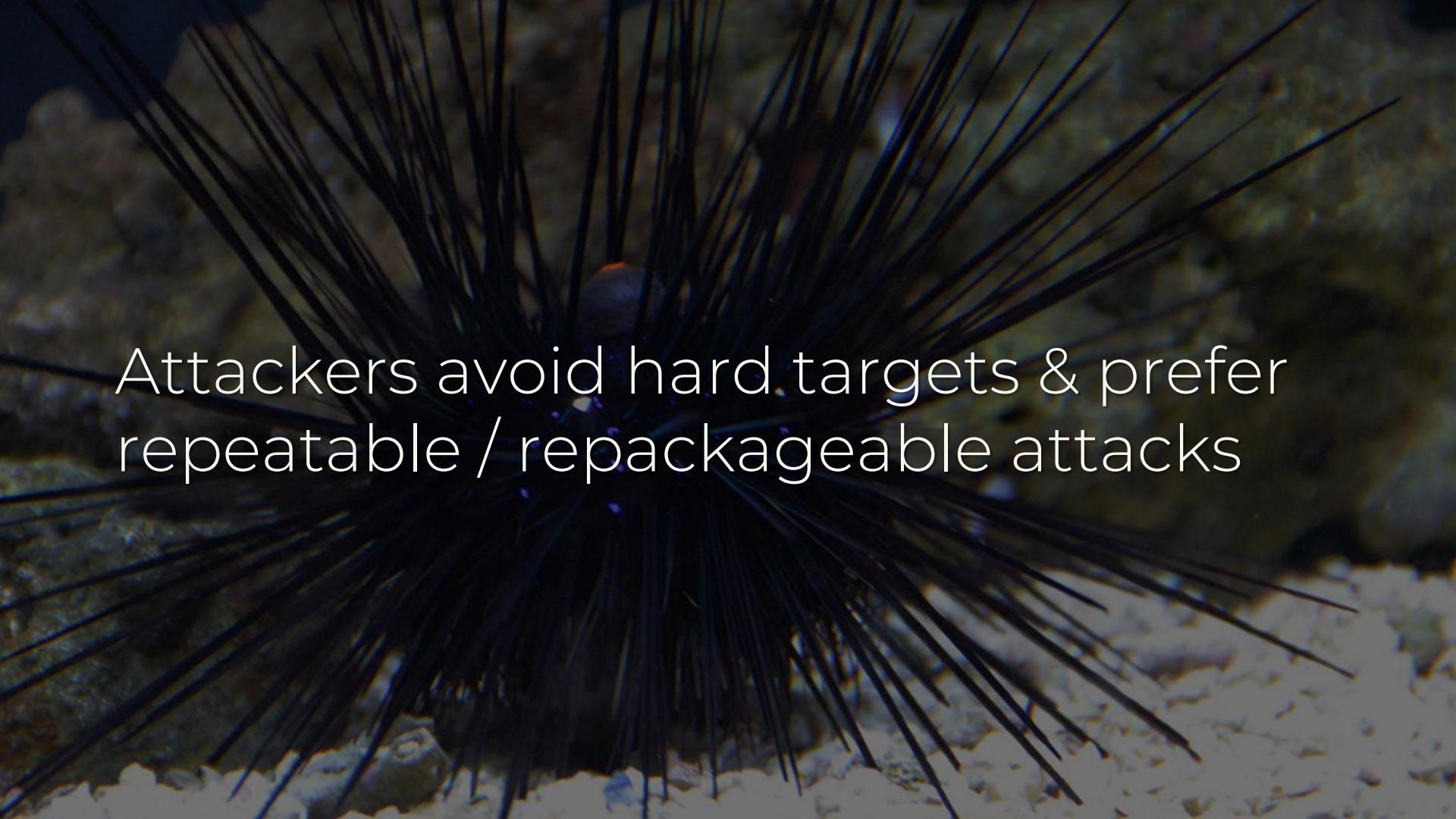
Super elite 0day (overweighted) vs.
phishing (underweighted)

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)

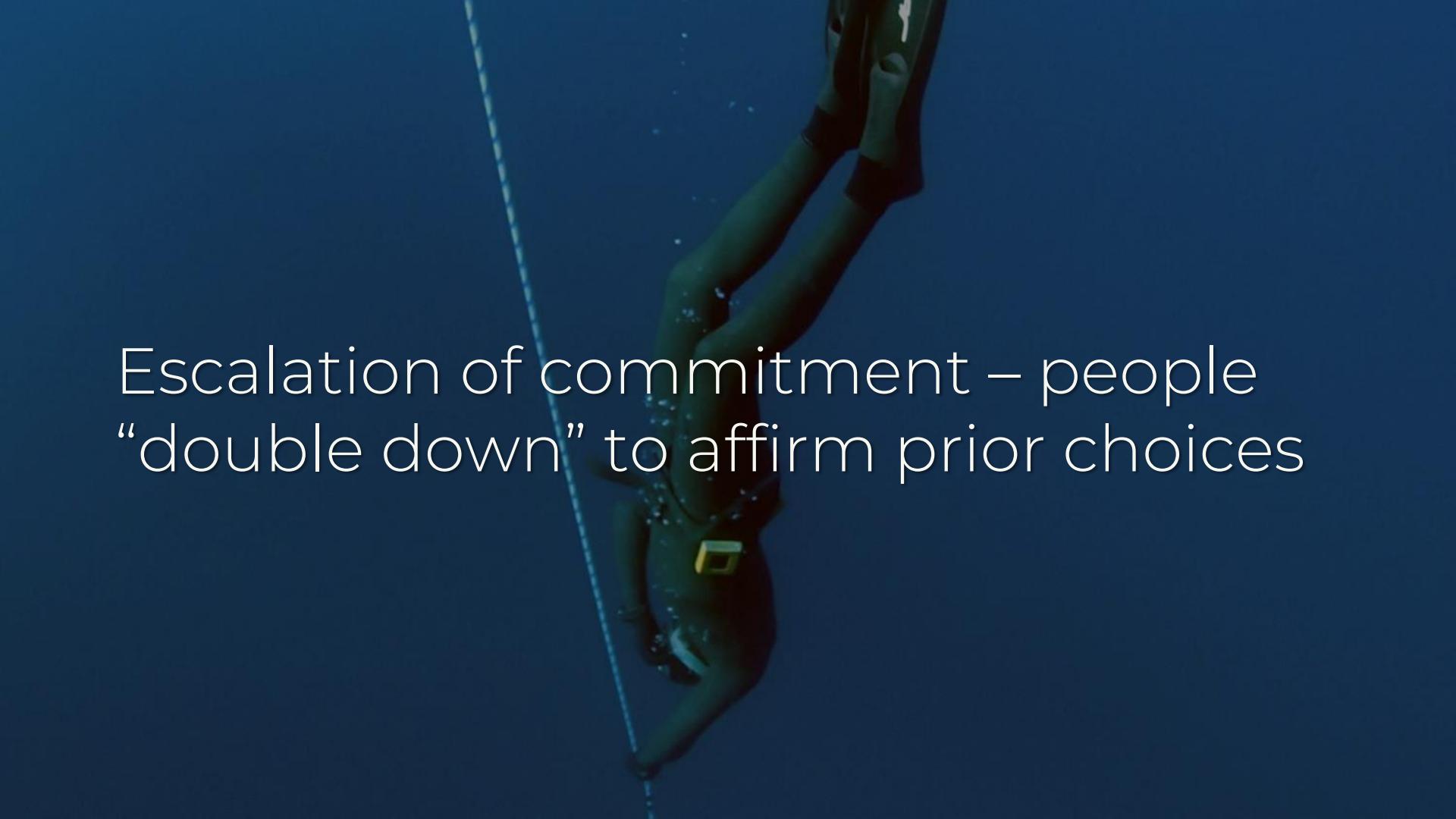


Availability heuristic – those headlines
about “Cybergeddon” influence you



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

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

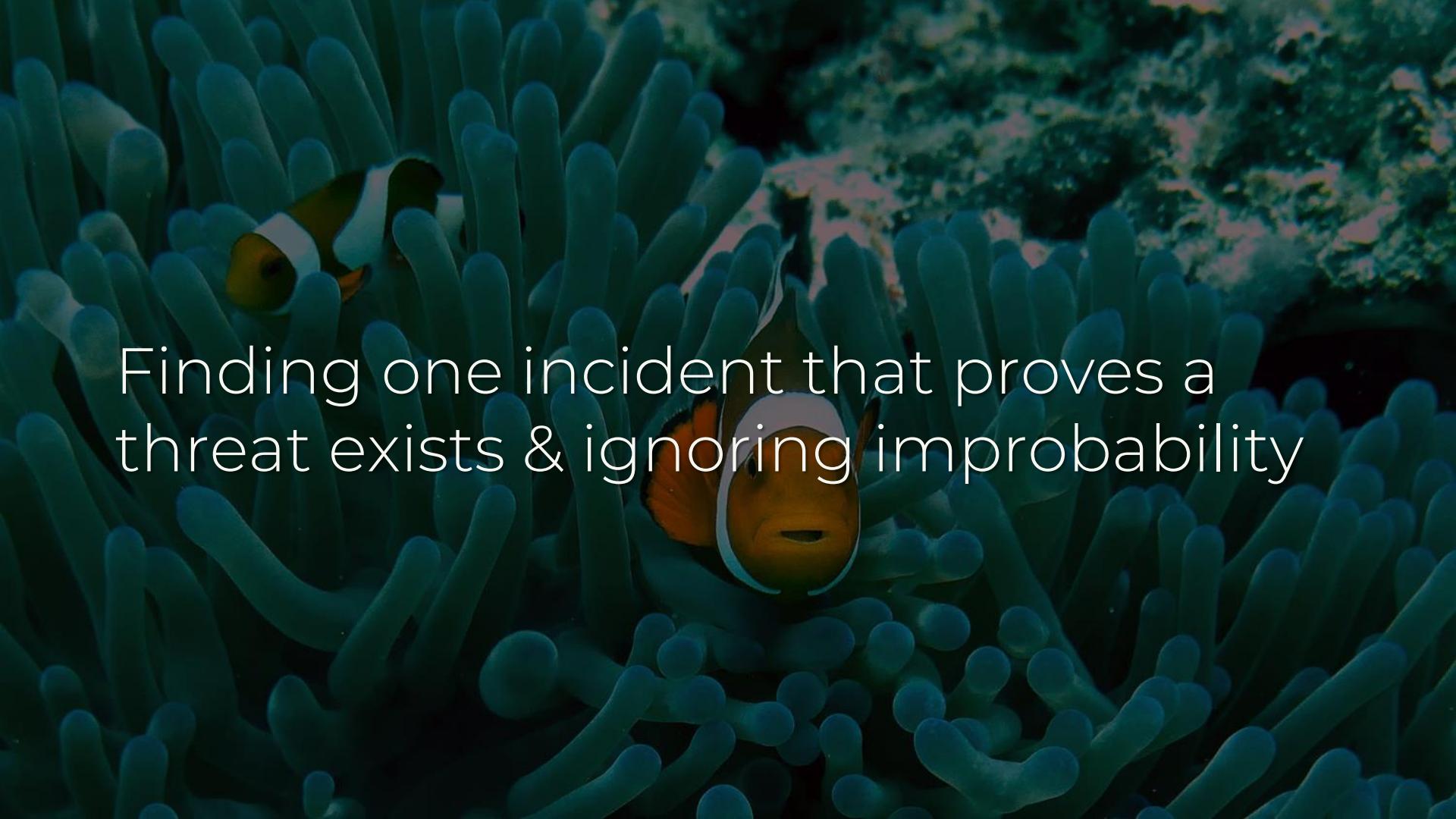
A diver in a dark blue suit and fins is suspended by a rope from a boat deck, looking down at the water.

