

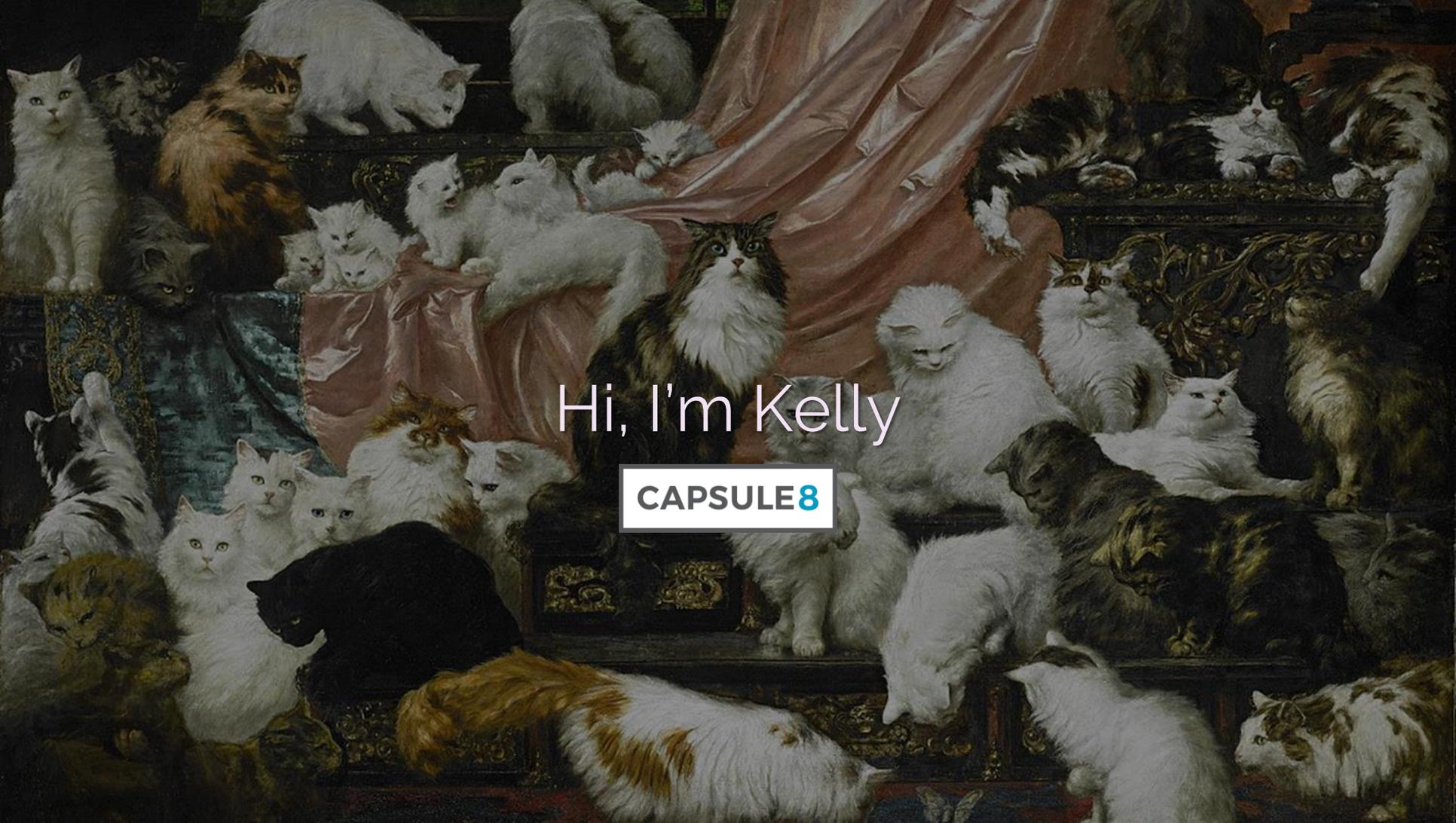
A man in a dark coat stands on a rocky outcrop, looking out over a misty, mountainous landscape. The scene is atmospheric and somewhat somber, with a large, dark rock formation in the foreground and a hazy, mountainous background. The man is seen from behind, looking towards the horizon.

