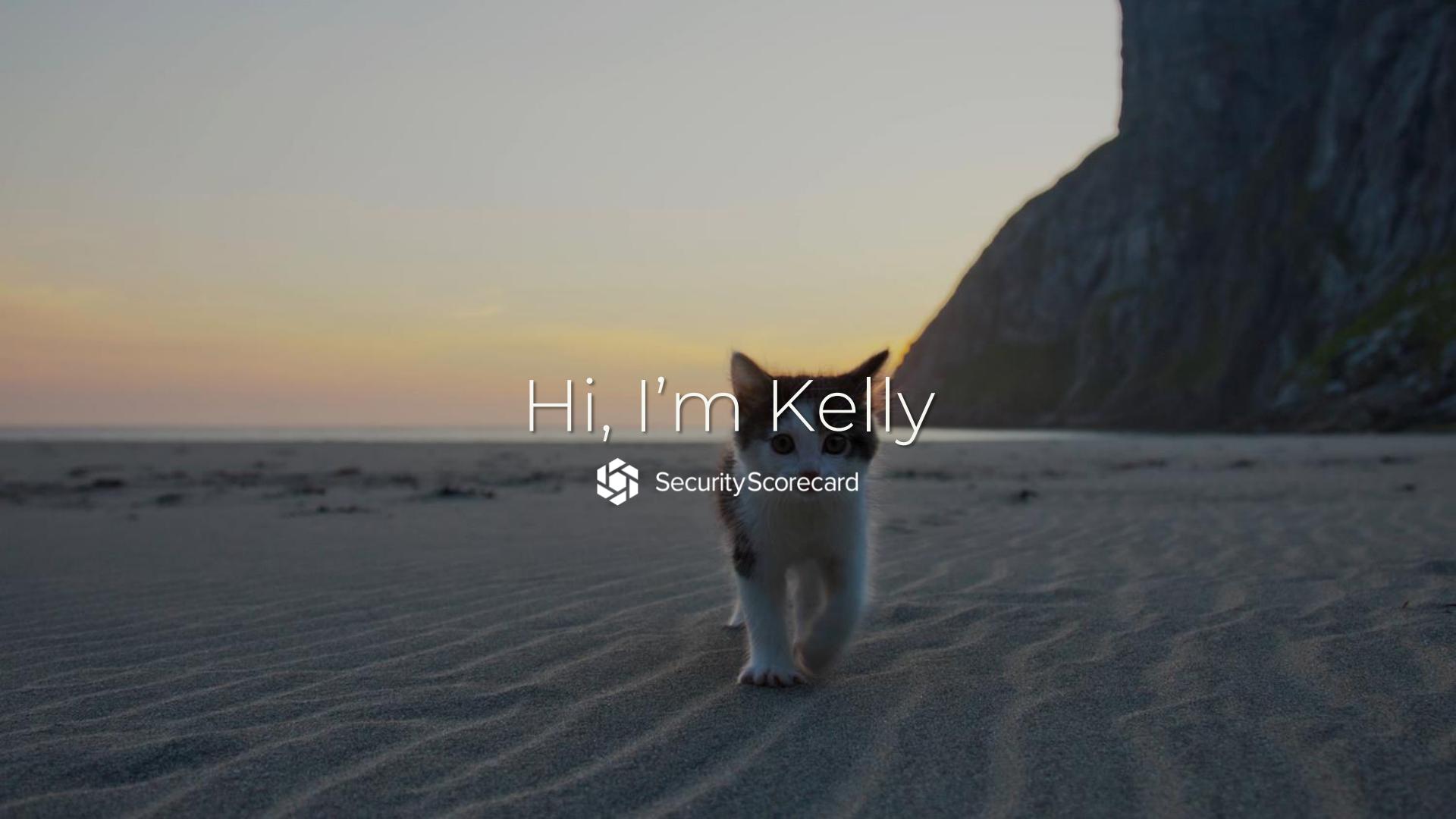


# Threat Prioritization: Freeing the White Whale

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. The horizon line is visible in the distance, and the overall mood is powerful and serene.

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.

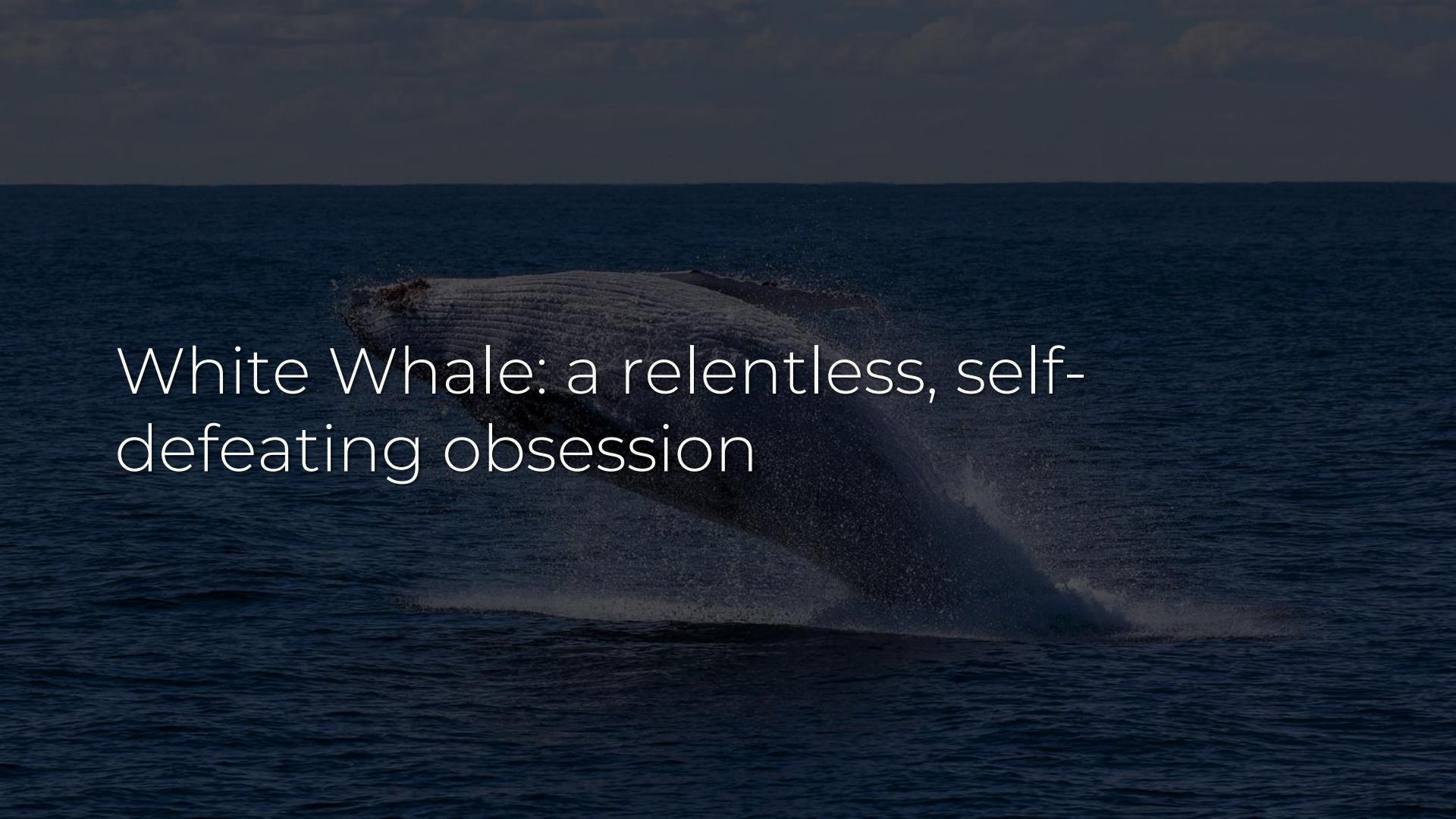
Hi, I'm Kelly



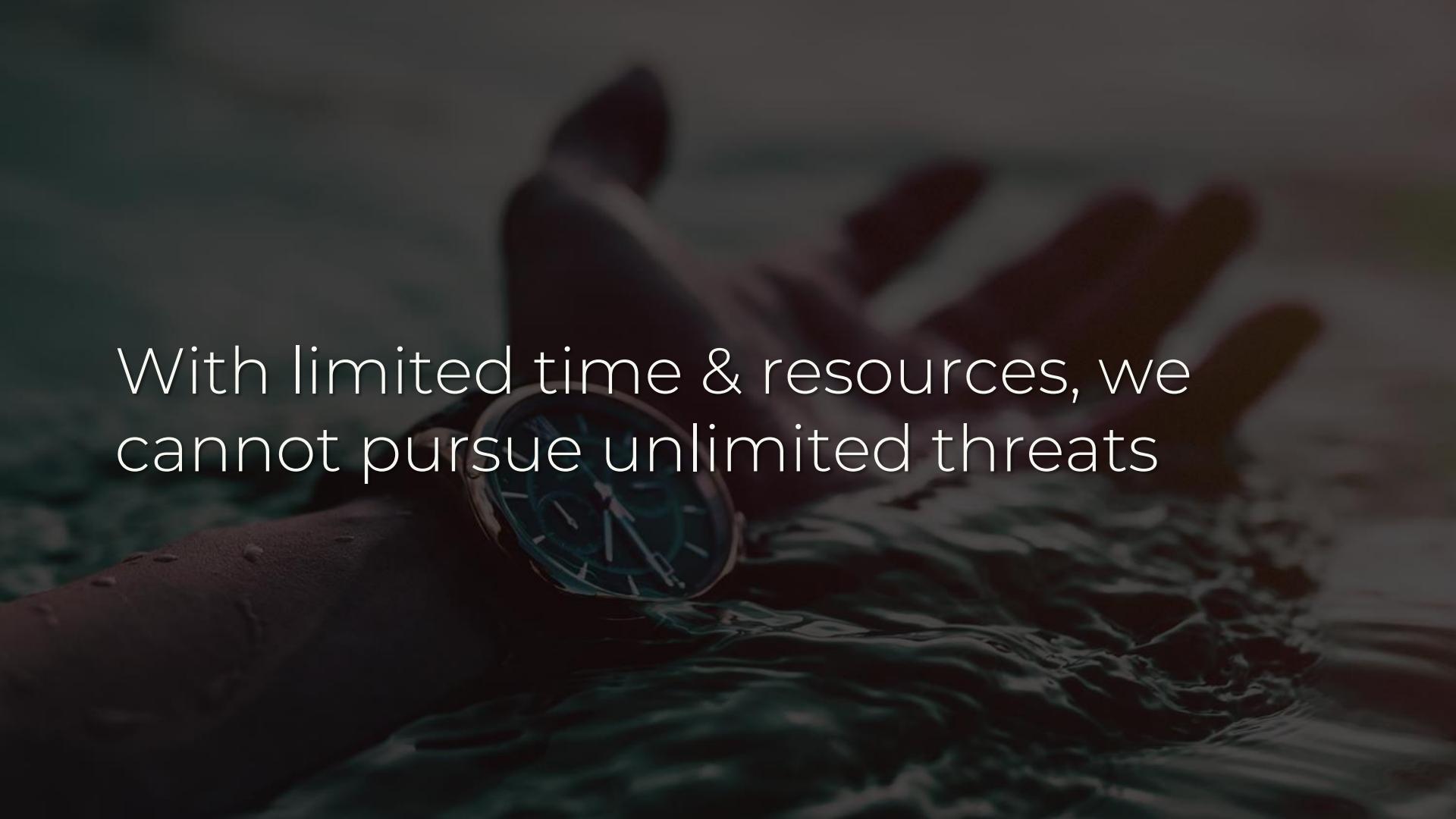
SecurityScorecard

“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 as it descends back into the ocean. The background shows a dark, cloudy sky over the vast expanse of the sea.

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, dark blue, with lighter, textured areas suggesting sunlight filtering through the surface or the presence of coral reefs below.