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

A dark, semi-transparent background image showing several clownfish swimming among the tentacles of a large sea anemone. The clownfish are bright orange with white stripes, and the anemones have long, flowing tentacles.

Continuing to use strategies or
vendors with limited efficacy or ROSI

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

A close-up photograph of two clownfish swimming among the tentacles of a sea anemone. One fish is positioned higher up on the left, facing right, while the other is lower down on the right, facing left. The sea anemone's tentacles are a vibrant greenish-blue color.

Finding one incident that proves a threat exists & ignoring improbability

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



Prioritization Framework

The background image shows a close-up of a dark, polished rock or mineral specimen. It has a smooth, reflective surface with various shades of brown, tan, and black. Internal reflections and highlights create a metallic and somewhat iridescent appearance, similar to a polished metal or a gemstone like a pearl. The lighting is dramatic, coming from the side to emphasize the texture and depth of the material.

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

A close-up photograph of a starfish swimming in clear blue water. The starfish has five arms and a textured, reddish-brown body. It is positioned centrally in the frame, facing towards the left.

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)

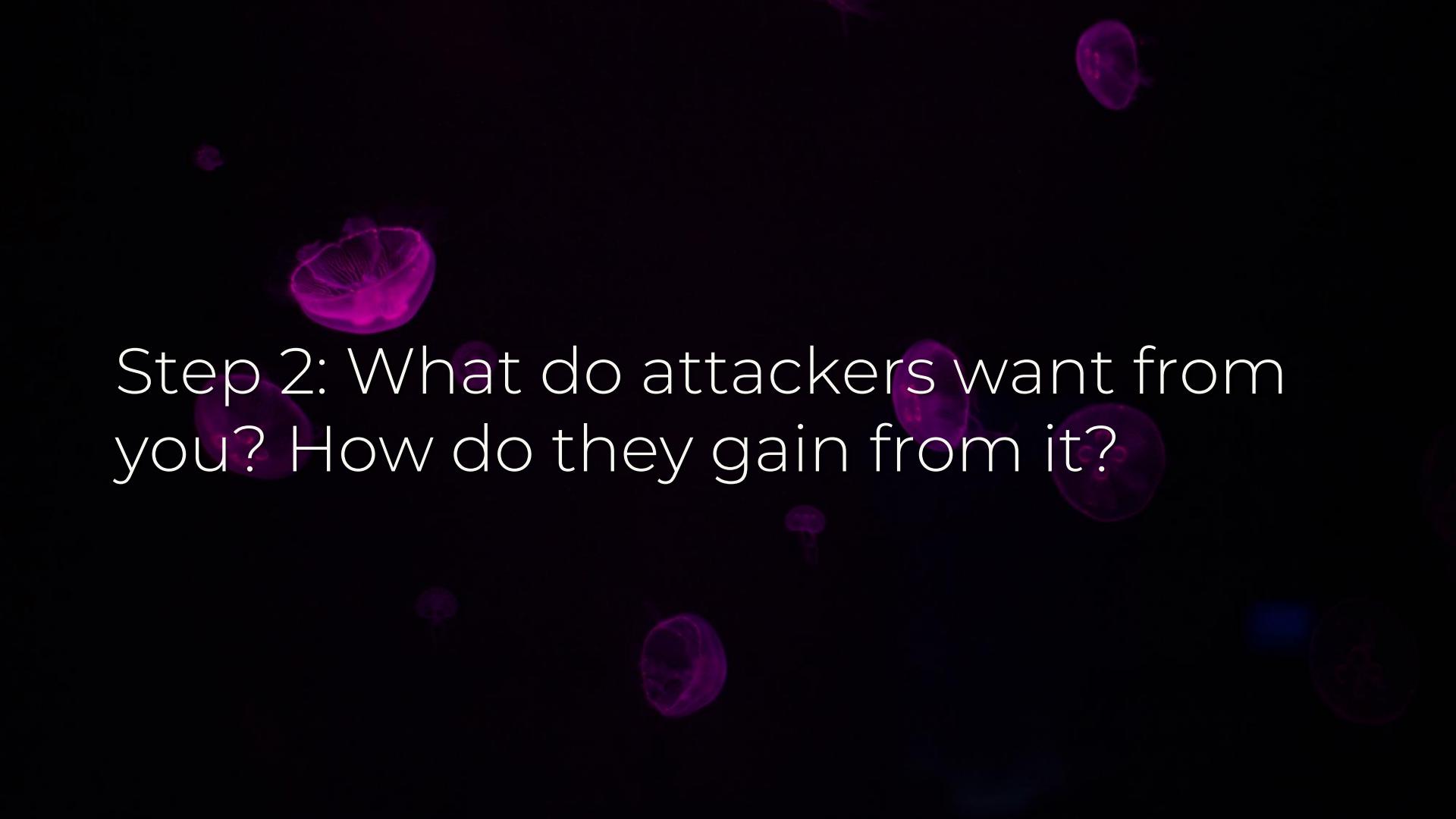
A large shark, possibly a hammerhead, swims through dark, slightly rippled water. The shark's body is angled downwards and to the right. The background is a deep, dark teal or black.

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

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

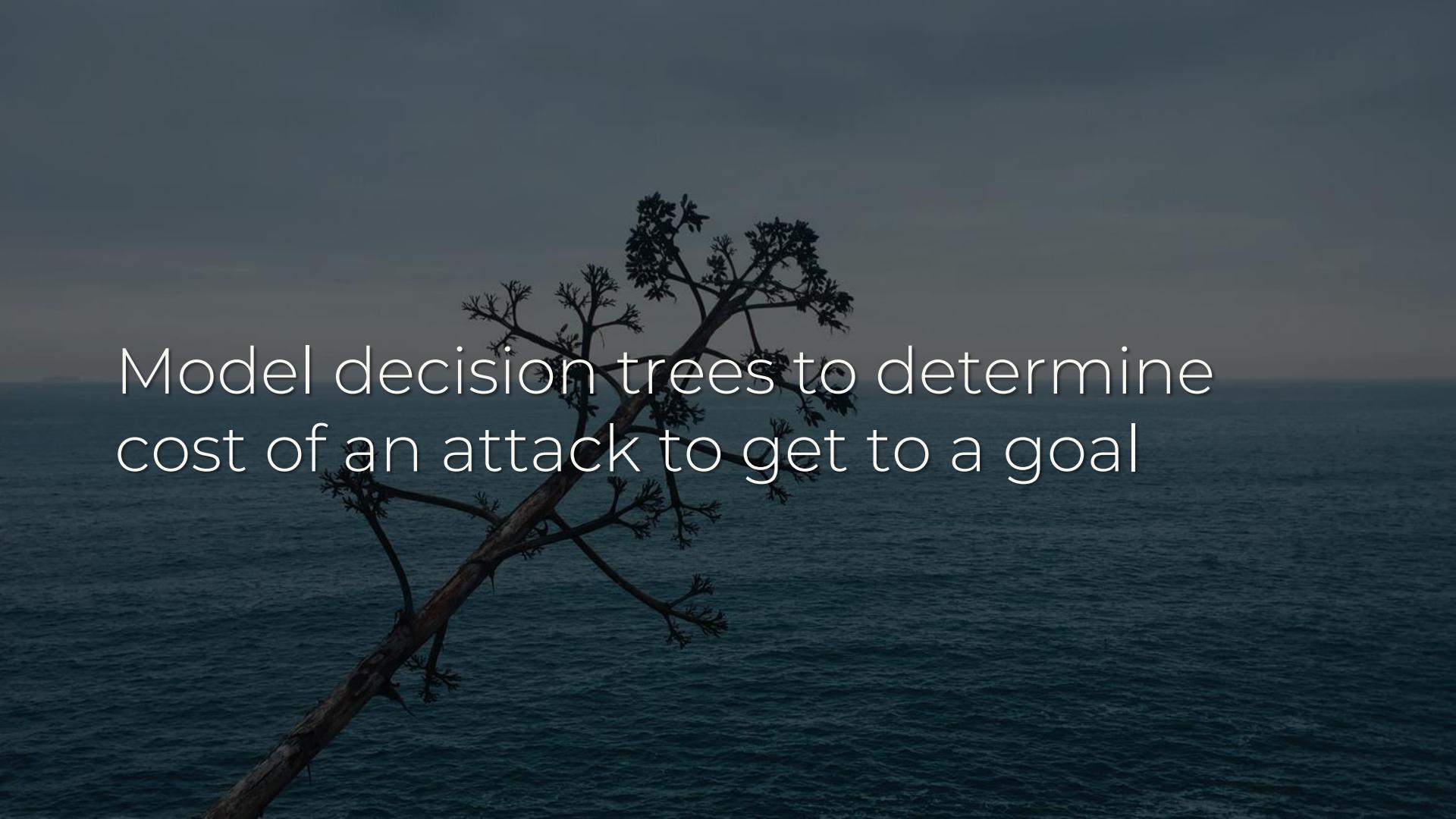
Read cyber insurance coverage for your industry, including exceptions

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

A dark, moody photograph of a tree branch silhouetted against a bright sky over a body of water. The branch curves from the bottom left towards the center, with clusters of small leaves or flowers at its tips. The background is a gradient from dark blue at the top to a lighter, hazy sky over a dark ocean.

