



Threat Prioritization: Freeing the White Whale

Kelly Shortridge (@swagitda_)

HackNYC 2018



Hi, I'm Kelly



SecurityScorecard

The background of the image is a dark, moody photograph of ocean waves. The water is a deep, dark blue, and the white foam of the waves is visible, creating a textured, turbulent appearance. The lighting is low, emphasizing the dark tones of the water.

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

— Herman Melville, *Moby Dick*

A photograph of a whale breaching the ocean surface. The whale's back and tail are visible above the water, creating a large splash of white water. The ocean is dark blue, and the sky is a dark, overcast grey. The text is overlaid on the left side of the image.

White Whale: a relentless, self-defeating obsession

A close-up photograph of a hand holding a watch over a body of water. The watch has a dark face with light-colored hands and markers. The background is a blurred, rippling surface of water. The overall image has a dark, moody aesthetic with a semi-transparent dark overlay.

With limited time & resources, we
cannot pursue unlimited threats

An aerial photograph of a small, dark boat on a dark teal sea. The water is deep and dark, with patches of lighter, sandy or coral reef areas visible in the background. The text is overlaid on the image in a white, sans-serif font.

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

- 
- An aerial photograph of a coastline. The ocean is dark blue, and the waves are white and foamy as they crash against the shore. The land is a mix of brown and green, suggesting a natural, possibly forested or agricultural, landscape. The overall tone is somewhat somber due to the dark colors of the water and the muted colors of the land.
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 shark is shown swimming in dark blue water, viewed from a side profile. The shark's body is sleek and tapers towards the tail. The lighting is dim, highlighting the shark's form against the dark background. The text is overlaid on the lower half of the image.

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 / repackagable 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 wetsuit is suspended from a rope, hanging upside down in a dark blue underwater environment. The diver's legs are spread apart, and their arms are also spread out. The background is a deep, dark blue, suggesting a deep underwater setting. The text is overlaid on the left side of the image.

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

A photograph of several clownfish swimming in a sea anemone. The clownfish have orange bodies with white stripes and black outlines. The anemone has many long, white, pointed tentacles. The background is dark, making the clownfish and anemone stand out.

Continuing to use strategies or vendors with limited efficacy or ROI

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


A photograph of two clownfish swimming in a sea anemone. The anemone has thick, greenish-brown tentacles. The clownfish are orange with white stripes. The image is dimly lit, giving it a dark, moody appearance. The text is overlaid in the center in a white, sans-serif font.

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

A stack of smooth, light-colored rocks is balanced on a dark, rocky shore. The background shows waves crashing against the rocks under a dark, overcast sky. The text is overlaid in white, centered horizontally.

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 five-pointed starfish is centered in the background, rendered in a dark, muted brown color against a deep blue, slightly textured background. The starfish's arms are spread out, and its central disk is visible. The overall aesthetic is clean and minimalist.

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 image shows two sharks swimming in a dark, deep-sea environment. The water is a deep teal or dark blue color, with some small white particles or bubbles visible. The sharks are positioned diagonally across the frame, with one in the foreground and another slightly behind and above it. The lighting is somewhat dim, highlighting the texture of the sharks' skin and their fins.

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

The background of the slide is a dark, black ocean scene filled with numerous jellyfish. The jellyfish are primarily a vibrant magenta or purple color, with some appearing as faint blue or white shapes. They are scattered throughout the frame, some in sharp focus and others blurred, creating a sense of depth and movement. The overall aesthetic is mysterious and somewhat ethereal.

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

Criminals need monetization & deeply
care about ROI

A dark, moody background featuring a silhouette of a tree branch against a dark blue sky and ocean. The text is centered in white.

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

An underwater scene with a dark greenish-blue background. Numerous small, light-colored bubbles are scattered throughout the water, particularly concentrated in the upper right quadrant. Light rays or beams are visible, creating a shimmering effect on the water's surface and within the bubbles. The overall texture is slightly grainy, suggesting a video or high-resolution still image.

Step 3: Cross-compare results

A school of sharks swimming in dark blue water. The sharks are silhouetted against the dark background, creating a sense of movement and depth. The text is centered over the image.

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

A satellite is shown in orbit over a coastal region. The satellite consists of a central white cylindrical bus and a long array of solar panels extending horizontally. The background shows a brown, hilly landscape meeting a dark blue ocean. The text is overlaid in white on the satellite and the landscape.