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

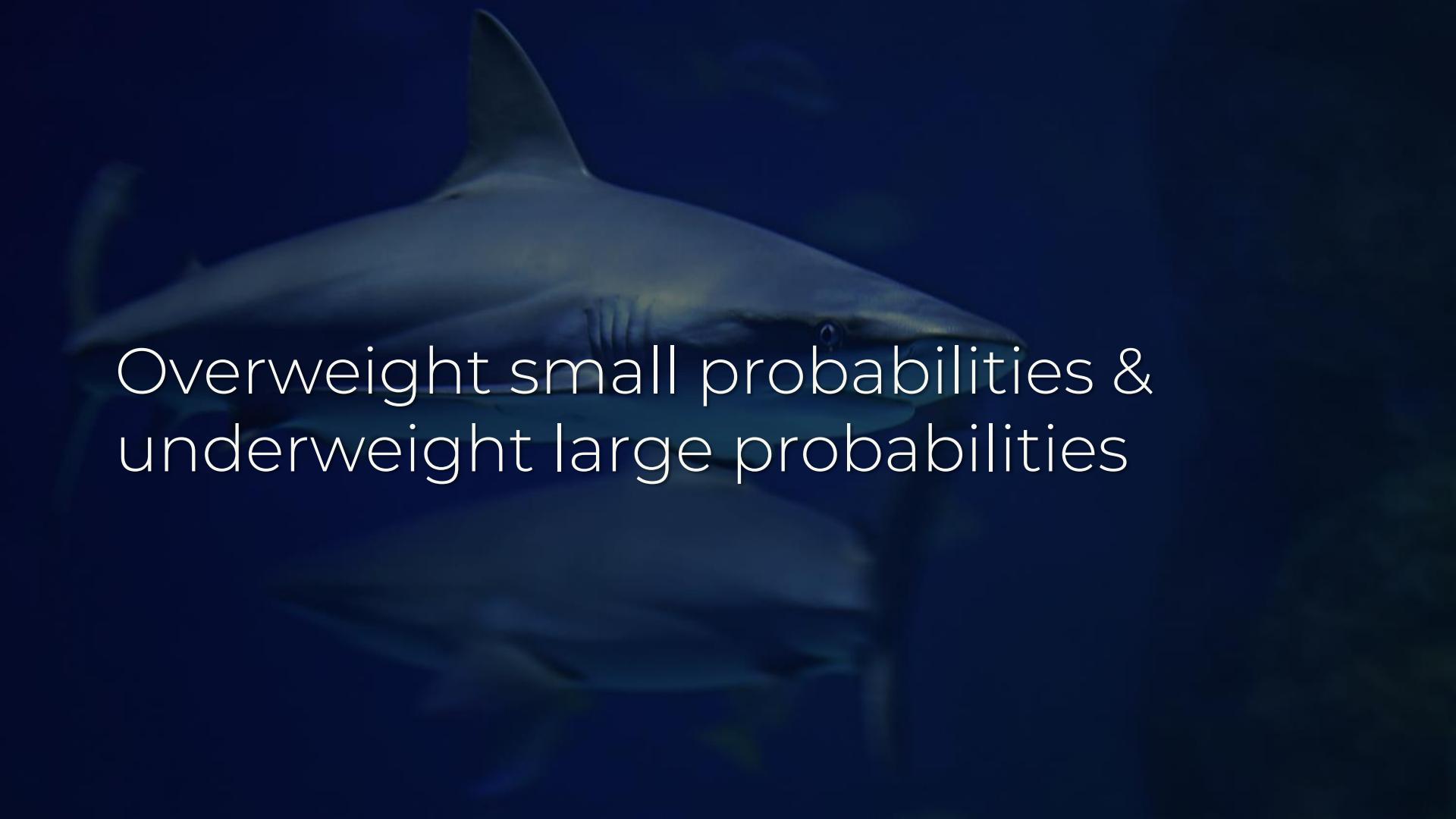
- 
1. Cognitive Biases
  2. Prioritization Framework
  3. Industry Examples



# 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 water. The shark's skin is a light grey-blue color, and its eye is visible. The background is a deep, dark blue.

Overweight small probabilities &  
underweight large probabilities

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

The background of the slide is a dark, moody photograph of a large school of fish, likely tuna or mackerel, swimming in a dark blue sea. The fish are silhouetted against a lighter background, creating a sense of depth and movement.

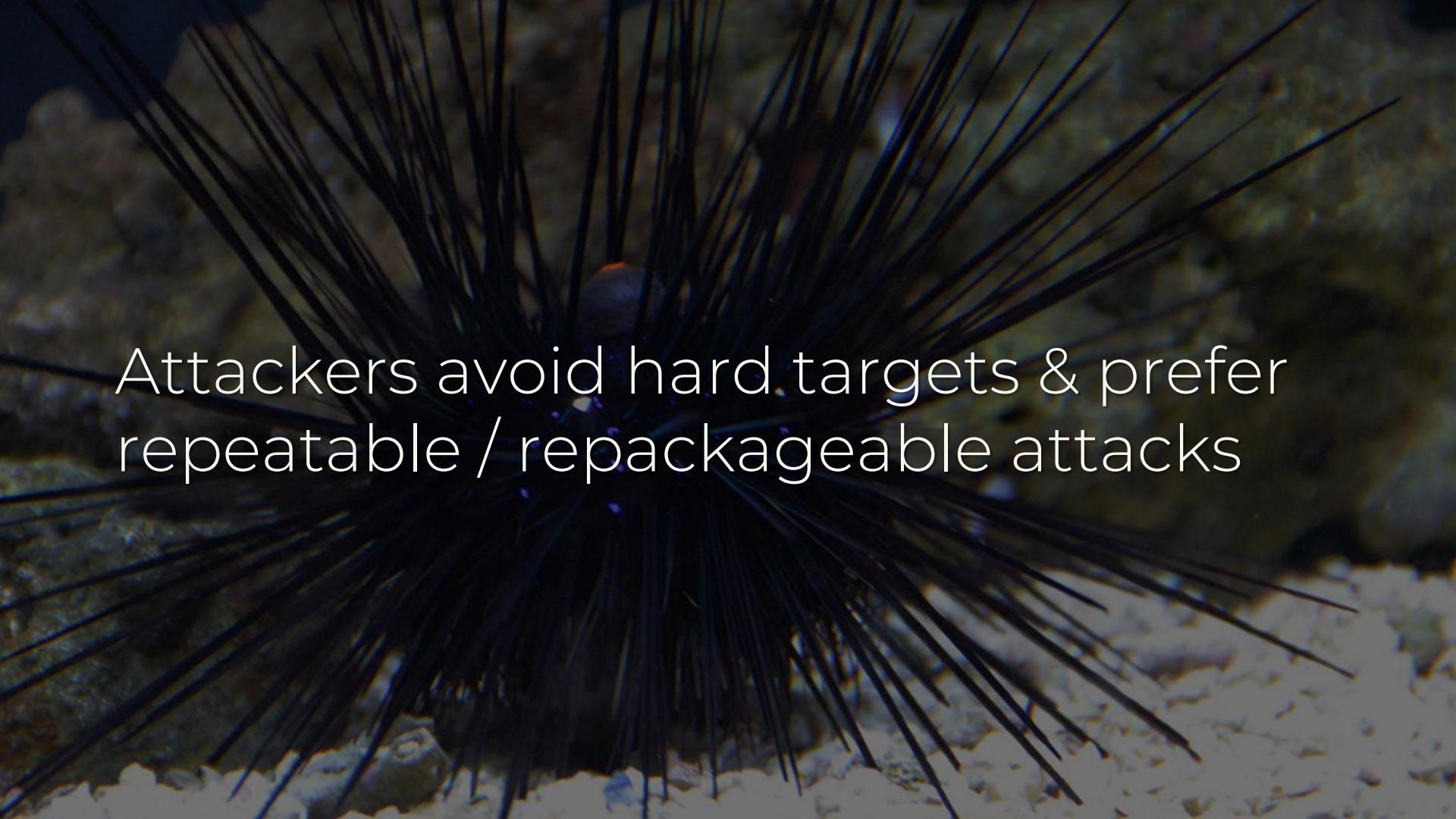
Super elite 0day (overweighted) vs.  
phishing (underweighted)

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)