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

A close-up, low-angle shot of turbulent, dark greenish-blue water. Numerous small, glowing white and blue particles, resembling bubbles or plankton, are scattered throughout the frame, creating a sense of depth and movement.

Step 3: Cross-compare results

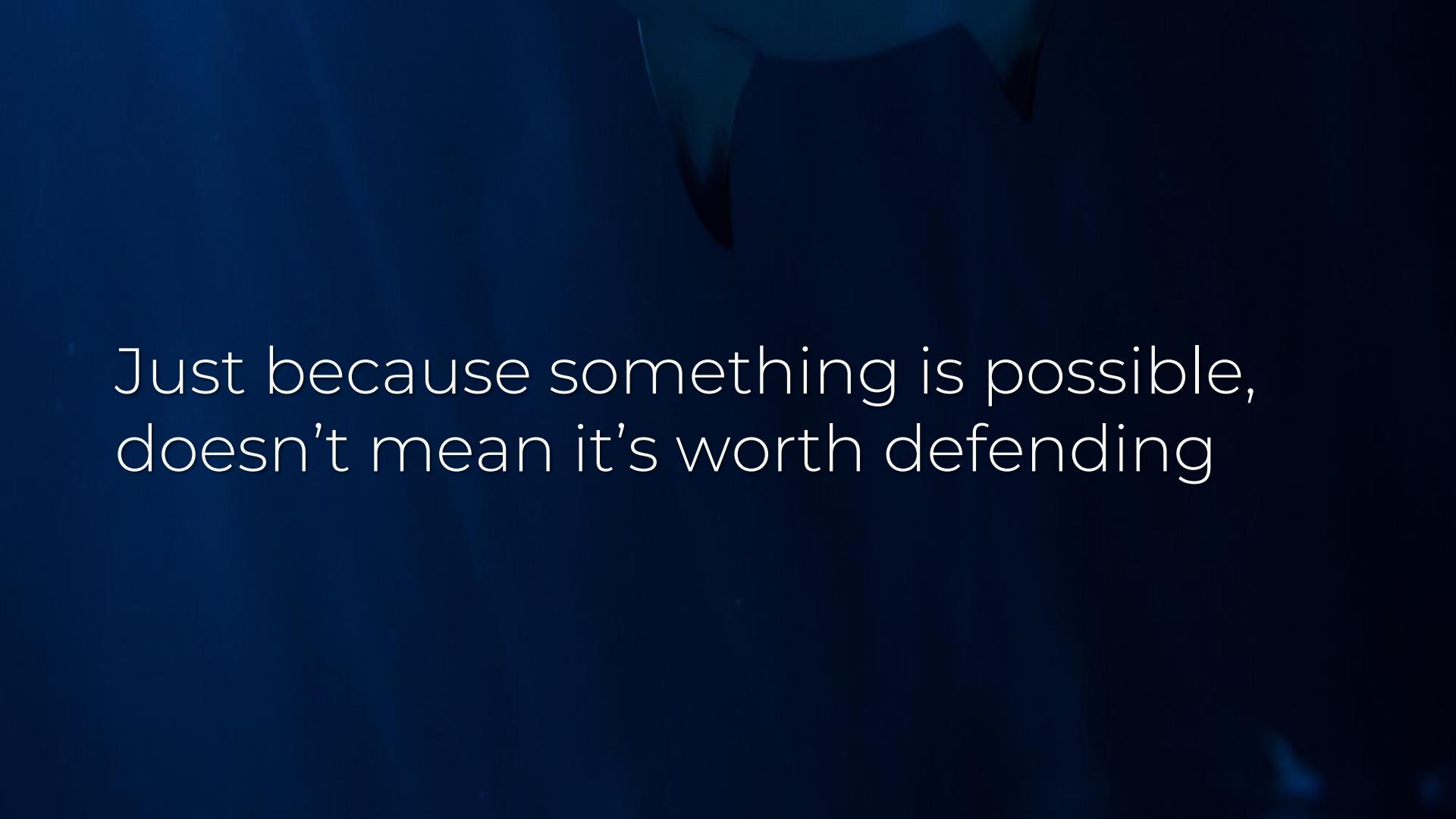


If you don't see *your* priority in Risk Factors, challenge your assumptions

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



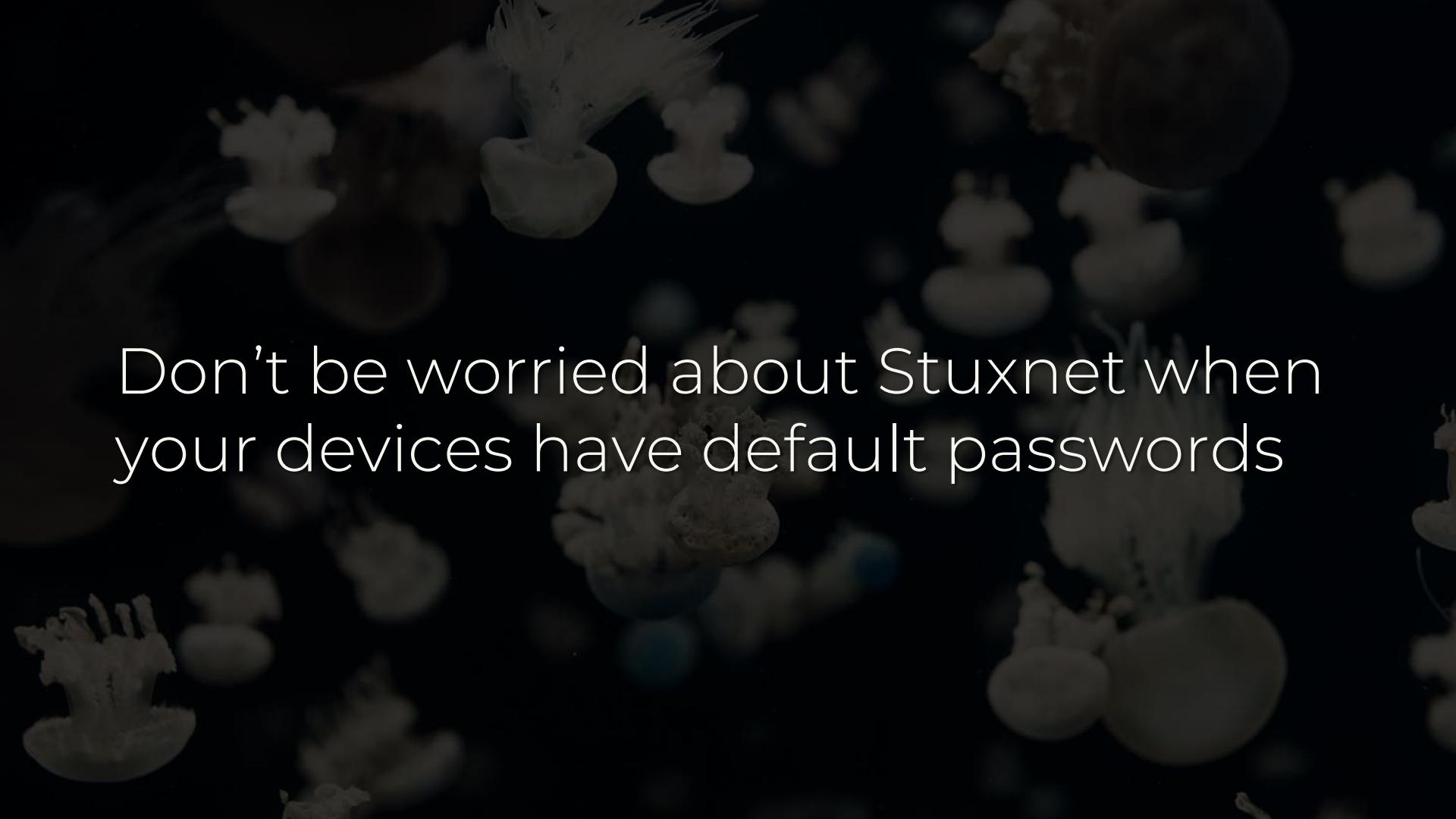
Just because something is possible,
doesn't mean it's worth defending