Hackers are unlikely to remotely crash
your satellite into space debris

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

A clownfish with a white stripe and a white line is swimming in a blue and purple underwater environment, surrounded by purple anemones. The fish is positioned in the center-right of the frame, facing right. The background is a deep blue with purple anemones on the left and right sides.

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

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



A dark, almost black background is filled with numerous faint, glowing jellyfish. The jellyfish are scattered across the frame, some in sharp focus and others blurred, creating a sense of depth and movement. The light from the jellyfish is a pale, ethereal glow, contrasting with the dark background.

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

Financial impact analysis is an essential part of your risk assessments



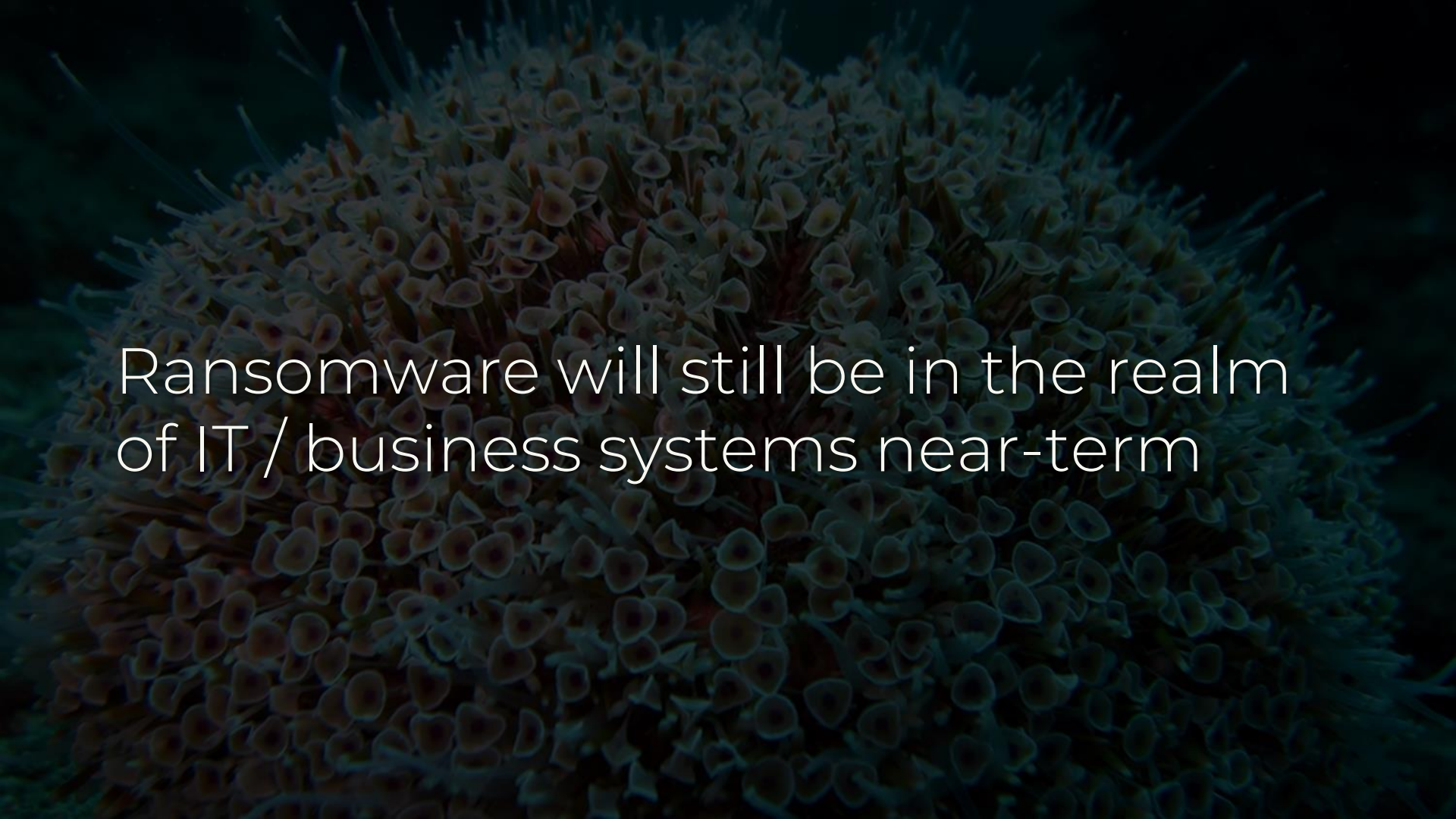
What are the 35%+ probability threats
you're underestimating?