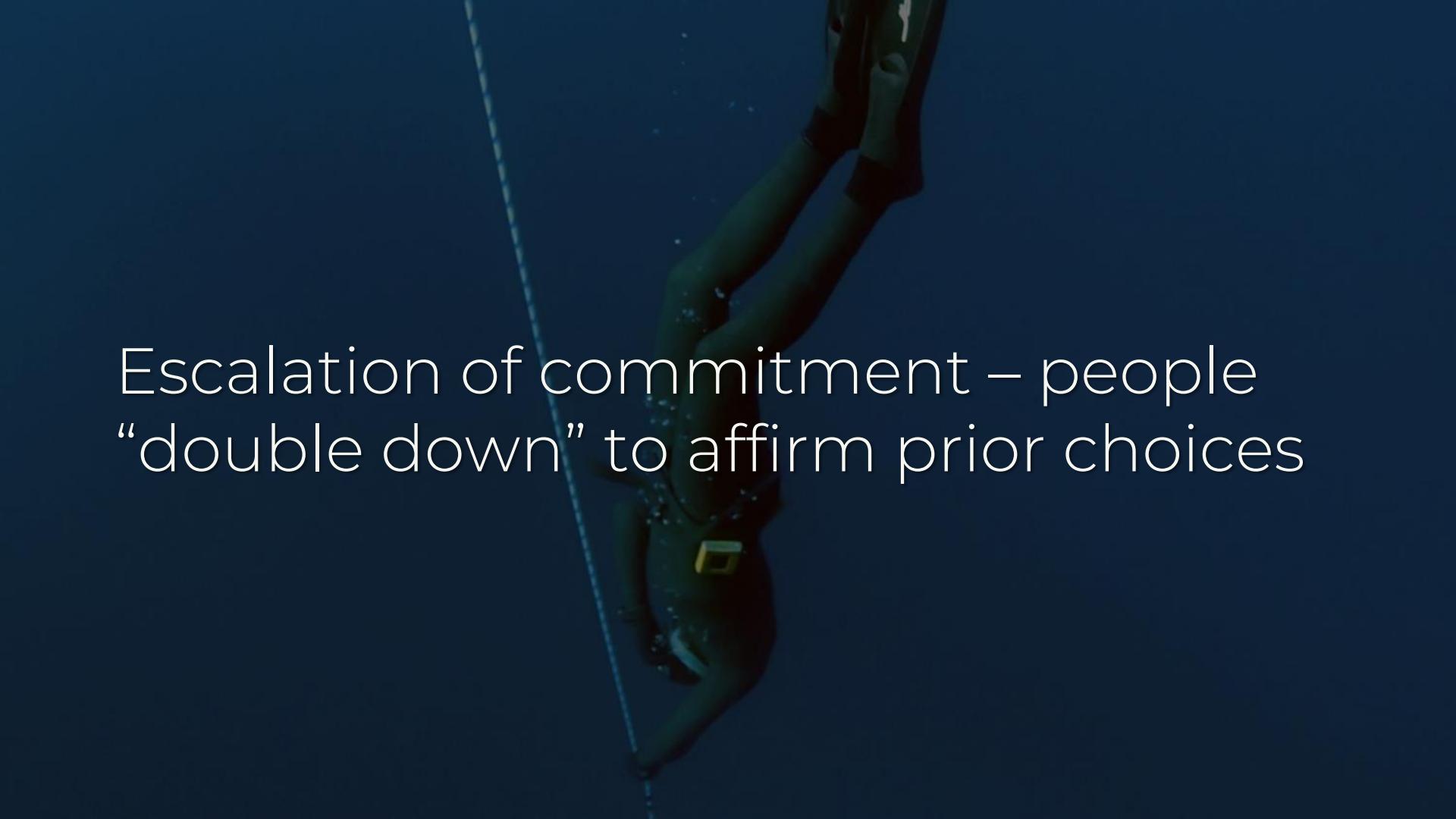


Availability heuristic – those headlines  
about “Cybergeddon” influence you



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

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

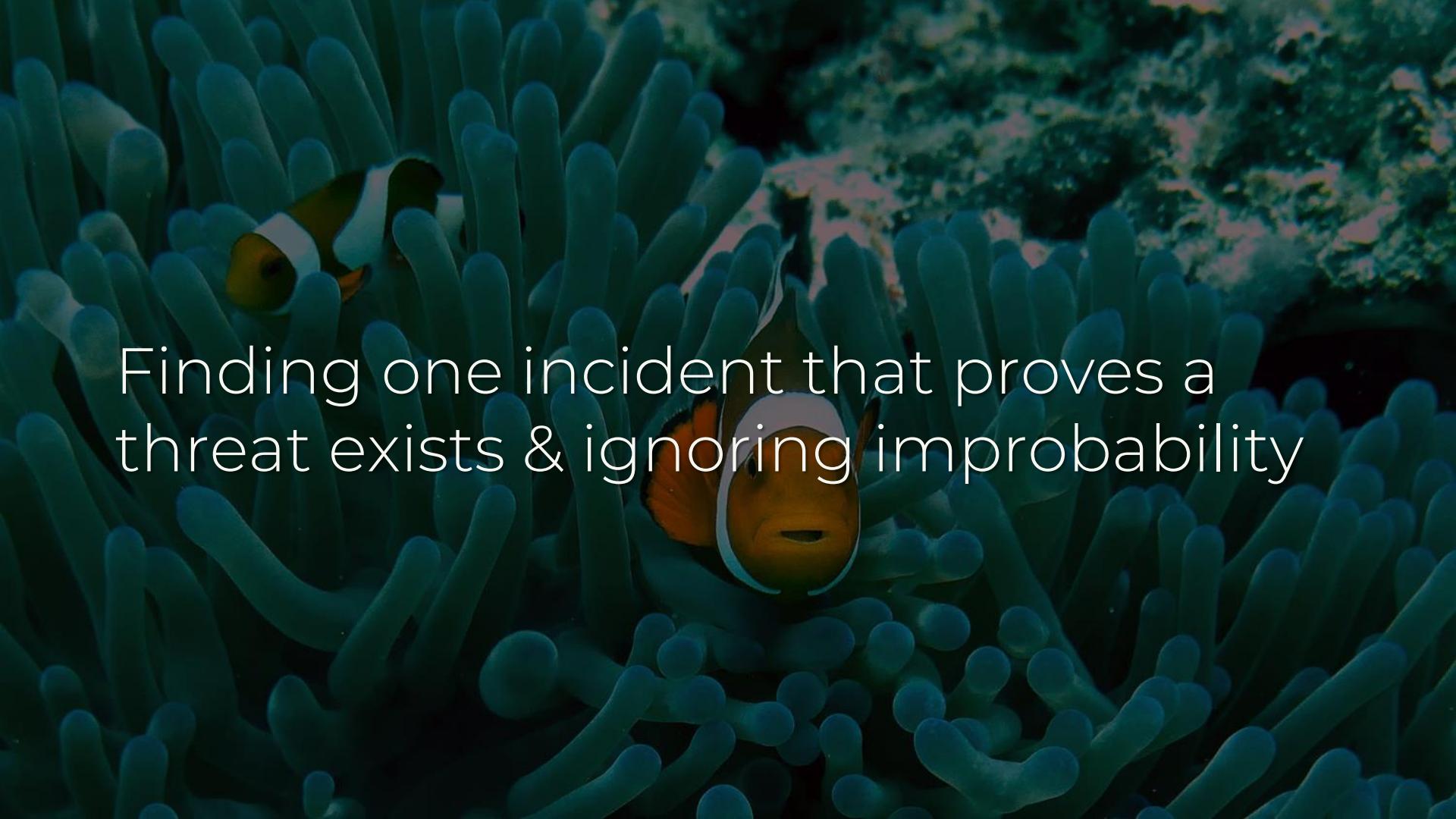


Escalation of commitment – people  
“double down” to affirm prior choices

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?

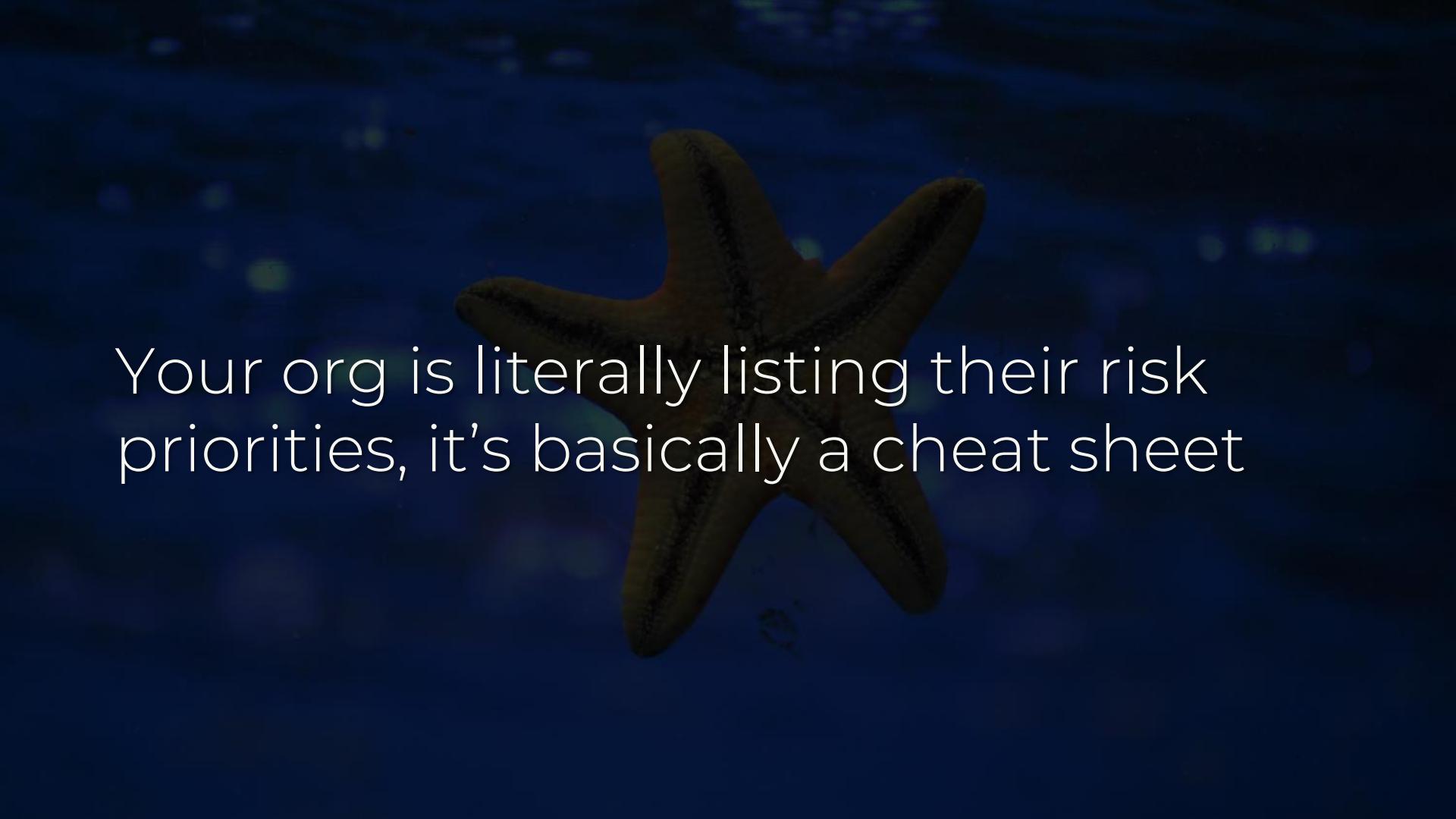
Go to your org's / your competitors'  
Investor Relations website

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, likely a five-pointed starfish, set against a dark, textured background that appears to be water or a rock surface. The starfish is oriented vertically, with its arms pointing upwards and outwards. Its body is a light color, possibly yellow or orange, with darker, mottled patterns on its arms.

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)

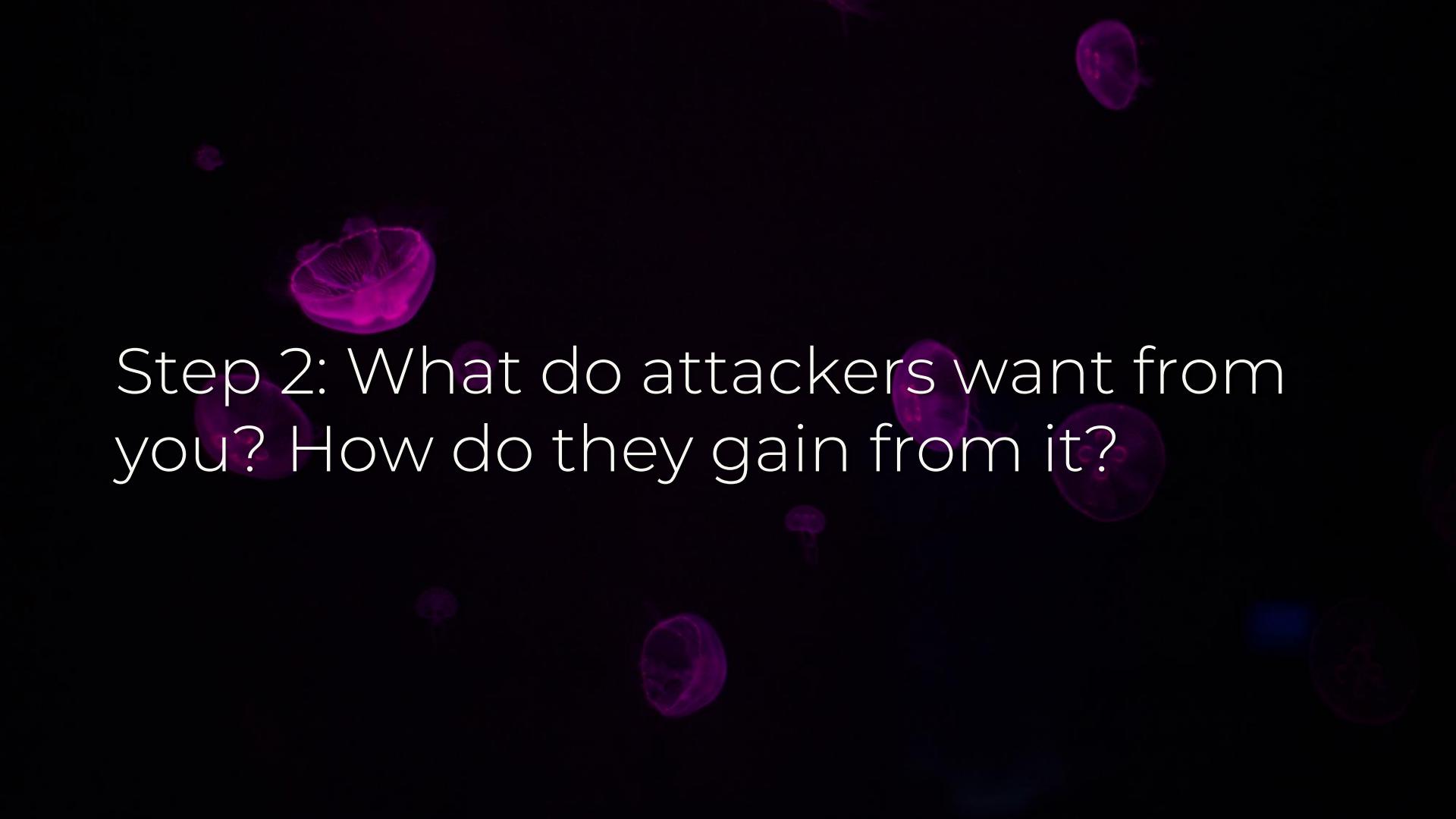
A large shark, possibly a hammerhead, swims through dark, slightly rippled water. The shark's body is angled downwards and to the right. The background is a deep teal or black.