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

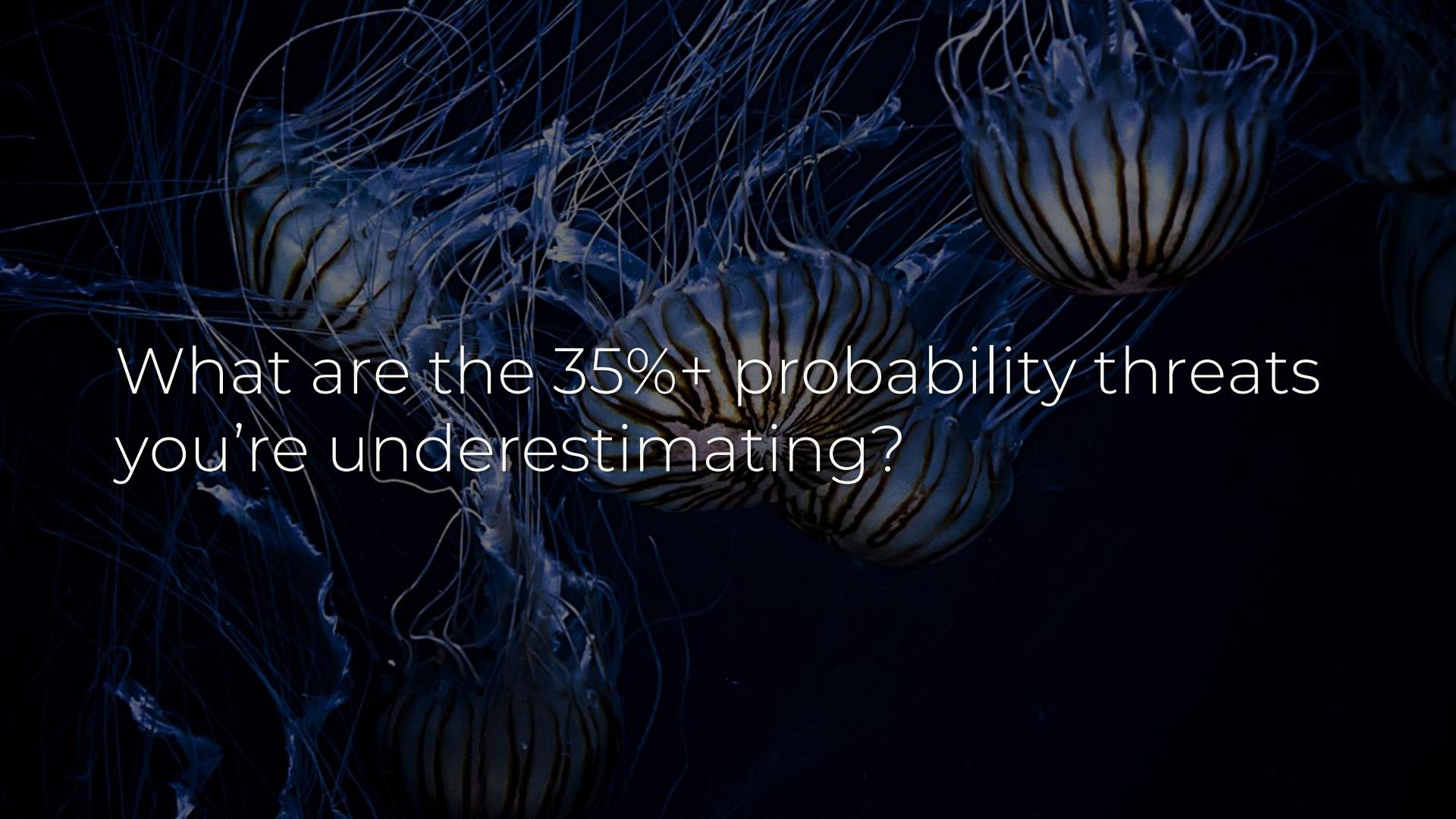
A large sea turtle is swimming in the ocean, its head above the surface. The water is a deep teal color. In the background, another turtle is visible, also swimming. The lighting is natural, coming from the surface of the water.

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



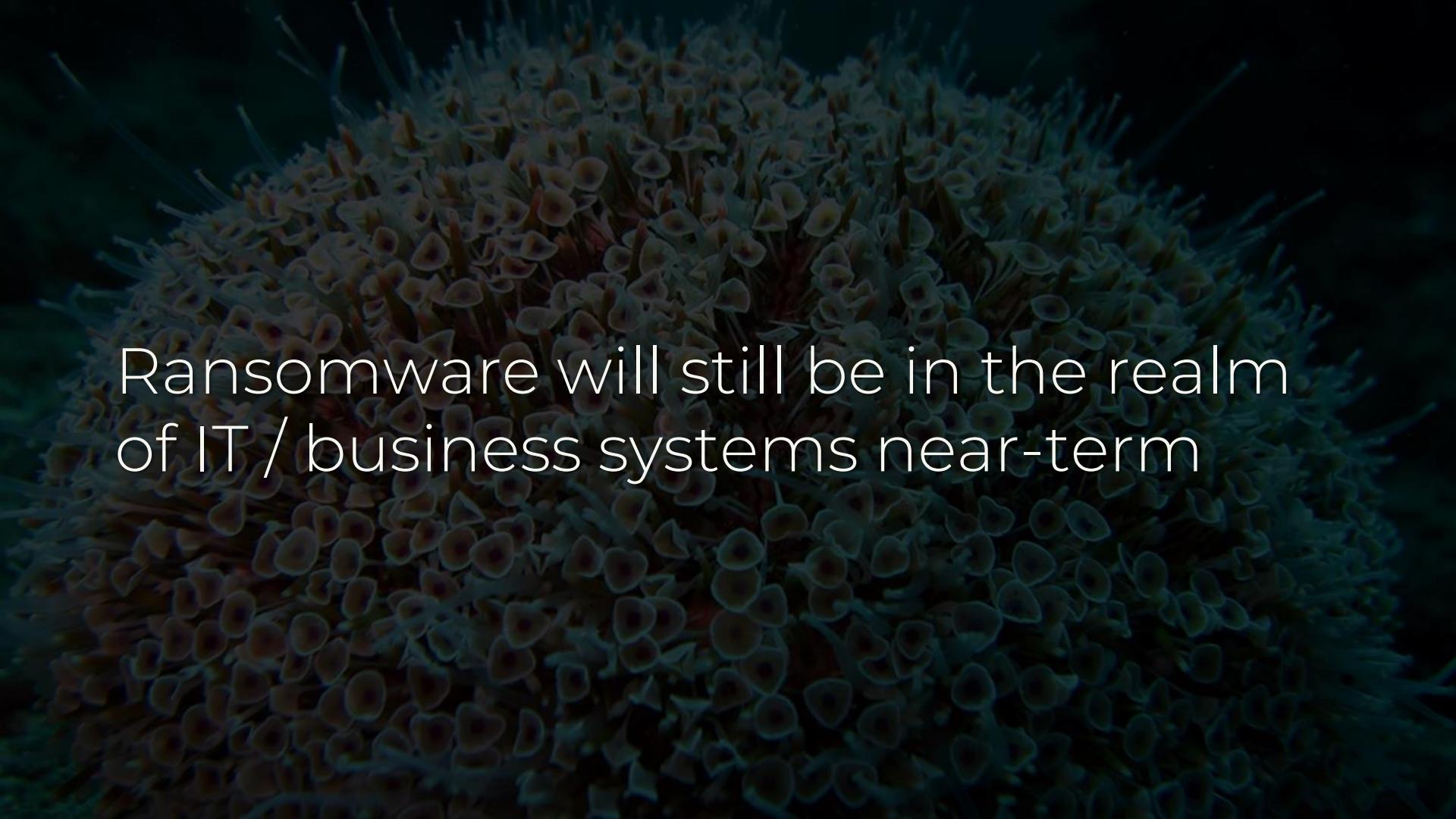
What are the 35%+ probability threats
you're underestimating?



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

A dramatic scene from the movie "The Leviathan". A massive whale is captured mid-leap, its dark body silhouetted against a bright spray of water. In the background, a smaller fish is also leaping, creating another splash. The ocean is dark and filled with white-capped waves.

DDoS attacks – spam or ransom

The background of the slide features a close-up photograph of a coral reef or anemone colony. The numerous tentacles or polyps are visible, creating a textured, organic pattern against a dark, moody background.

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

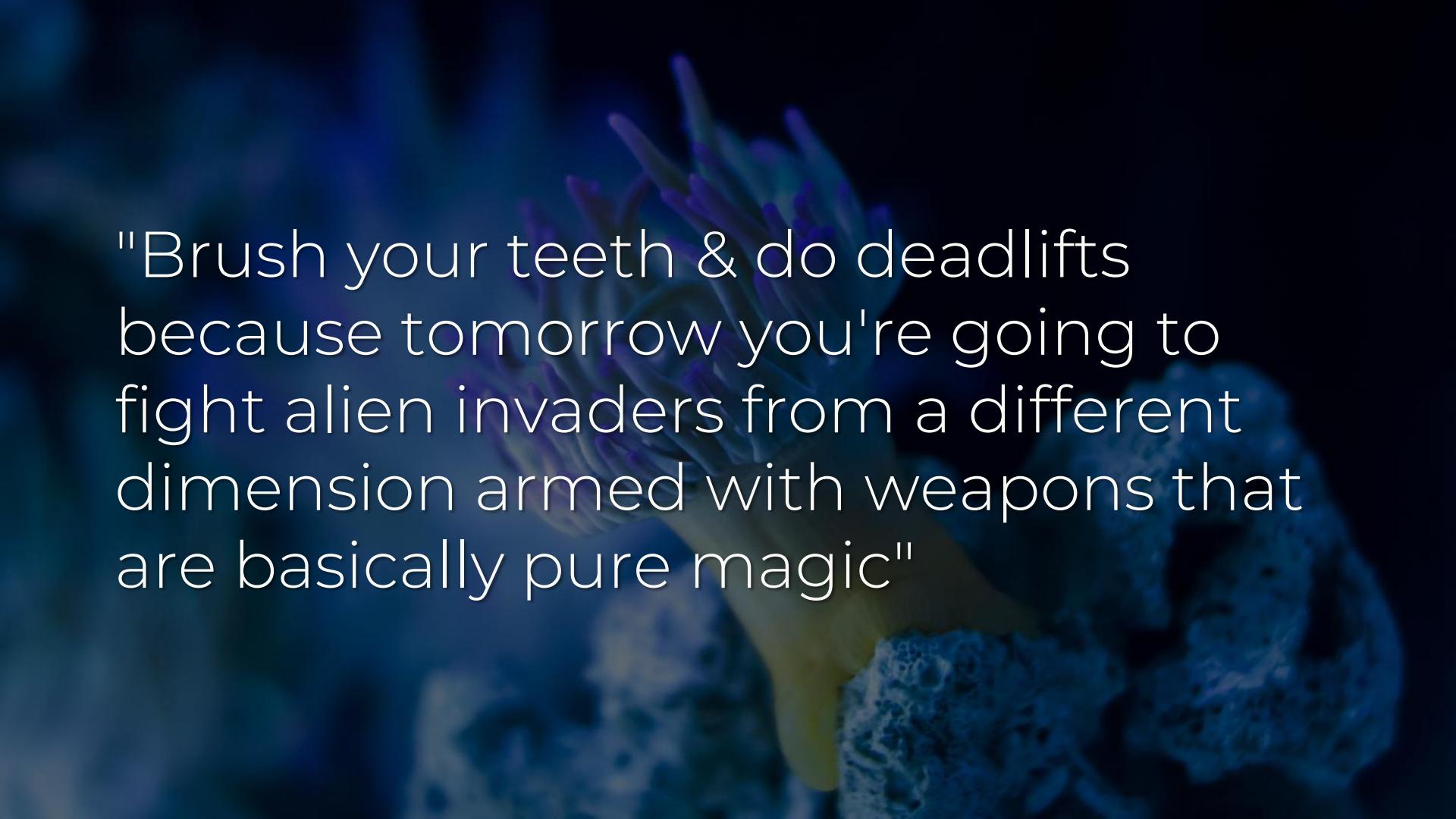
Time & resources required to port ransomware to OT = poor ROI

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

The background of the slide is a dark, textured blue, resembling the surface of the ocean at night. In the upper right quadrant, a single flying fish is captured mid-leap, its body arched as it cuts through the dark water. The ocean's surface is filled with small, white-capped waves. In the lower left corner, there's a faint, glowing outline of a coastal city or town, with numerous small lights visible along its coastline.