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

A dark seal is shown in the water, attacking a white duck. The duck is being held by the seal's mouth and is being thrown into the air, with its wings and feet visible. The water is dark blue and has some white foam from the splash. The background shows a dark, rocky shoreline.

DDoS attacks – spam or ransom

A dense field of small, light-colored flowers or seedlings, possibly a type of clover or similar plant, growing in a dark, shadowed environment. The plants are tightly packed and their colors range from pale yellow to light green, contrasting sharply with the dark background.

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

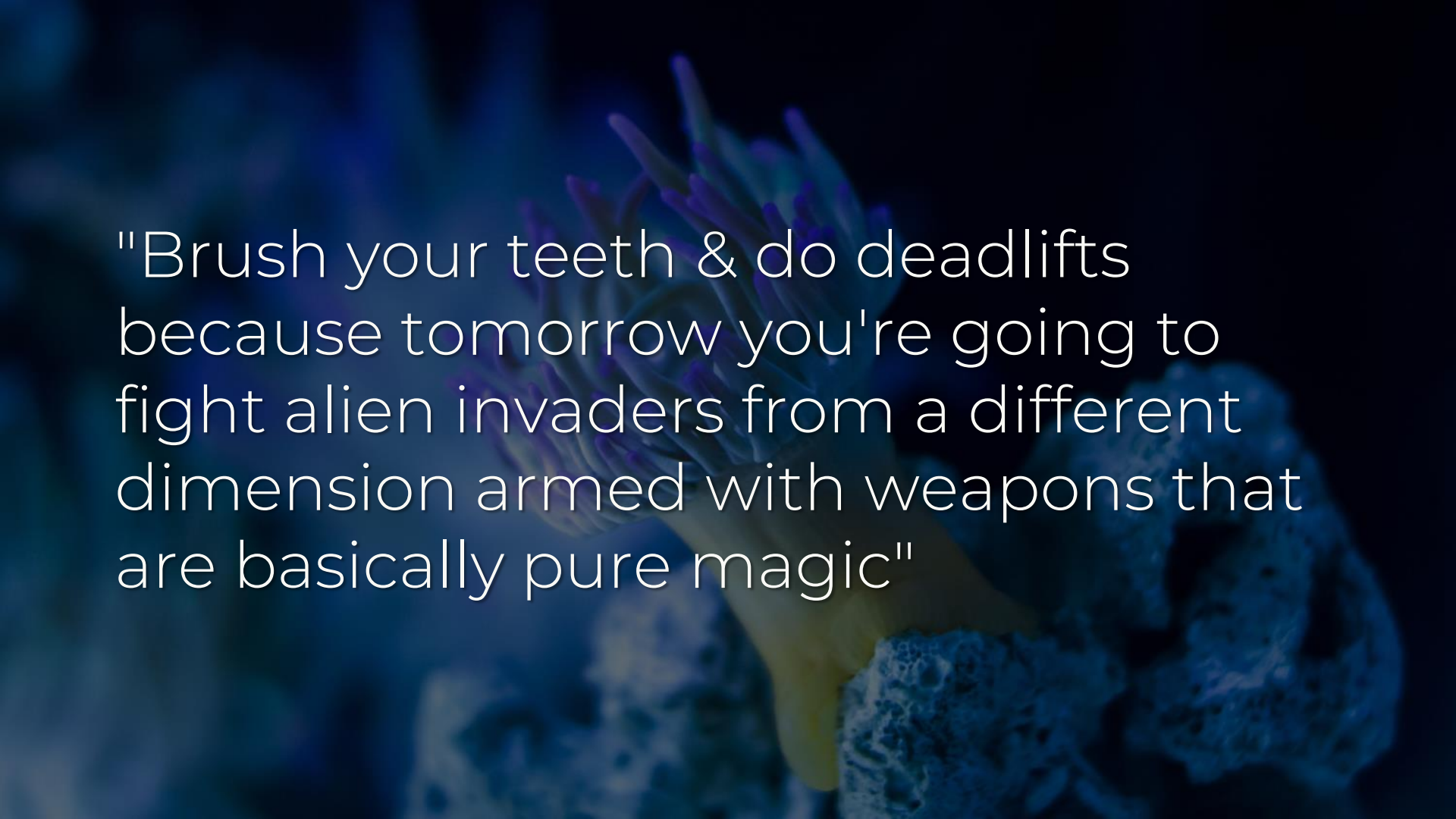
Time & resources required to port
ransomware to OT = poor ROI

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

A photograph of two orcas breaching the water surface. The orca on the left is in the foreground, its head and back visible above the water. The orca on the right is slightly behind and to the right, also breaching, with a splash of water around its head. The water is dark blue-grey. The text is overlaid in the center of the image.