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

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

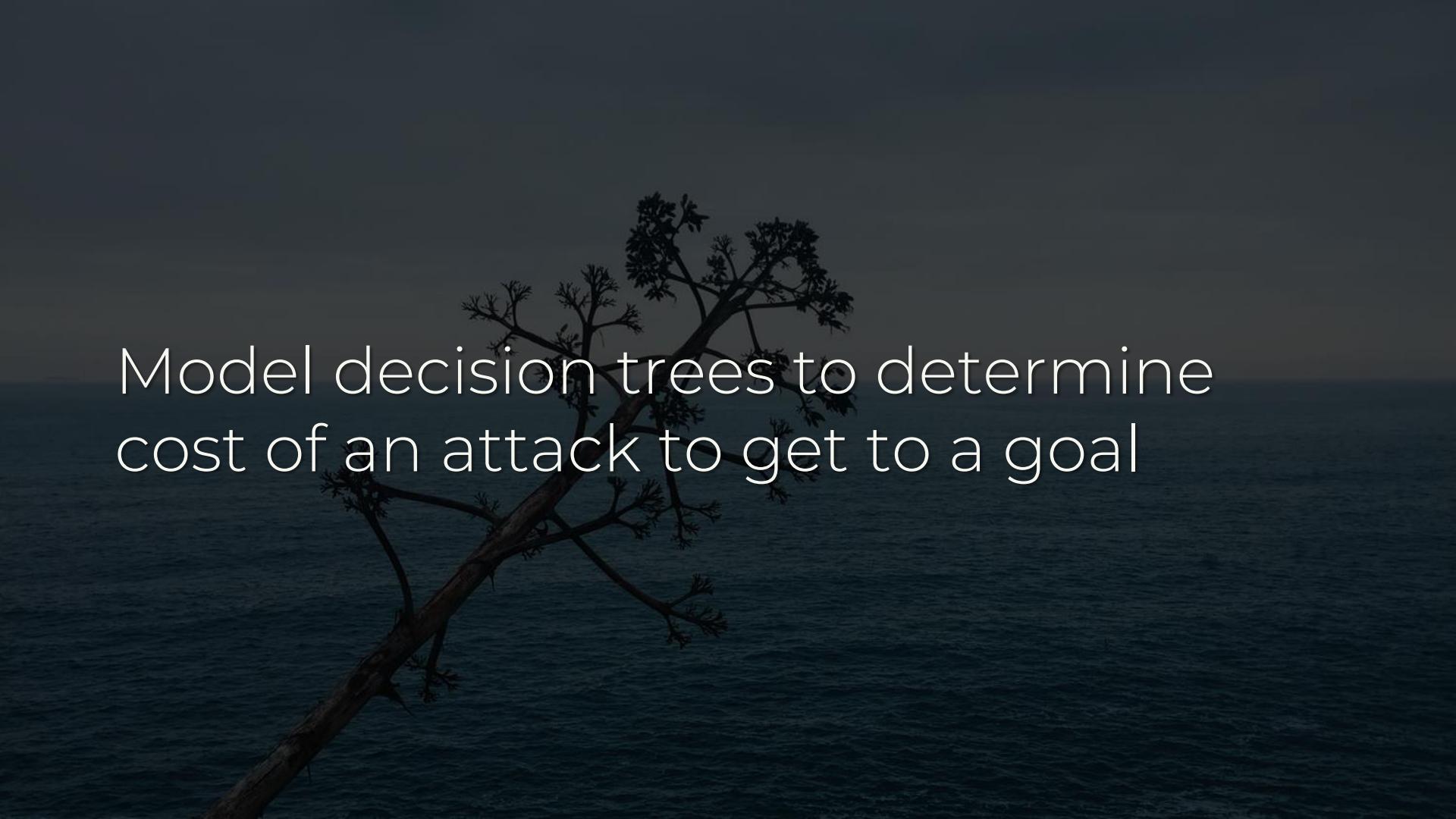
Read cyber insurance coverage for your industry, including exceptions

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

The background of the slide is a dark, atmospheric photograph. A large, gnarled tree branch with many small, leafy sprouts extends from the bottom left towards the center. The branch is silhouetted against a lighter area that suggests a sky over water. The overall mood is mysterious and contemplative.

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



Step 3: Cross-compare results

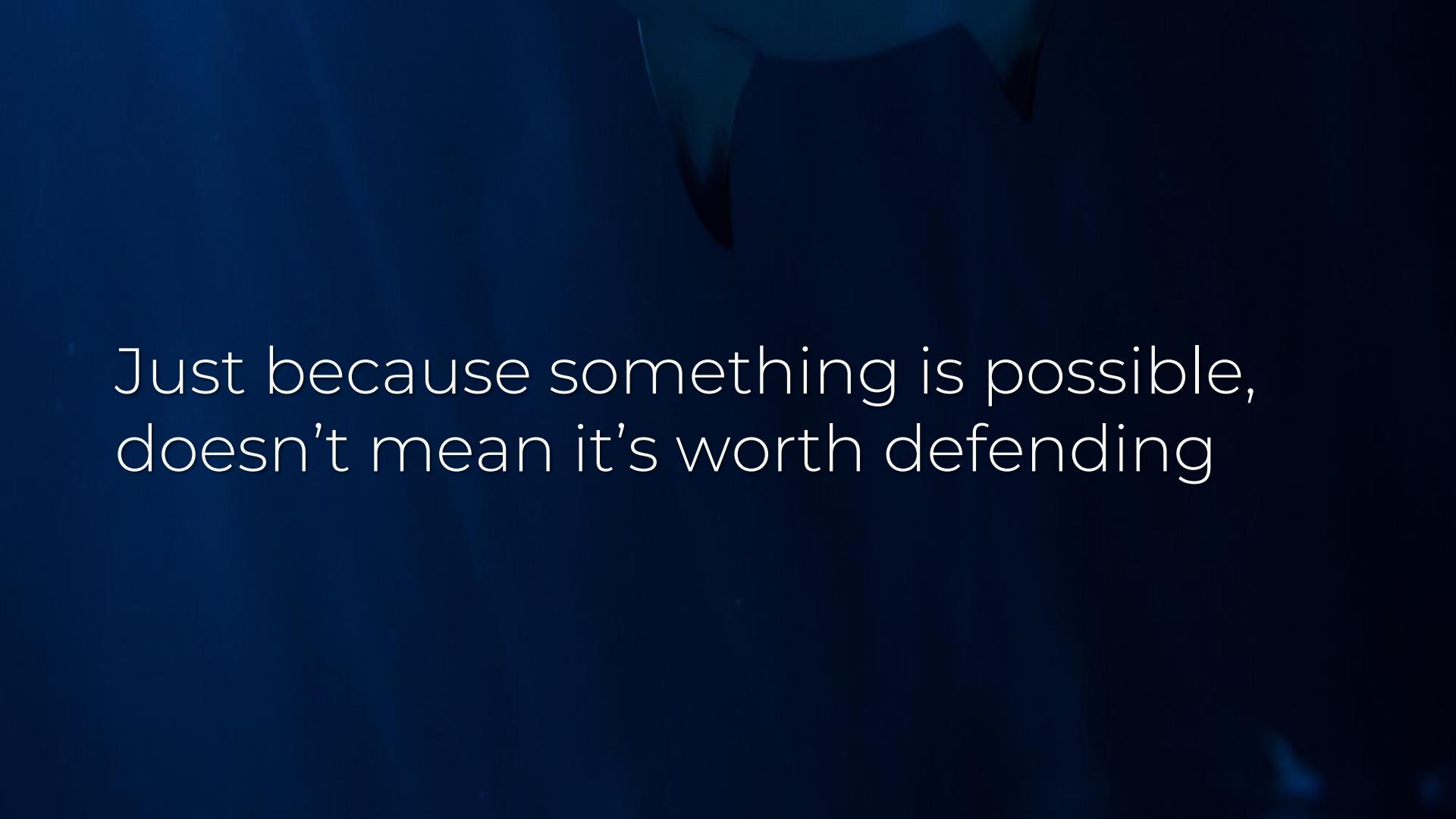


If you don't see *your* priority in Risk Factors, challenge your assumptions

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



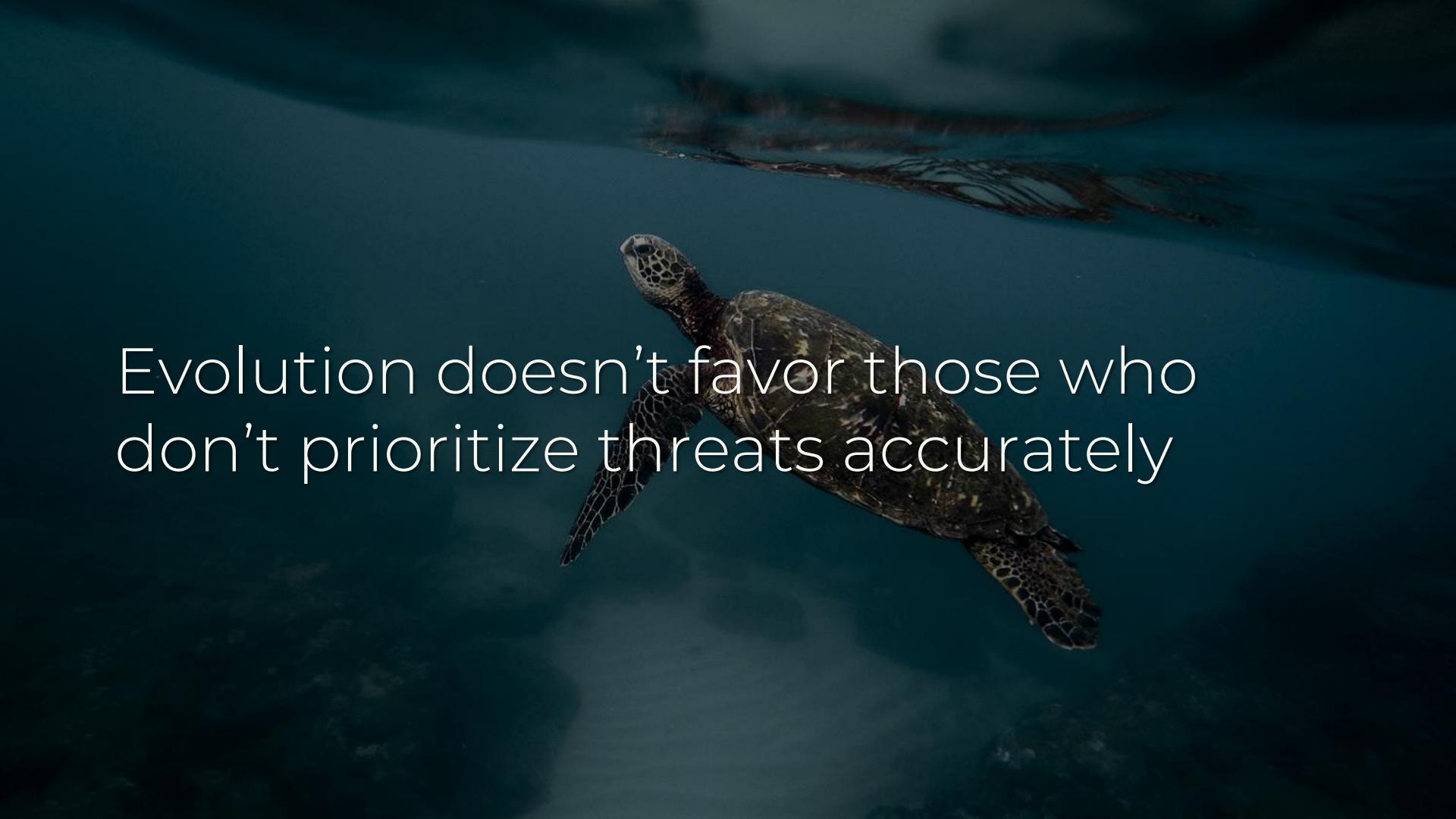
Hackers are unlikely to remotely crash  
your satellite into space debris



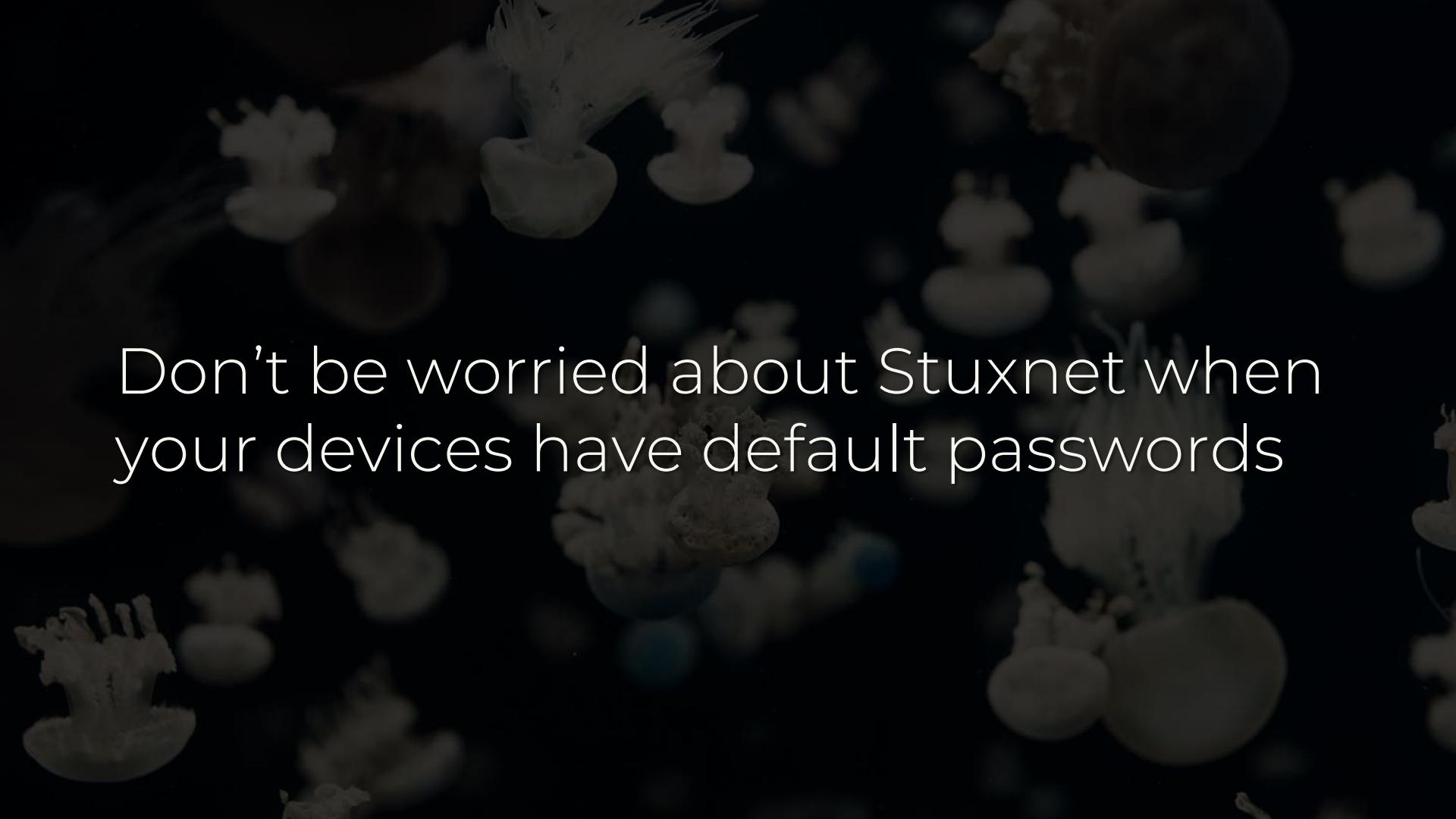
Just because something is possible,  
doesn't mean it's worth defending

A close-up photograph of a clownfish, likely a Clark's anemonefish, swimming gracefully among the tentacles of a vibrant red sea anemone. The fish has its characteristic orange body with white stripes and a white belly. The background is a dark, out-of-focus underwater scene.