Operational efficiency is seen as a
competitive advantage now

Project management: negotiations,
development, optimization

Tech: operational unavailability,
inefficiency, or disruption

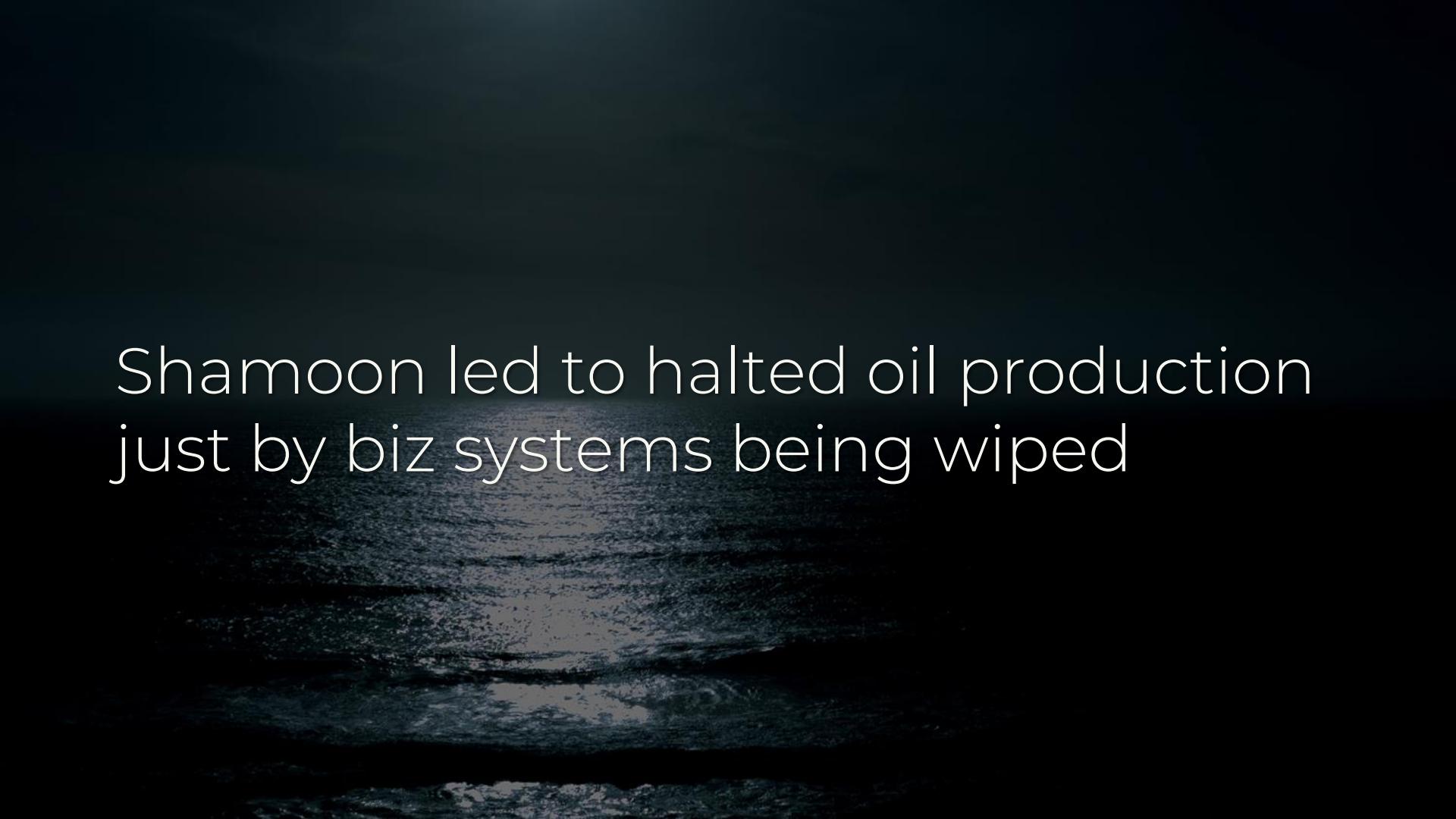
Infosec: physical harm, asset damage,
op disruption, biz system compromise

A large offshore oil rig is silhouetted against a dark, hazy sky. The rig's complex metal structure, including its derrick and various platforms, is visible. It stands in a body of water, with distant land or hills visible in the background.

Oil rig = >\$500mm

Refinery = \$5bn - \$15bn

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

A dark, grainy photograph showing an industrial facility, likely an oil rig, at night. The scene is mostly in shadow, with some lights reflecting off the water in the foreground.

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

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

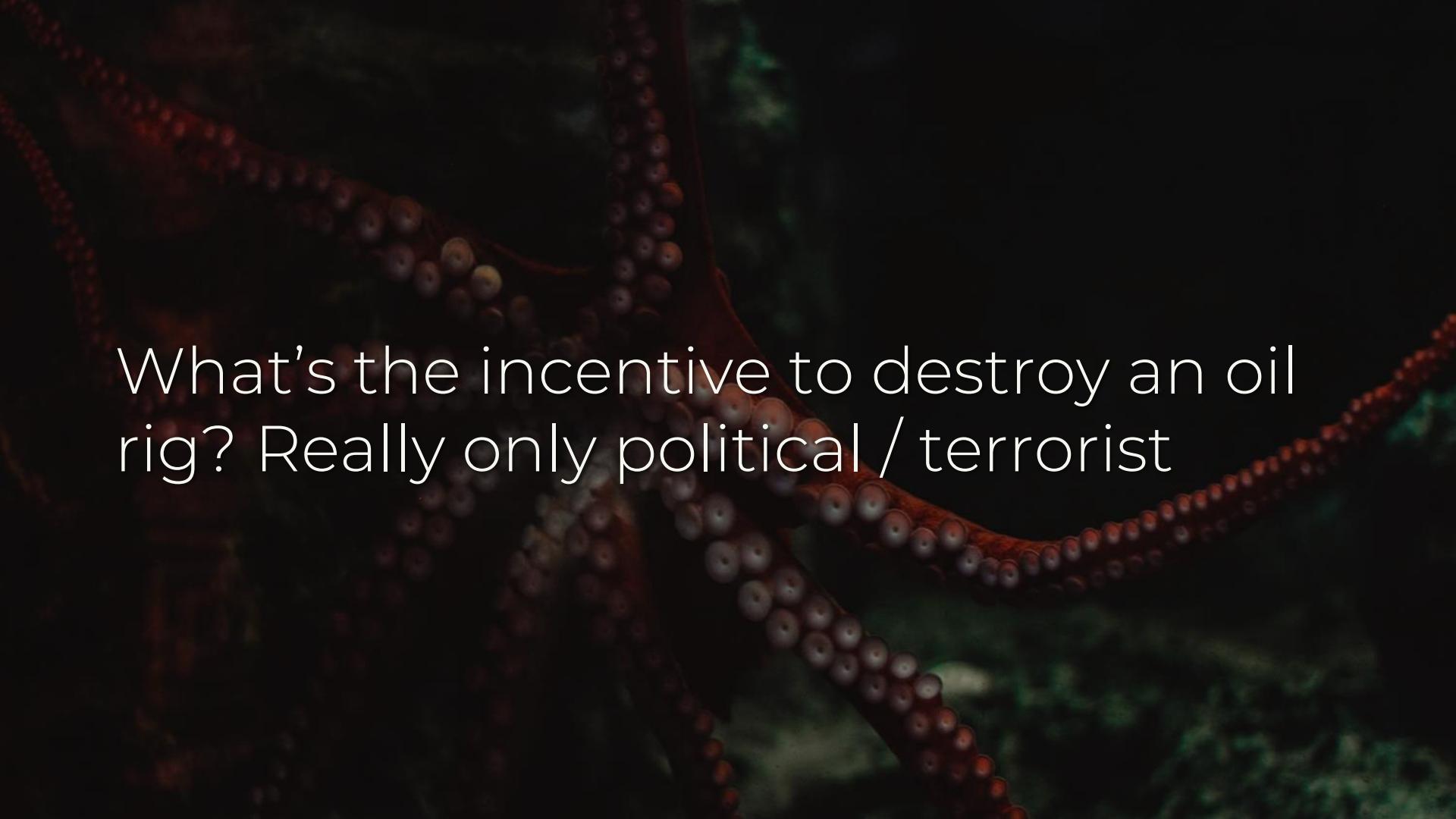
What is being insured by cyber insurance for oil & gas?

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?