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

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

A hand holding a glowing blue and purple alien weapon against a dark blue background. The weapon has a yellow handle and a blue, crystalline body with purple, spiky protrusions. The background is a dark blue gradient with some blurred, glowing elements.

"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?

A dark, stormy ocean at night with a lightning bolt striking the water. The sky is dark with some light clouds, and the water is dark with some white foam from waves. A bright lightning bolt strikes the water in the distance, creating a bright flash and a small plume of white water. The overall mood is dramatic and ominous.

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

A flying fish is captured mid-leap, its wings fully extended, as it moves from the surface of the water into the air. The water is a deep, dark blue with visible ripples and a splash of white foam where the fish exited. The fish is positioned in the upper right quadrant of the frame. The overall scene is set against a dark, moody background of the ocean.

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 politics / terrorism

Nation-states also want leverage in negotiations – business data

The background of the slide features two eels with a mottled, spotted pattern in shades of blue and white. They are positioned in a dark, monochromatic blue environment, possibly underwater. The eel on the left is larger and more prominent, while the one on the right is smaller and partially obscured. The overall lighting is dim, creating a mysterious and somewhat ominous atmosphere.

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

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

The background is a dark teal color with a dynamic splash of water. Numerous small, clear water droplets are scattered across the frame, creating a sense of movement. In the lower right quadrant, a slice of bright orange citrus fruit is visible, partially submerged. To its left, a single, dark red strawberry is also present. The overall composition is clean and modern, with the text overlaid in a white, sans-serif font.

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

Insurance, redundancy, & serenity
prayer for physical assets

A night sky photograph featuring the Milky Way galaxy. The galaxy's bright, star-filled band stretches diagonally across the frame from the upper left towards the lower right. In the foreground, the dark silhouette of a utility pole stands prominently, with its cross-arms and insulators visible. Several power lines extend from the pole across the sky. The background is a deep, dark blue, densely populated with stars. The overall scene is a blend of natural celestial beauty and human-made infrastructure.

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

A large, textured, brownish rock formation, possibly a biological specimen or a mineral deposit, is the central focus of the image. It has a rough, porous appearance with various shades of brown and tan. The background is a dark, deep blue-green, suggesting an underwater environment. The overall lighting is dim, creating a moody and somewhat mysterious atmosphere.

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

A large school of fish swimming in deep blue water, with a dark silhouette of a forest in the foreground.

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?

An aerial photograph of a forest, showing a complex network of tree canopies. The image is overlaid with a dark teal color, which makes the text stand out. The text is centered and reads:

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

A dramatic sunset or volcanic eruption over a dark sea with a rocky cliff in the foreground. The sky is filled with dark, heavy clouds, and the horizon is a mix of deep blue and purple. The water is dark, with some lighter patches reflecting the light from the sky. The foreground shows a dark, jagged rock formation.

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?

A dark, stormy sky with a bright lightning bolt striking down from the clouds, illuminating the scene. The lightning bolt is the central focus, with its energy radiating outwards. The background is a deep, dark blue-black, with some lighter, hazy clouds visible near the horizon.

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

A wide-angle photograph of a beach at sunset. The sky is filled with large, dark clouds illuminated from below by the setting sun, creating a palette of deep reds, oranges, and yellows. The sun is positioned on the right side of the horizon, just above the ocean. In the foreground, the wet sand of the beach reflects the vibrant colors of the sky. A single bird is walking in the shallow water on the right side of the frame. On the left, a large, dark rock formation juts out into the sea. The overall mood is serene and contemplative.

A photograph of a whale's tail fluke emerging from the ocean surface. The tail is dark and curved, with water splashing around its base. The background is a vast, dark blue ocean under a dark sky.


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

A photograph of several dolphins swimming in the ocean. The water is a deep, dark blue with gentle ripples. The dolphins' dark, sleek bodies are partially visible above the surface, with their dorsal fins prominently shown. One dolphin in the foreground is creating a splash of white water as it moves. The overall scene is serene and natural.

Free yourself from the burden of
defending against all threats



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

An underwater photograph showing a large school of dark fish swimming in the upper right, and a smaller school of yellow-striped fish in the upper left. In the lower left, there is a coral reef with several bright orange fish. The background is a deep, dark blue, suggesting a deep-sea environment.

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