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

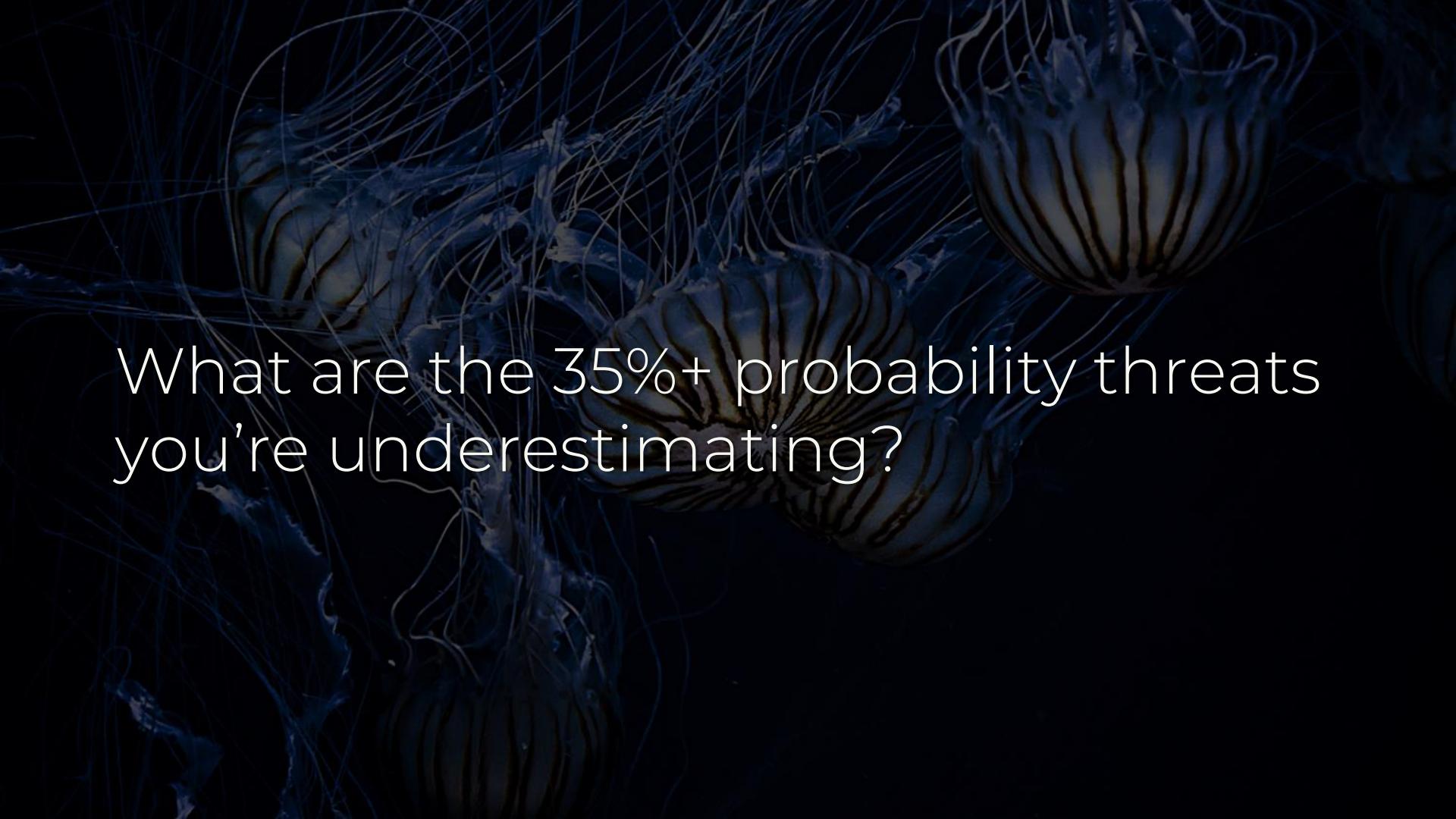
A large sea turtle is swimming gracefully through dark blue, slightly choppy water. The turtle's head is above the surface, and its patterned shell and long, thin tail are clearly visible. Another turtle is partially visible in the background, also swimming towards the right.

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



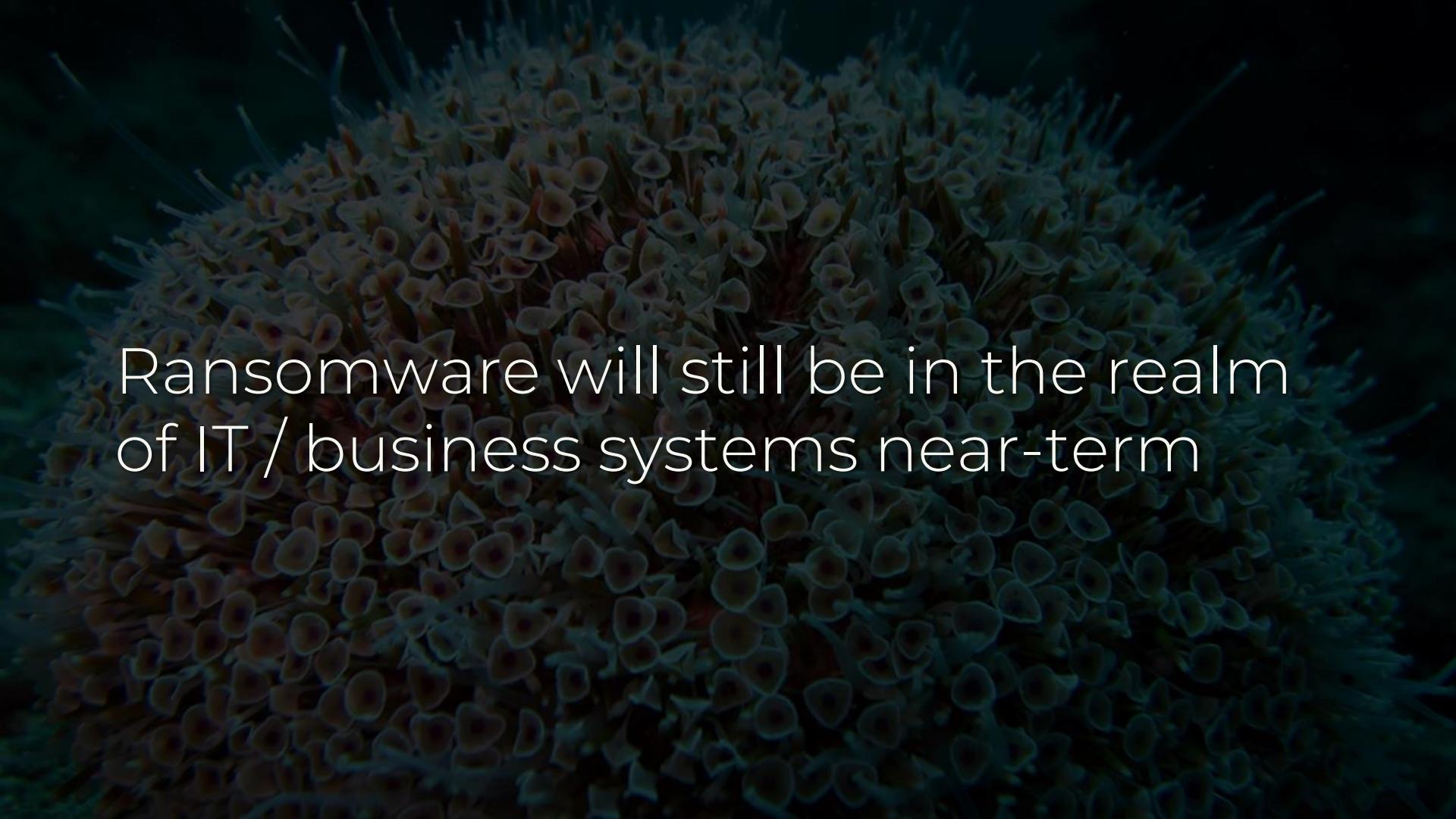
What are the 35%+ probability threats  
you're underestimating?



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

A dramatic photograph of a seal leaping out of dark, choppy ocean waves. The seal is captured mid-air, its body arched as it moves from left to right. Its front flippers are extended downwards, and its back flipper is tucked under its body. Water splashes around its head and tail. The background consists of more turbulent waves under a dark, cloudy sky.

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 as small, rounded structures with darker tips, set against a dark, textured background.

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

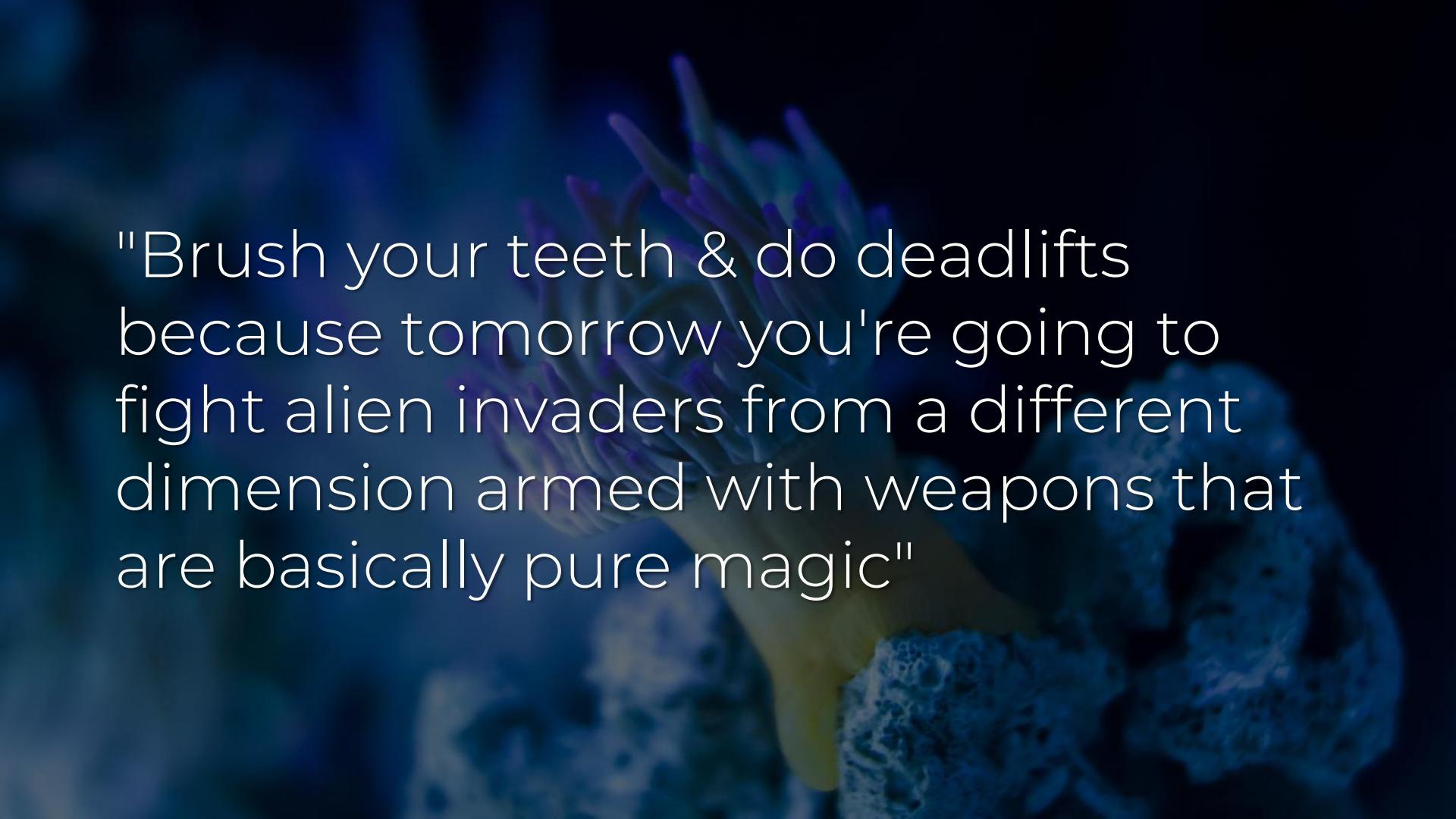
Time & resources required to port ransomware to OT = poor ROI

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 subtle, glowing highlights that suggest distant city lights or reflections on the water's surface.