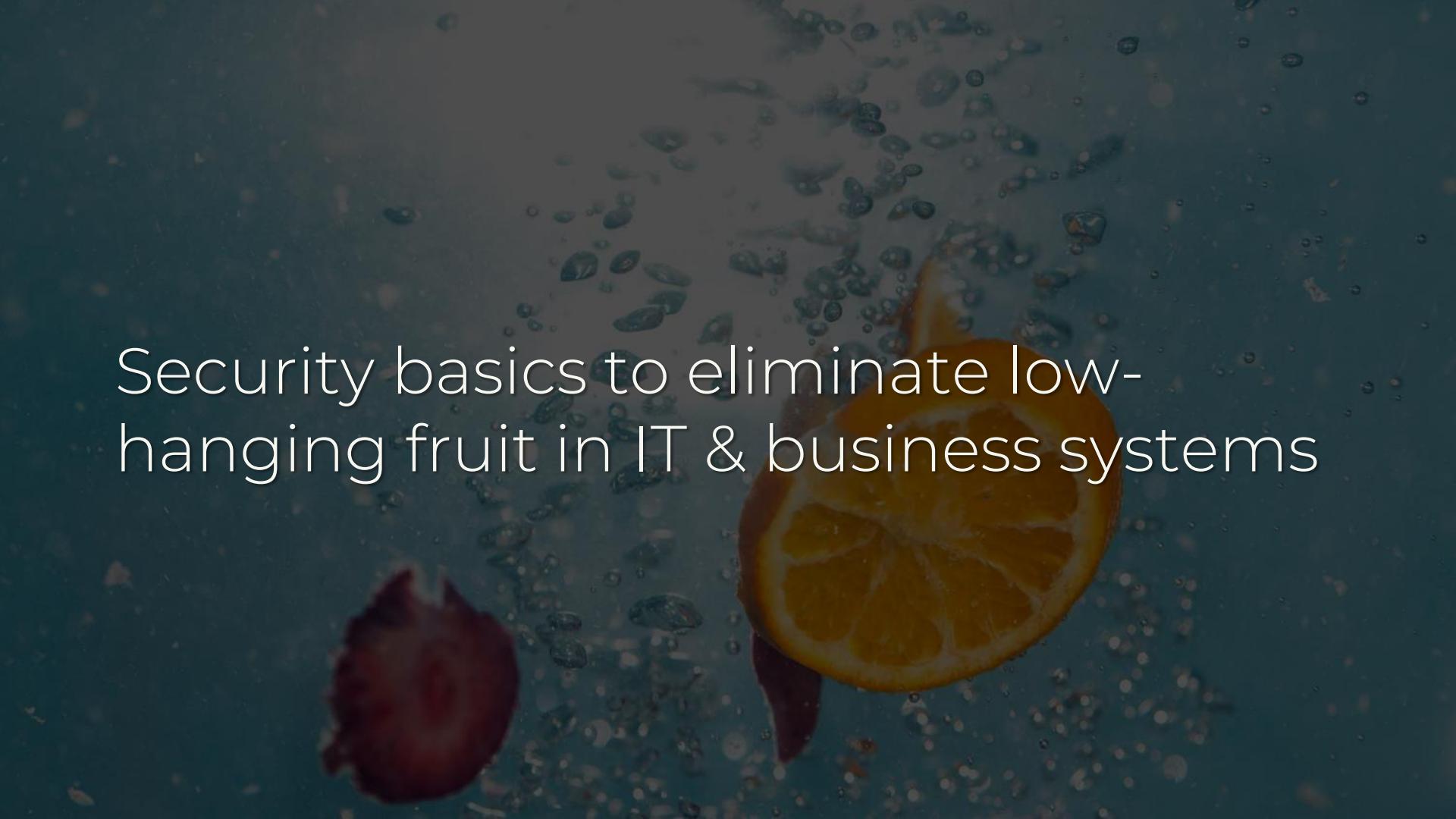
What's the incentive to destroy an oil rig? Really only political / terrorist

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?

A close-up photograph of two oranges partially submerged in water. One orange is visible in the foreground on the left, and another is in the center-right. Numerous small, translucent bubbles are scattered throughout the water, creating a sense of depth and texture.

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

Insurance, redundancy, & serenity
prayer for physical assets

A tall utility pole stands prominently against a dark, star-filled night sky. The pole is dark and silhouetted, with several horizontal cross-arms supporting multiple power lines that fan out across the frame. In the lower-left foreground, the word "Telecom" is written in a large, white, sans-serif font. The background is a deep navy blue, filled with numerous small white stars of varying brightness.

Telecom

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

Uptime requirements, network disruption, service interruptions

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

A close-up, low-angle shot of a large elephant's head and trunk. The elephant's skin is dark and textured with wrinkles. Its trunk is curled slightly. The background is dark and out of focus.

Telecom companies = slow-moving,
curious creatures

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

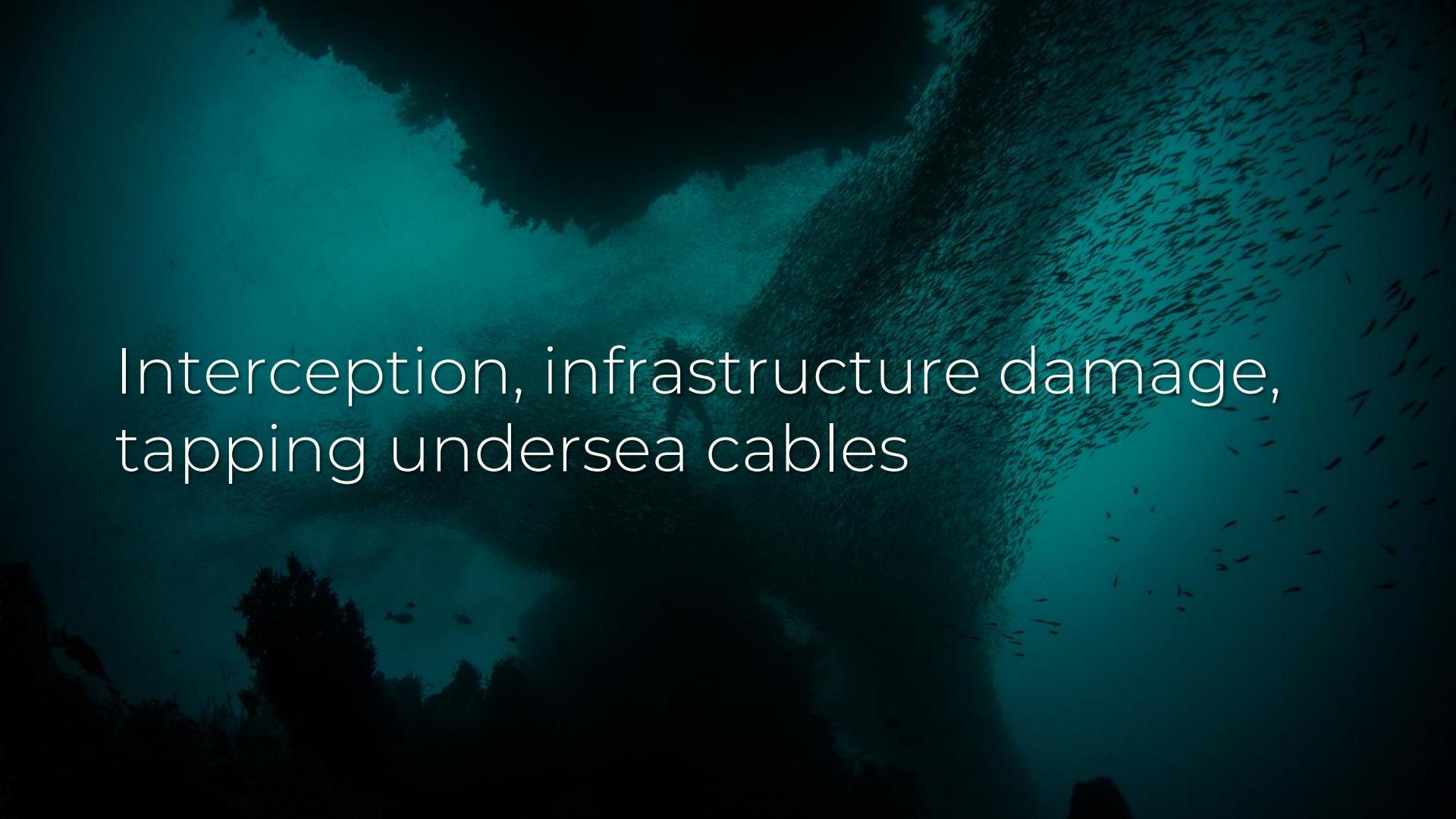
GDPR means PII may matter – privacy
hasn't been economical before



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

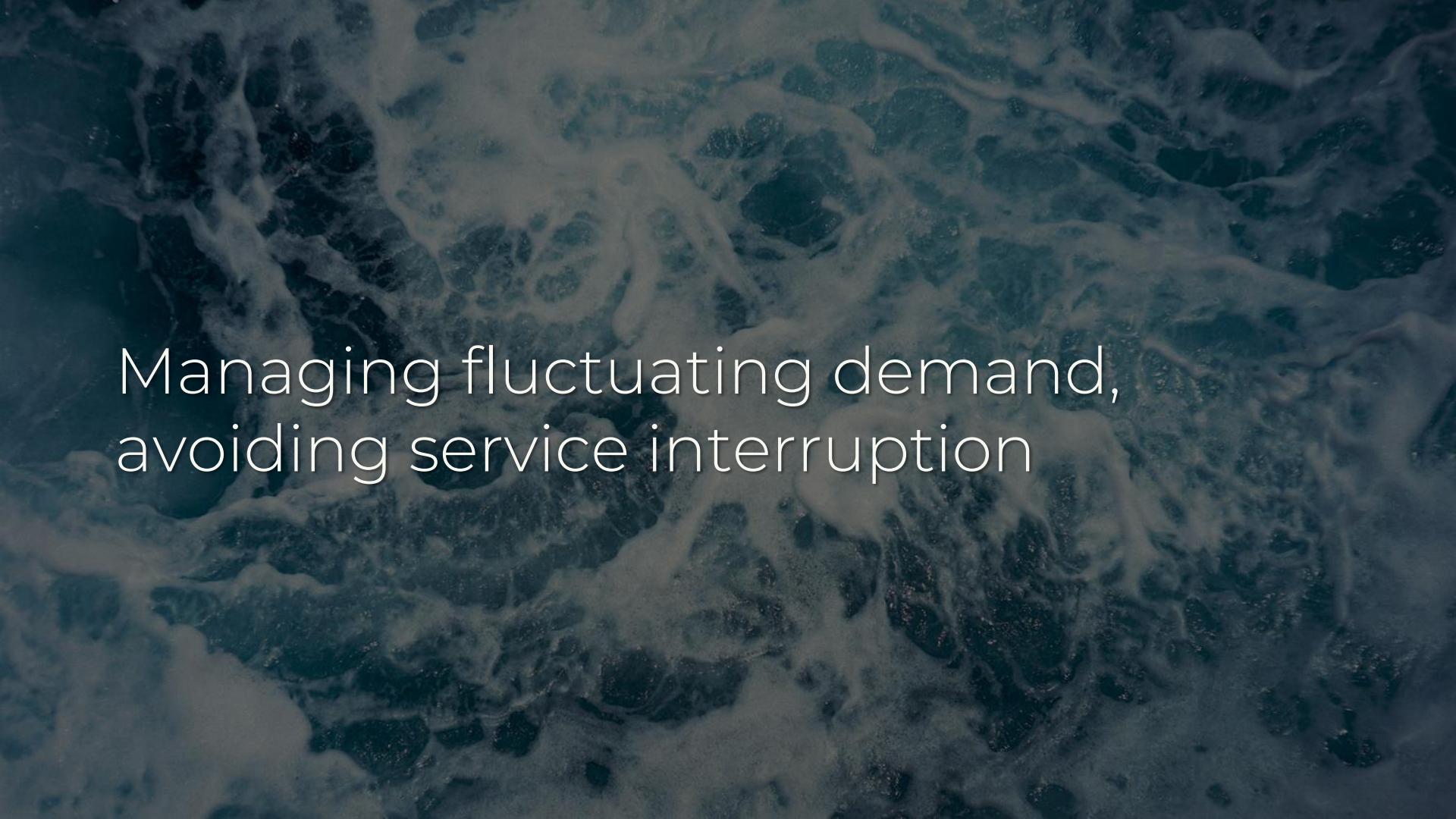
Step 3: Where do Risk Factors & attacker goals align?

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

Transportation



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

The background of the slide is a dark, grainy aerial photograph of a river system. The river flows from the bottom left towards the top right, creating a complex network of white-water rapids and calm, brownish-green pools. The surrounding land is heavily forested, with dark green trees that appear as a dense, textured pattern against the lighter water. The overall mood is mysterious and organic.

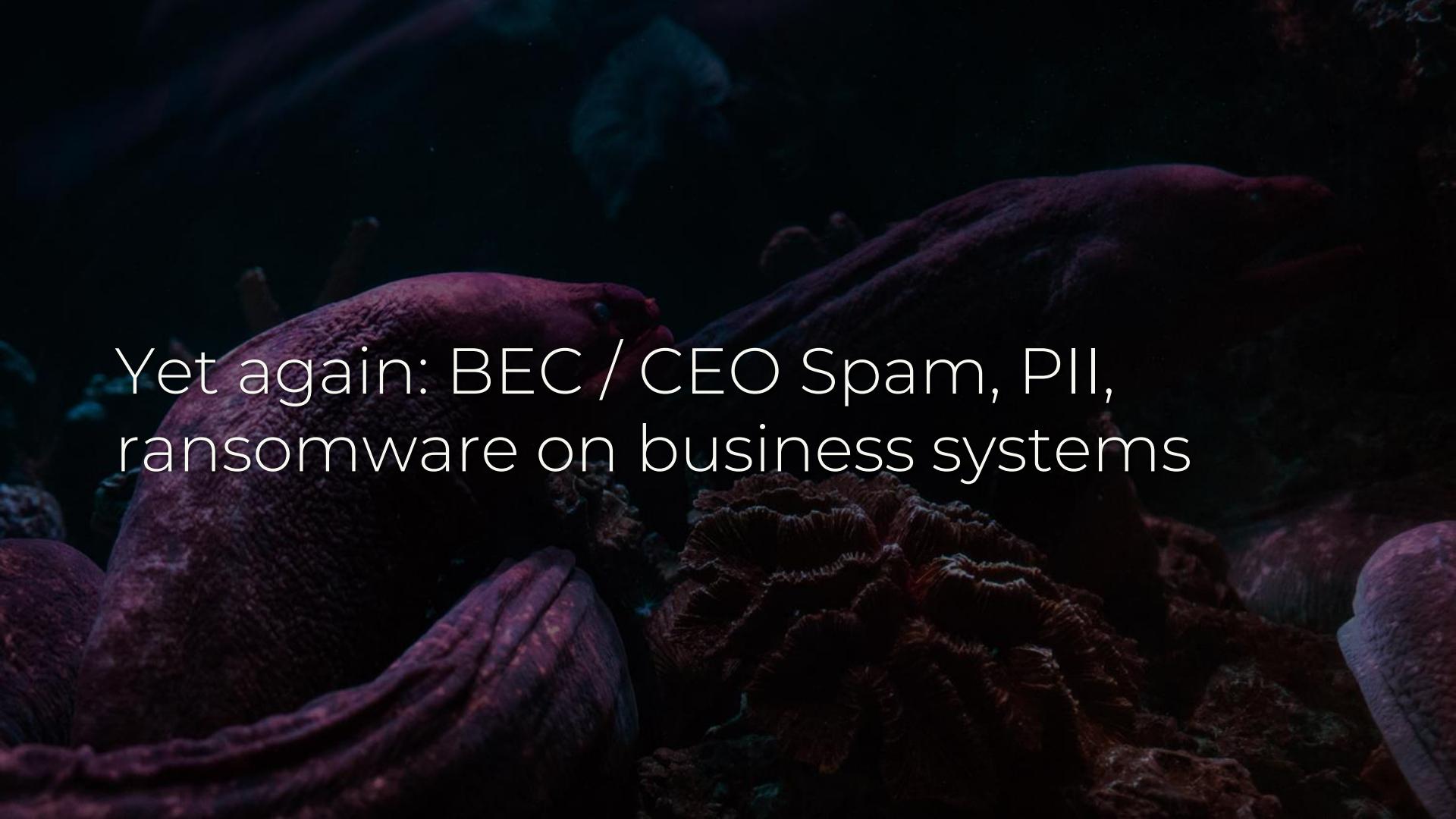
Managing fluctuating demand,
avoiding service interruption



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

A large pile of seized drug containers, likely made of plastic, stacked haphazardly. They are dark-colored with some lighter spots and appear to be filled with a granular substance. The containers are piled high, filling most of the frame.

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

The background image is a photograph of a sunset or sunrise over a body of water. The sky is filled with vibrant orange, red, and purple clouds. In the distance, dark silhouettes of hills or mountains are visible against the bright horizon. The overall atmosphere is dramatic and peaceful.

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?

The background of the slide is a photograph of a night sky. Dark, heavy clouds dominate the upper half, with several bright, branching lightning bolts striking across them from left to right. The horizon line is visible at the bottom, showing a faint reflection of the lightning on the water or ground below.

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

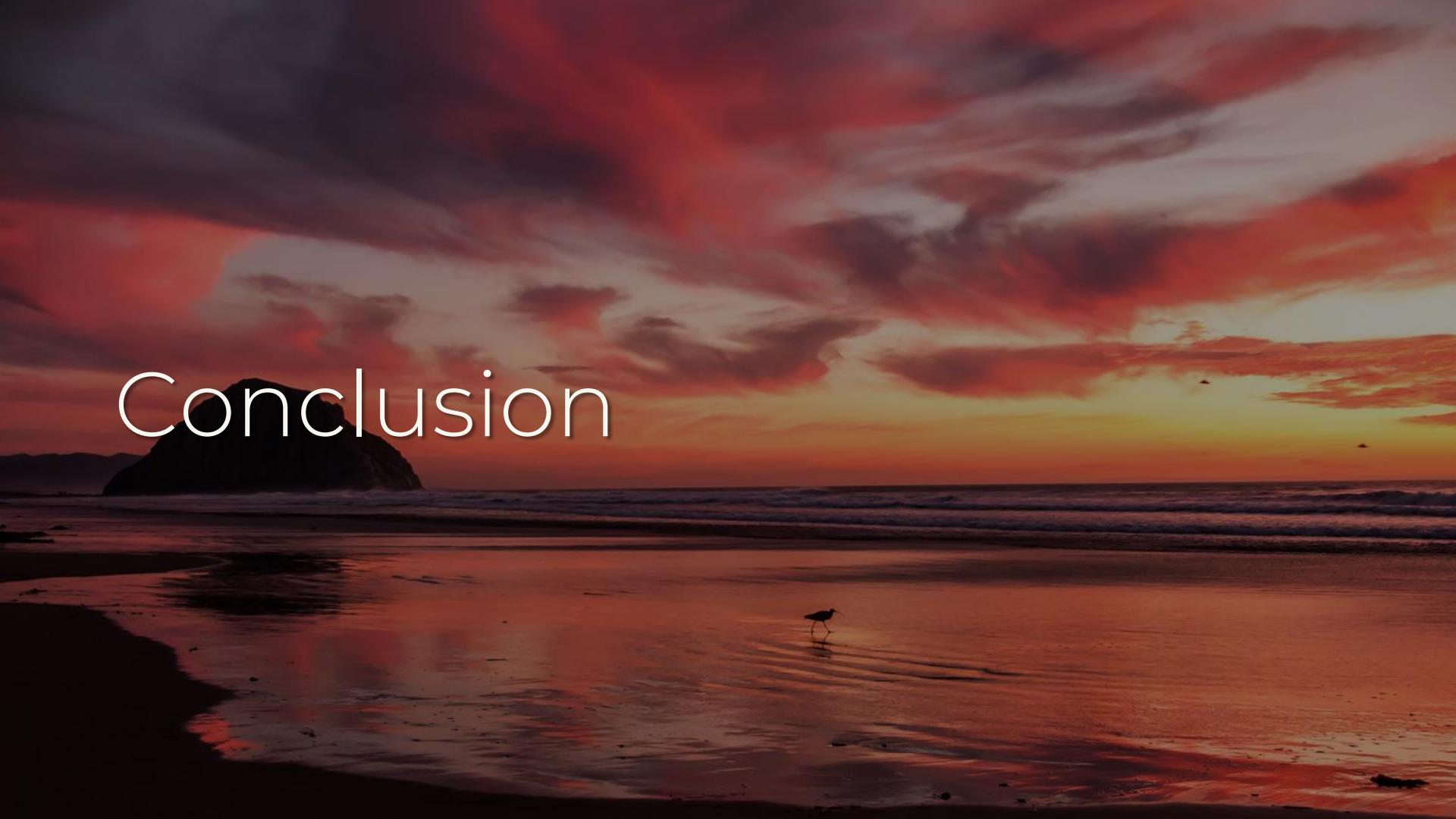
Time element expense, eg systems failure, without physical damage

A dark, grainy photograph showing a massive school of small, silvery fish swimming in a dense, swirling mass. The perspective is from above, looking down into the center of the swarm.