Operational efficiency is seen as a  
competitive advantage now

Project management: negotiations,  
development, optimization

Tech: operational unavailability,  
inefficiency, or disruption

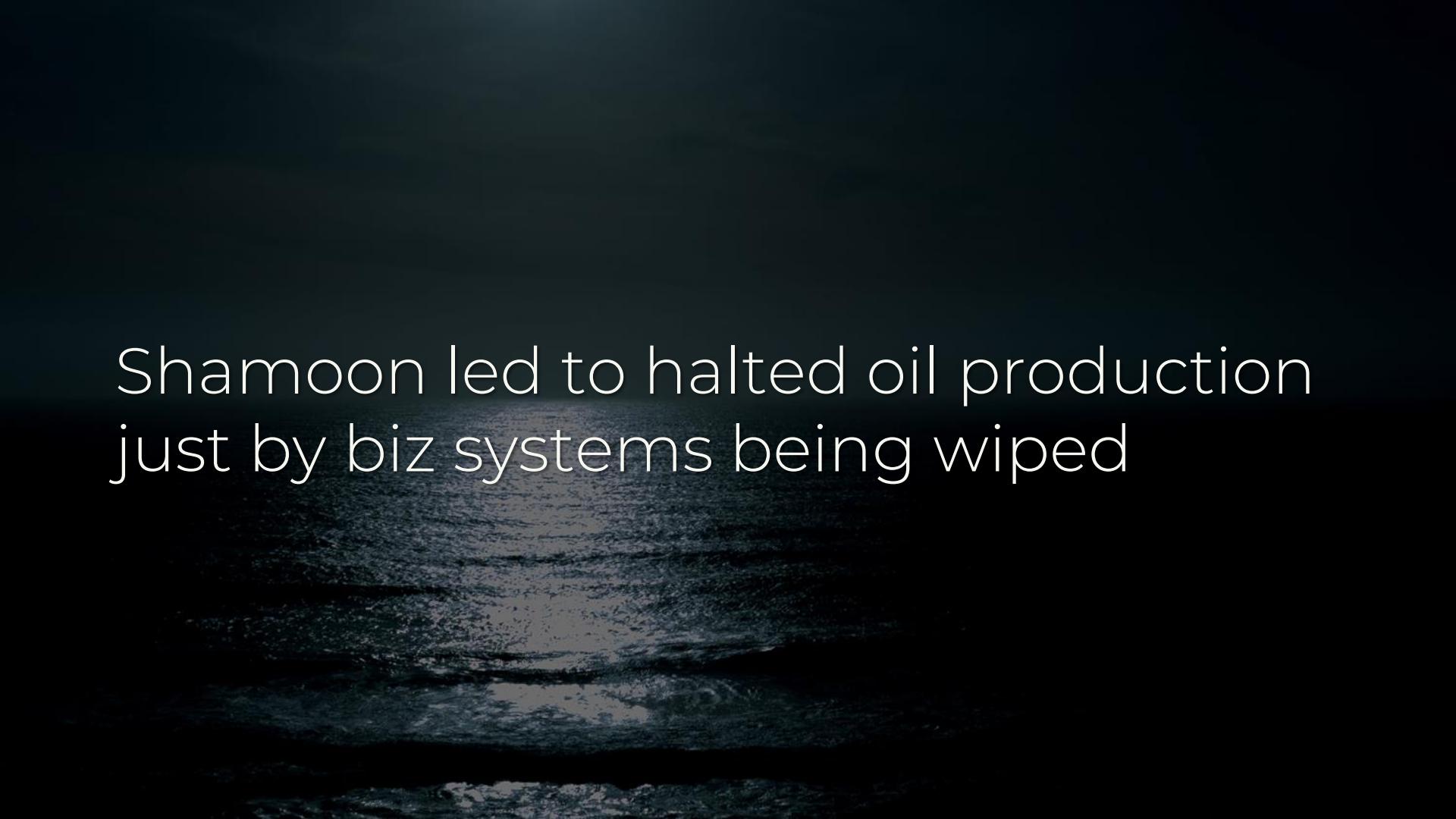
Infosec: physical harm, asset damage,  
op disruption, biz system compromise

A large offshore oil rig is silhouetted against a dark, hazy sky. The rig's complex steel structure, including its derrick, walkways, and various platforms, is visible. It stands in the middle ground, with the dark ocean in the foreground and a faint horizon line.

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

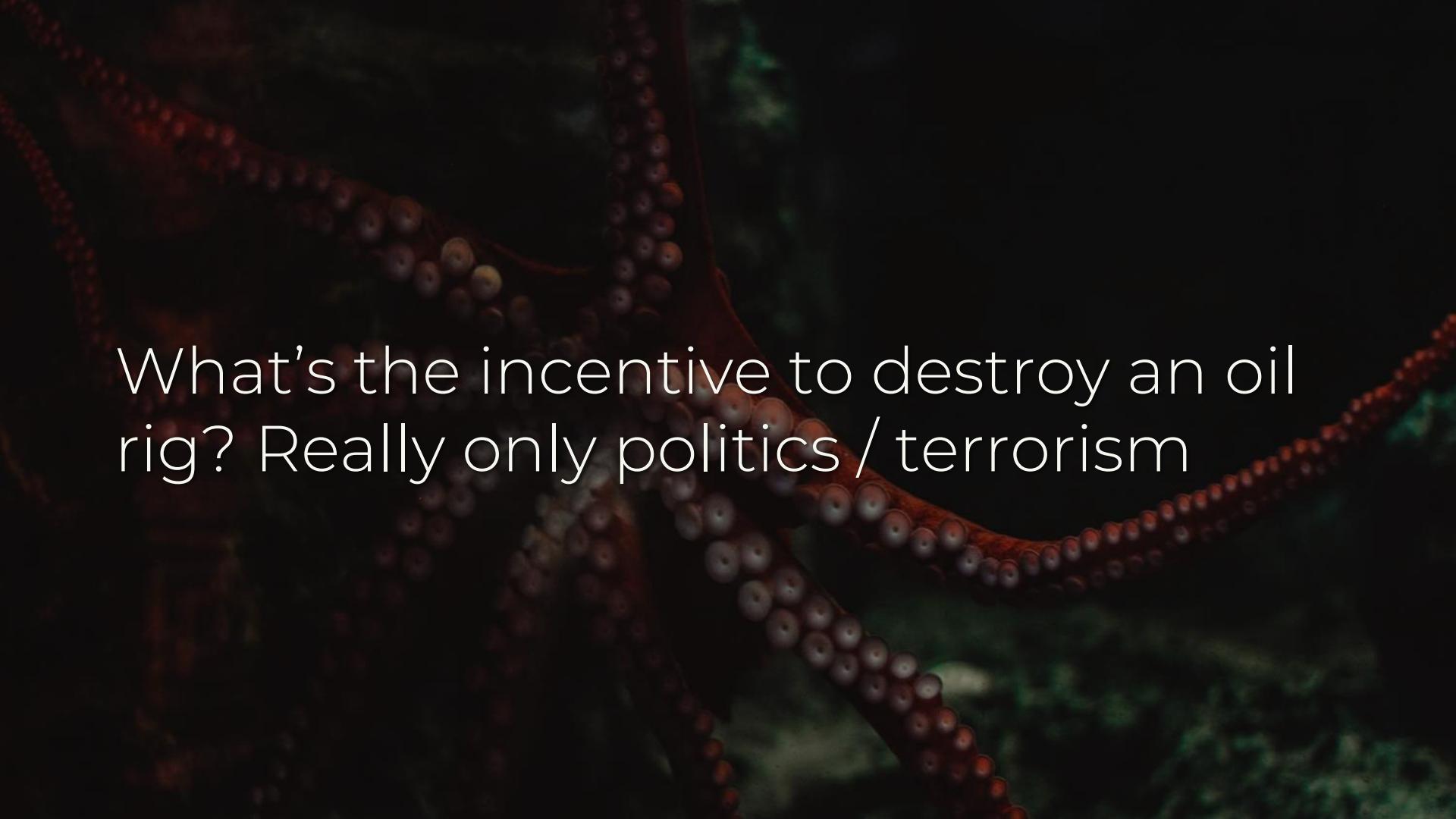
What is being insured by cyber insurance for oil & gas?

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?



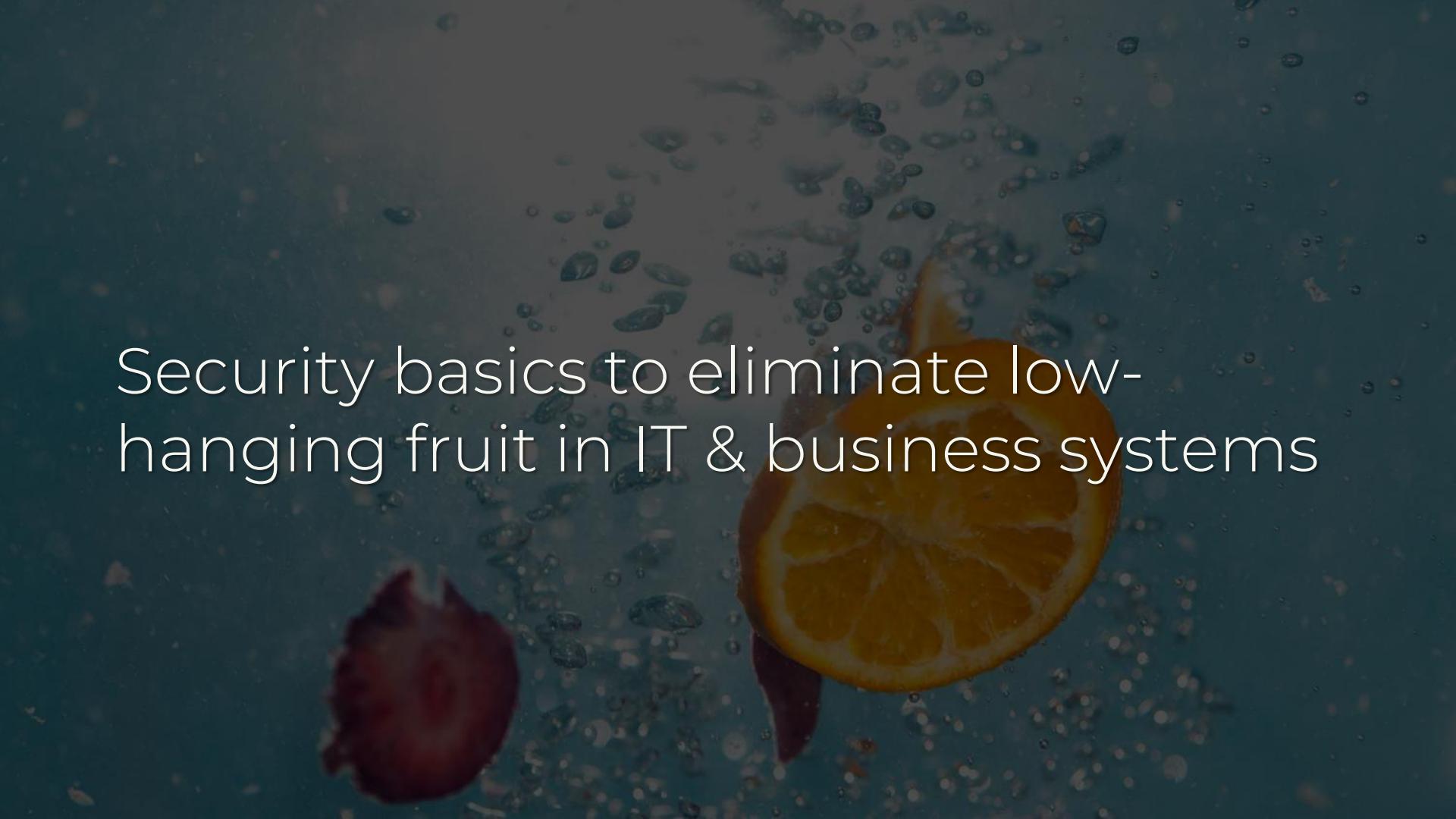
What's the incentive to destroy an oil rig? Really only politics / terrorism

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 multiple cross-arms and insulators holding wires. In the foreground, the word "Telecom" is written in a large, white, sans-serif font.