Cargo coverage includes damage,
theft, misdirection, interruptions

Most data breaches involving PII are excluded, along with ransomware

Conclusion



A dark, grainy photograph of a whale breaching the ocean. The whale's body is visible above the water, with its tail and a spray of water at the point of entry. The background is a dark, textured sea.

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

A dark, moody photograph of two dolphins swimming in the ocean. Their dorsal fins are visible above the water's surface, creating a sense of movement. The water is a deep blue, with some white foam from their movement.

Free yourself from the burden of
defending against all threats



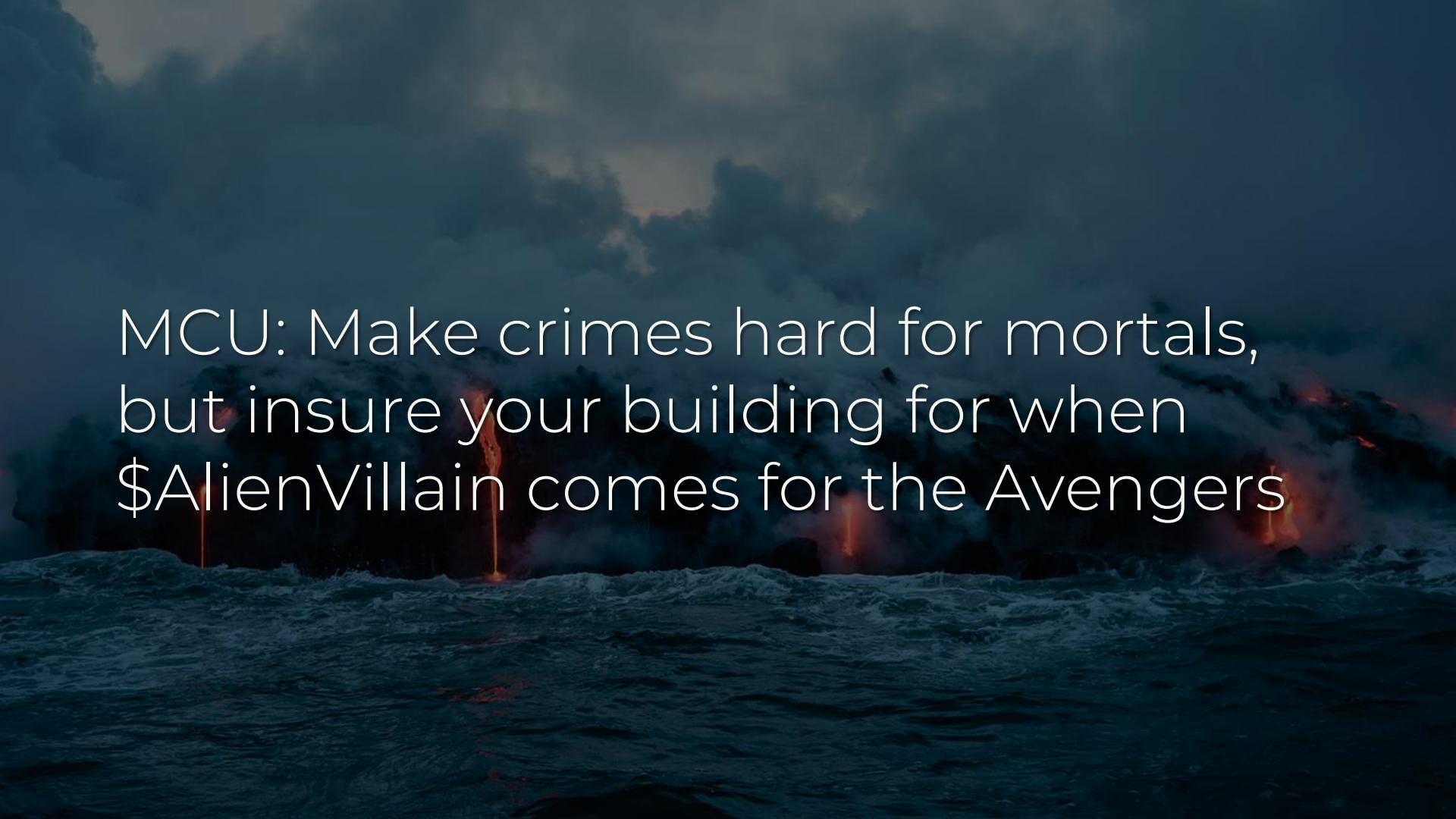
Where you can excel: how digital risks
can connect to your business risks

The background of the slide is a dark, atmospheric underwater scene. In the upper right, a massive school of small, silvery fish swims in a dense, swirling pattern. In the lower left, a smaller group of more colorful fish, including some bright orange and yellow ones, swims over a coral reef. The overall mood is mysterious and deep.

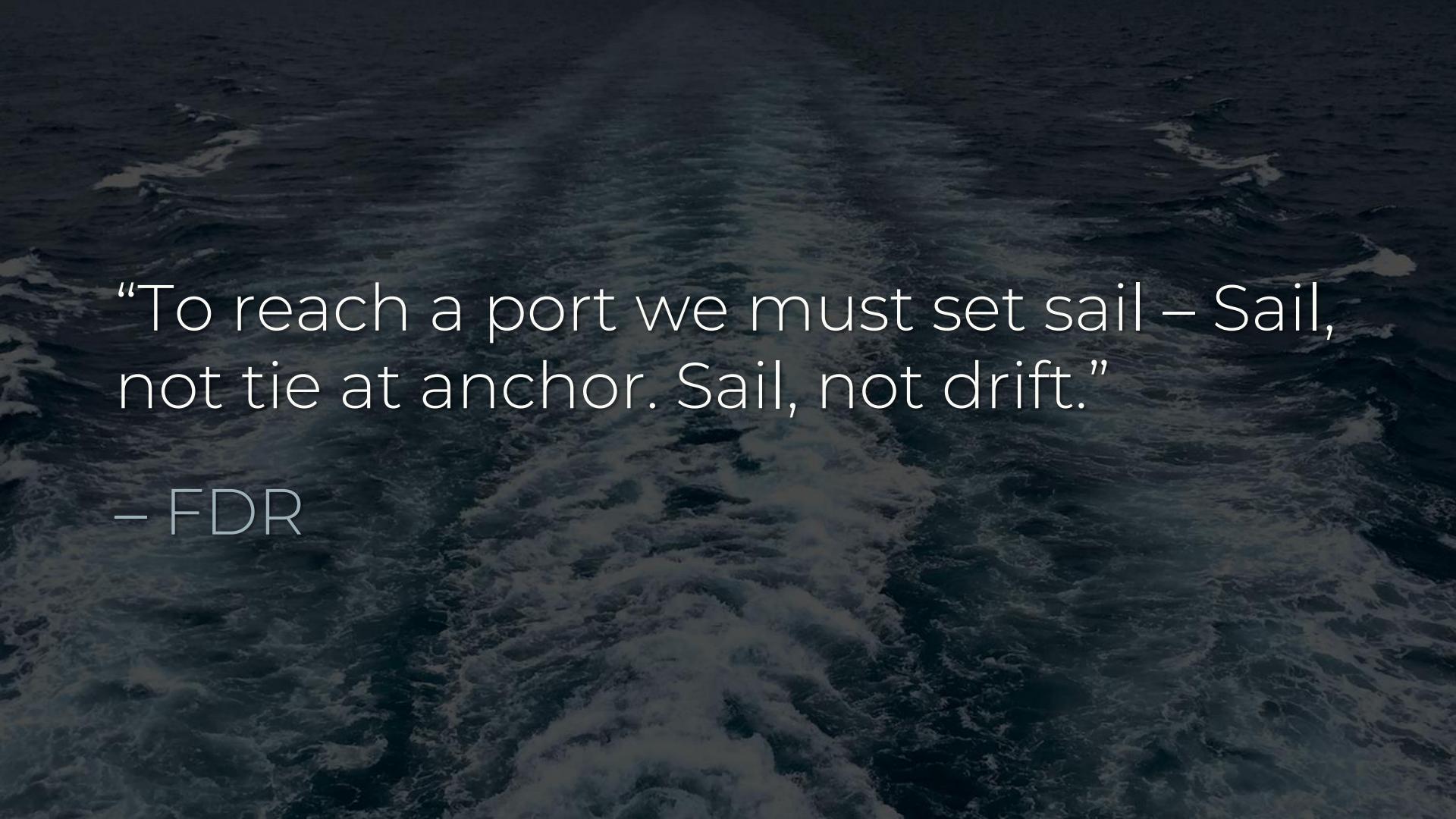
Identify where your org's risks meet
what attackers actually want



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

The background of the image shows a dark, turbulent sea in the foreground, with several bright orange and red streams of lava flowing from a volcano into the water. The sky above is filled with heavy, dark clouds, creating a somber and apocalyptic atmosphere.

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

The background of the image is a dark, textured view of ocean waves, suggesting a stormy or choppy sea. The lighting is low, creating deep shadows and bright highlights on the water's surface.

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

– FDR



@swagitda_



/in/kellyshortridge



kelly@greywire.net