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

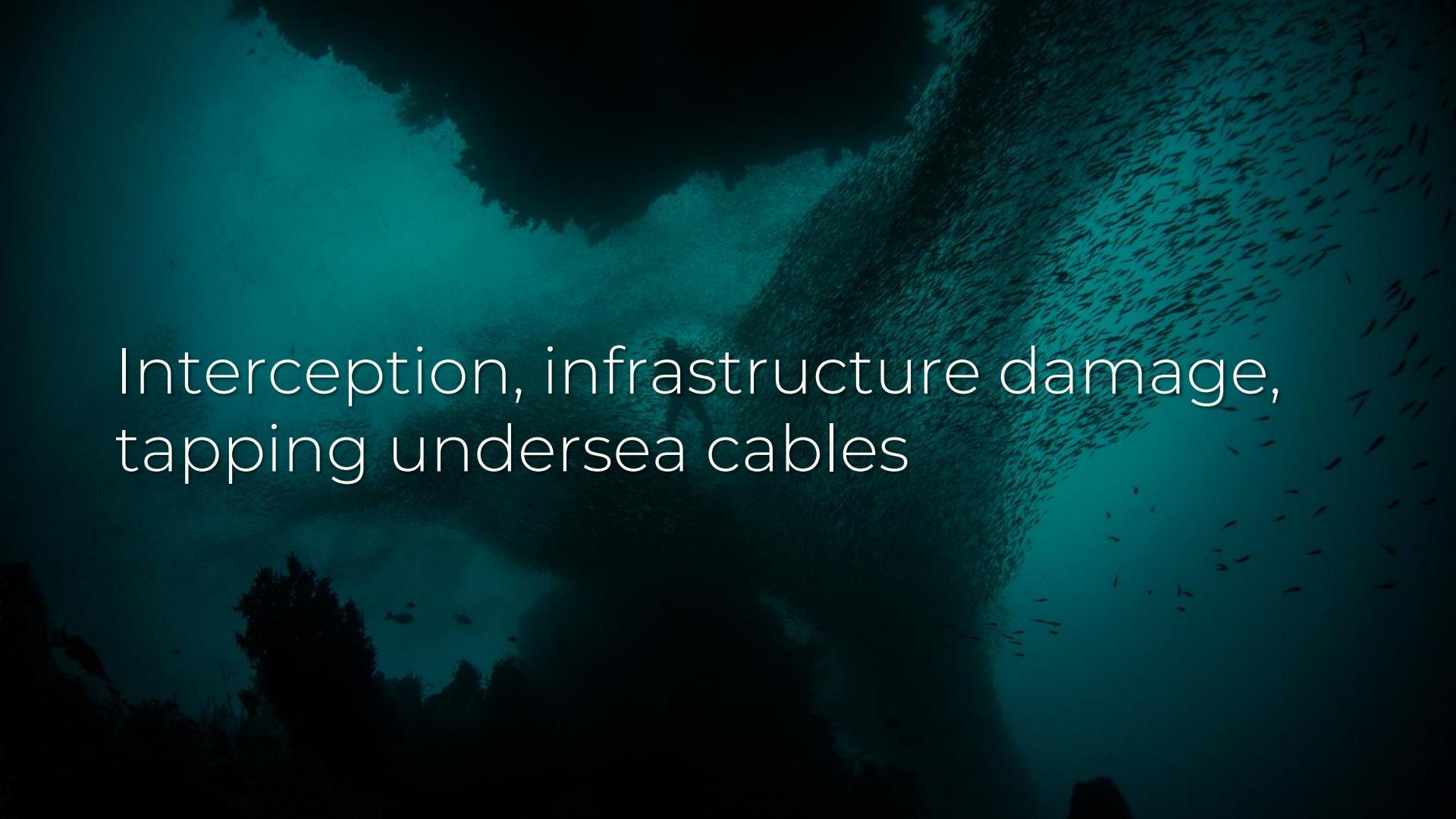
GDPR means PII may matter – privacy  
hasn't been economical before



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

The background of the slide is a dark, moody photograph of a forest at night. A bright, hazy light source, possibly the moon or a fire, is visible through the trees in the distance, casting long shadows and creating a sense of mystery. The overall color palette is dominated by deep blues and blacks.

Interception, infrastructure damage,  
tapping undersea cables

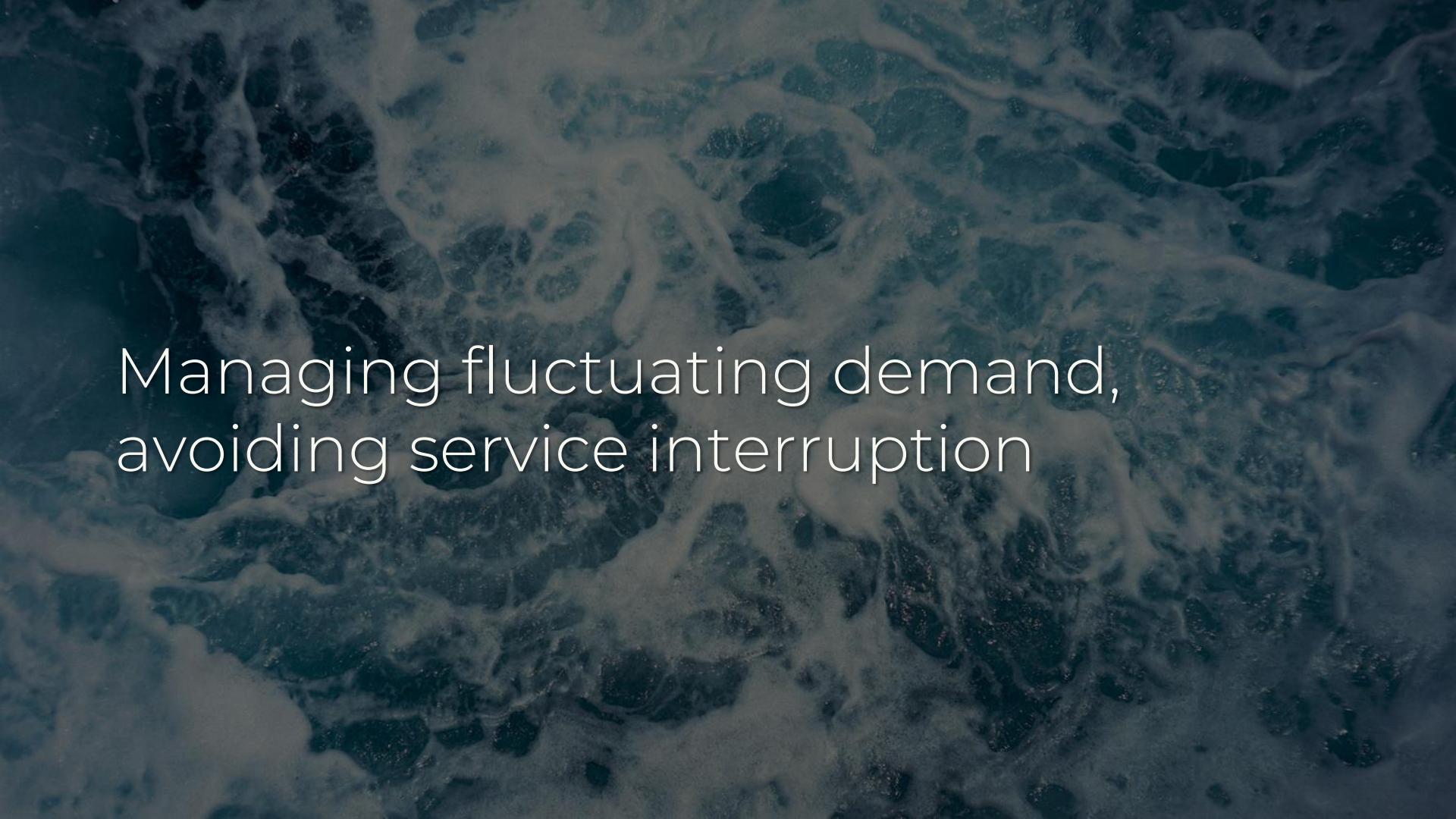
Step 3: Where do Risk Factors & attacker goals align?

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.

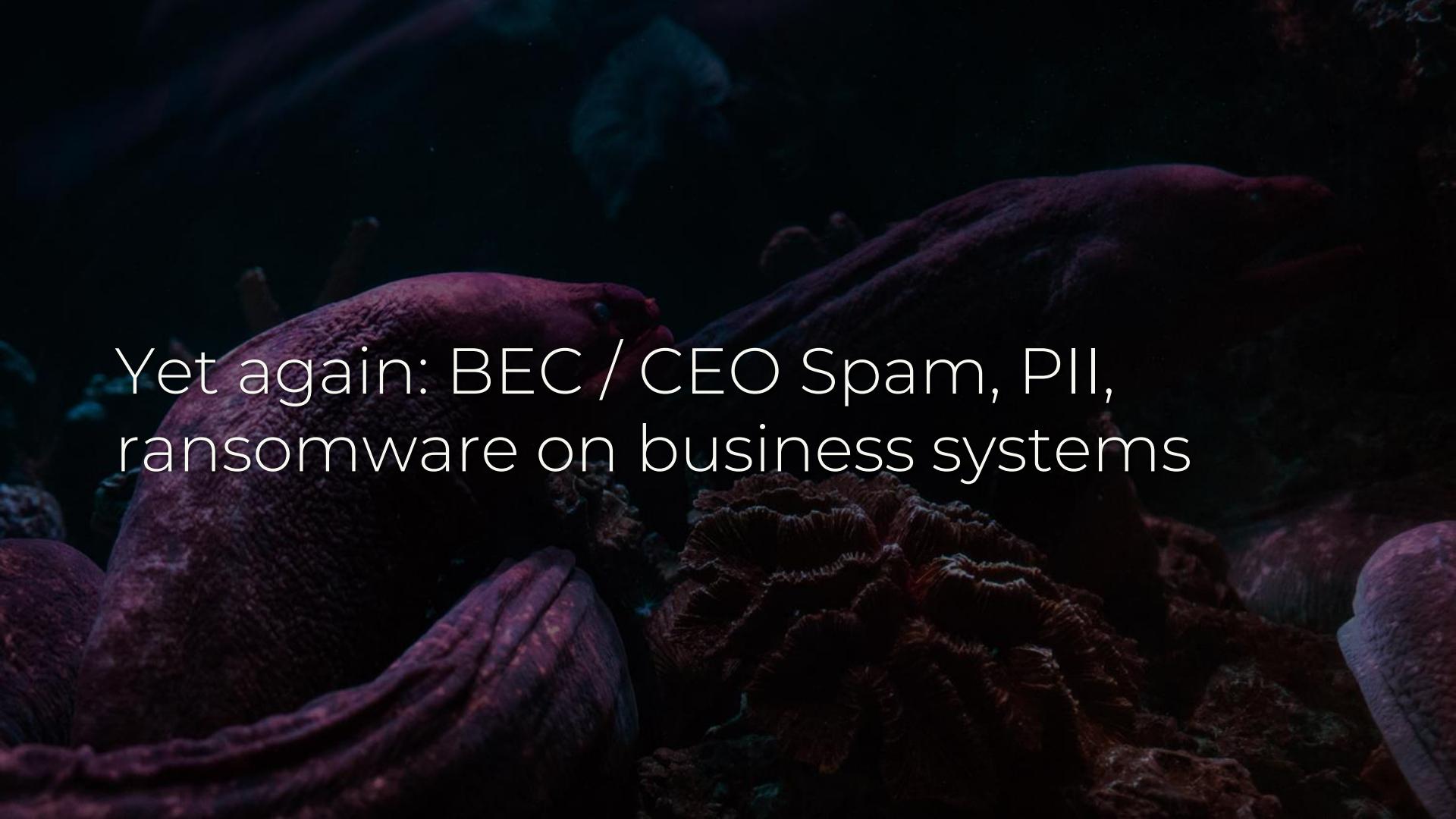
Managing fluctuating demand,  
avoiding service interruption



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, possibly white or yellow, markings. 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 bright, jagged lightning bolts striking across them, particularly on the left side. Below the clouds, a faint glow from a distant fire or explosion is visible on the horizon. The lower half of the image is a deep, dark sea, its surface slightly rippled.

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

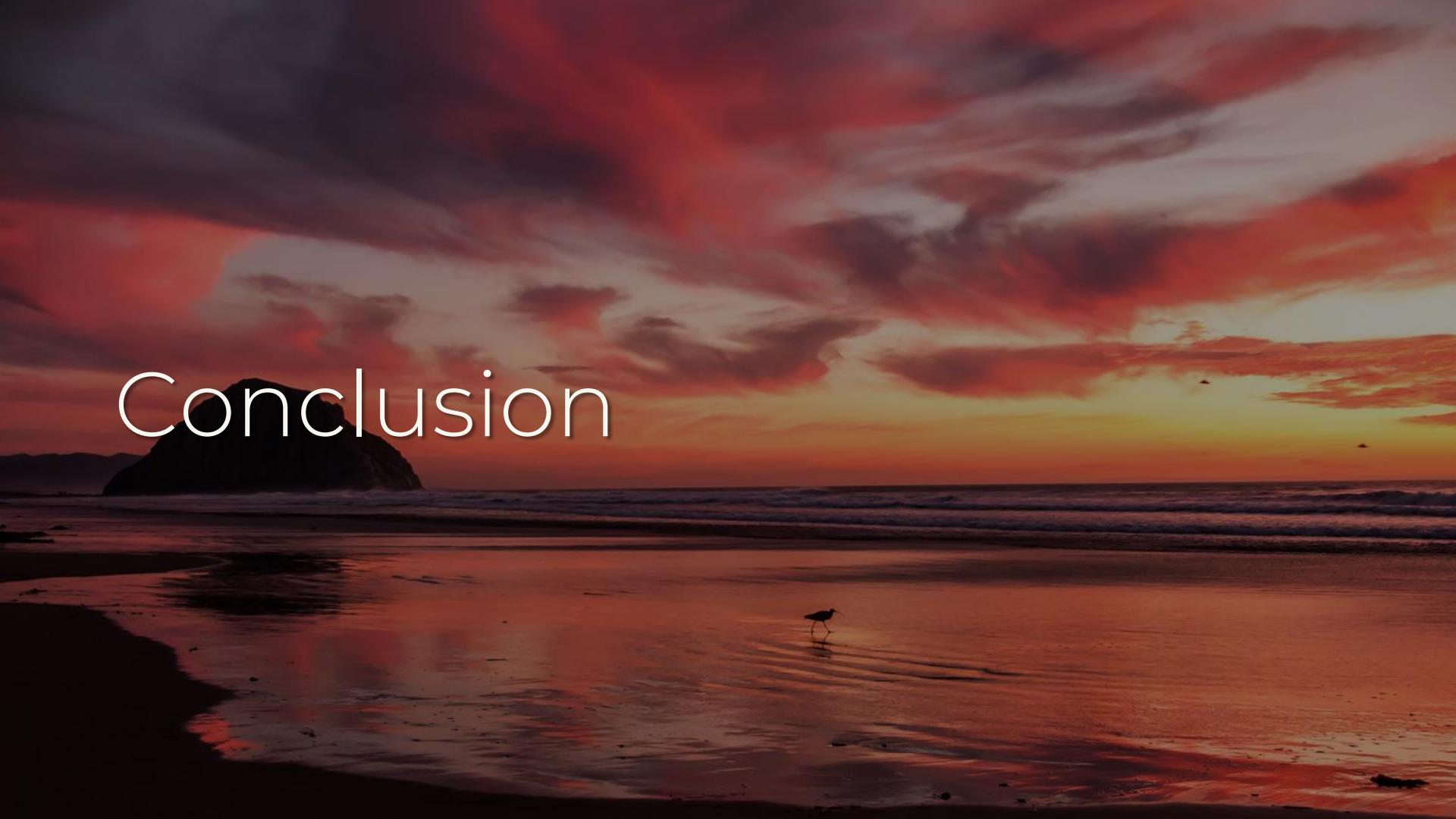
Time element expense, eg systems failure, without physical damage

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



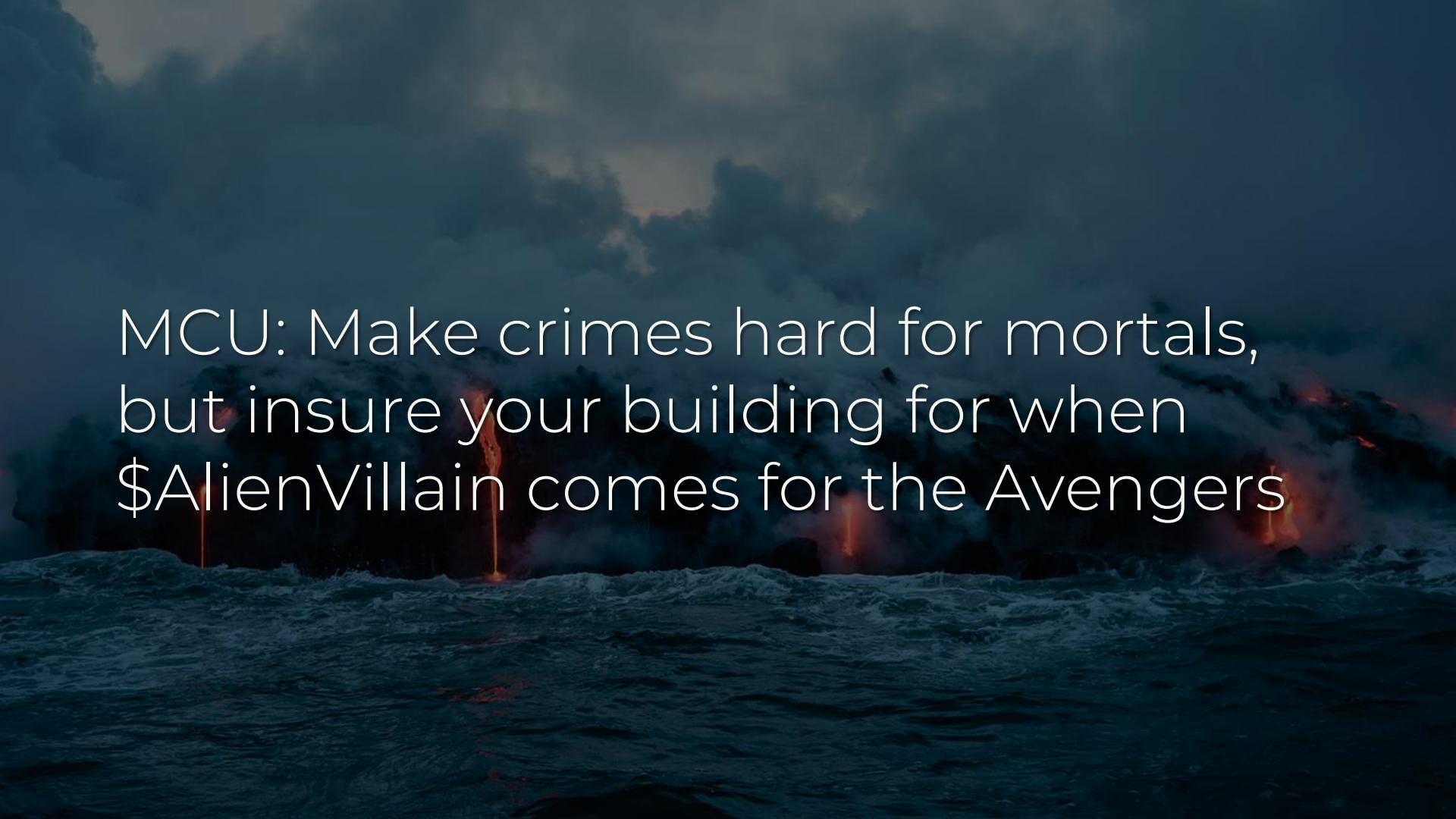
Where you can excel: how digital risks  
can connect to your business risks

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.

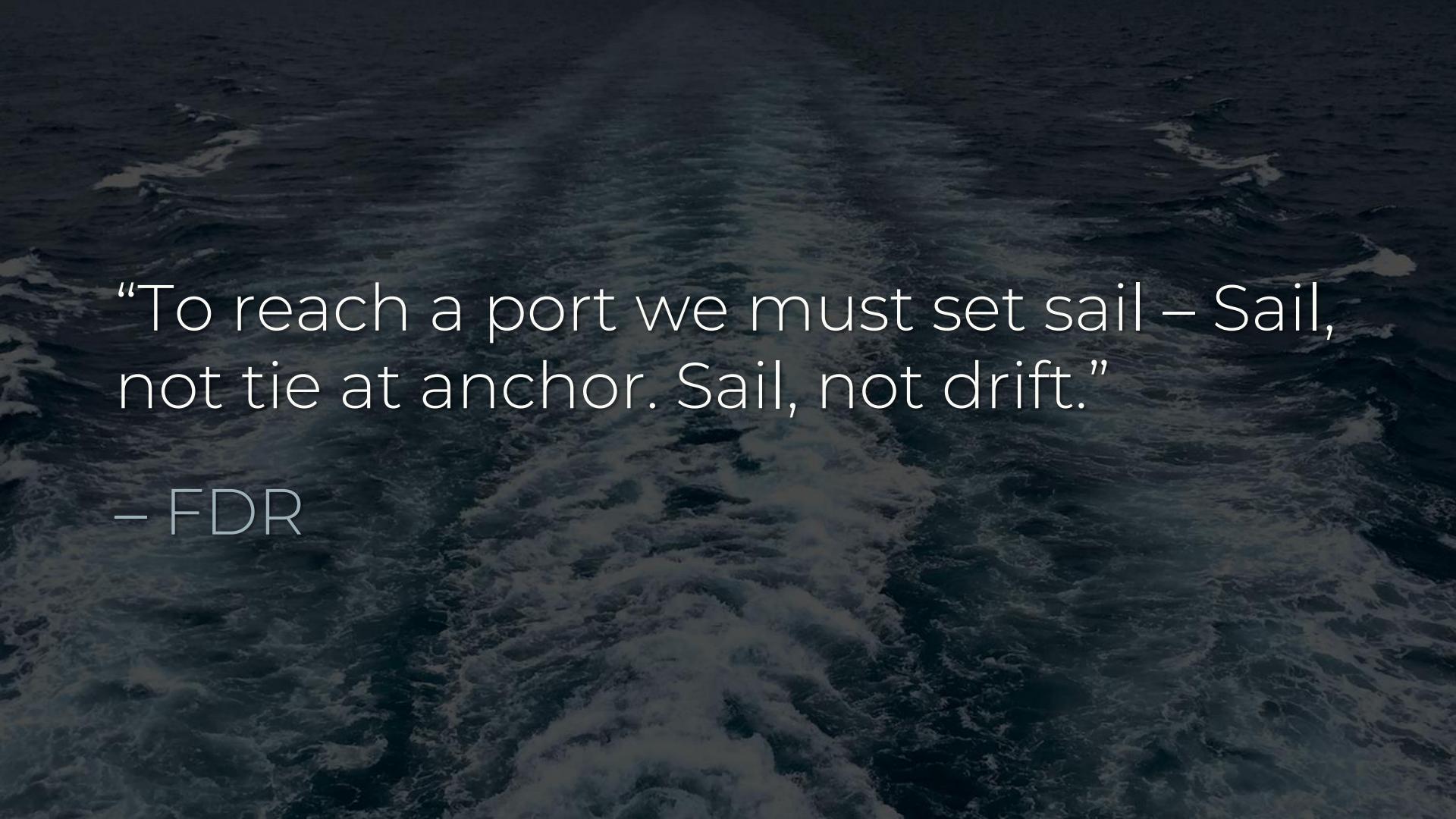
Identify where your org's risks meet  
what attackers actually want



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

The background of the image is a dark, moody landscape featuring a lava flow from a volcano. The lava is bright orange and red, contrasting sharply with the dark, turbulent ocean waves in the foreground. Above the horizon, a heavy cloud cover of dark grey and black clouds hangs over the scene, 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