# TO ERR IS HUMAN:

## The Complexity of Security Failures

Kelly Shortridge (@swagitda\_)

Hacktivity 2019 Keynote



Hi, I'm Kelly

CAPSULE 8

“To err is human; to forgive, divine.”  
– Alexander Pope

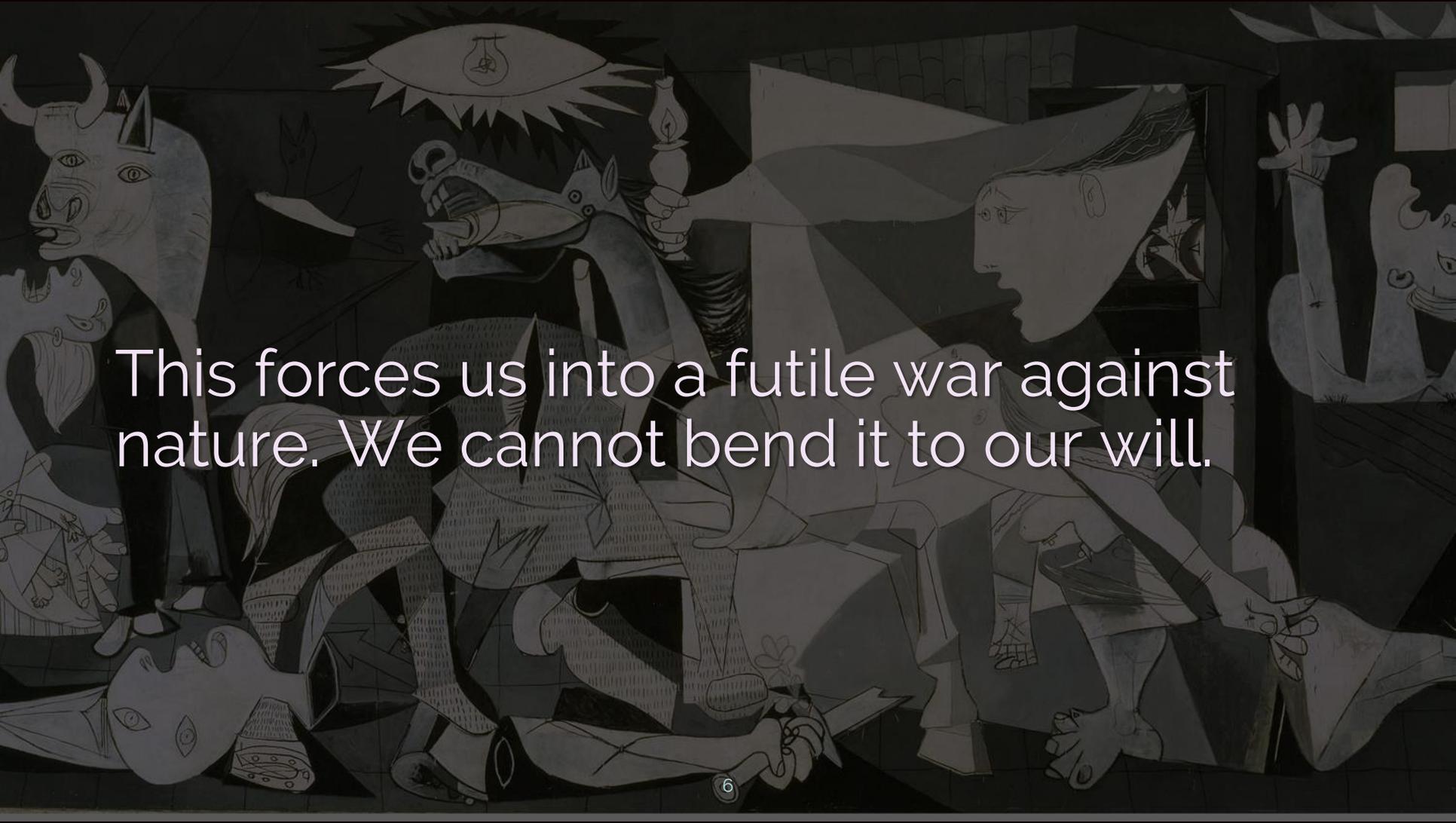




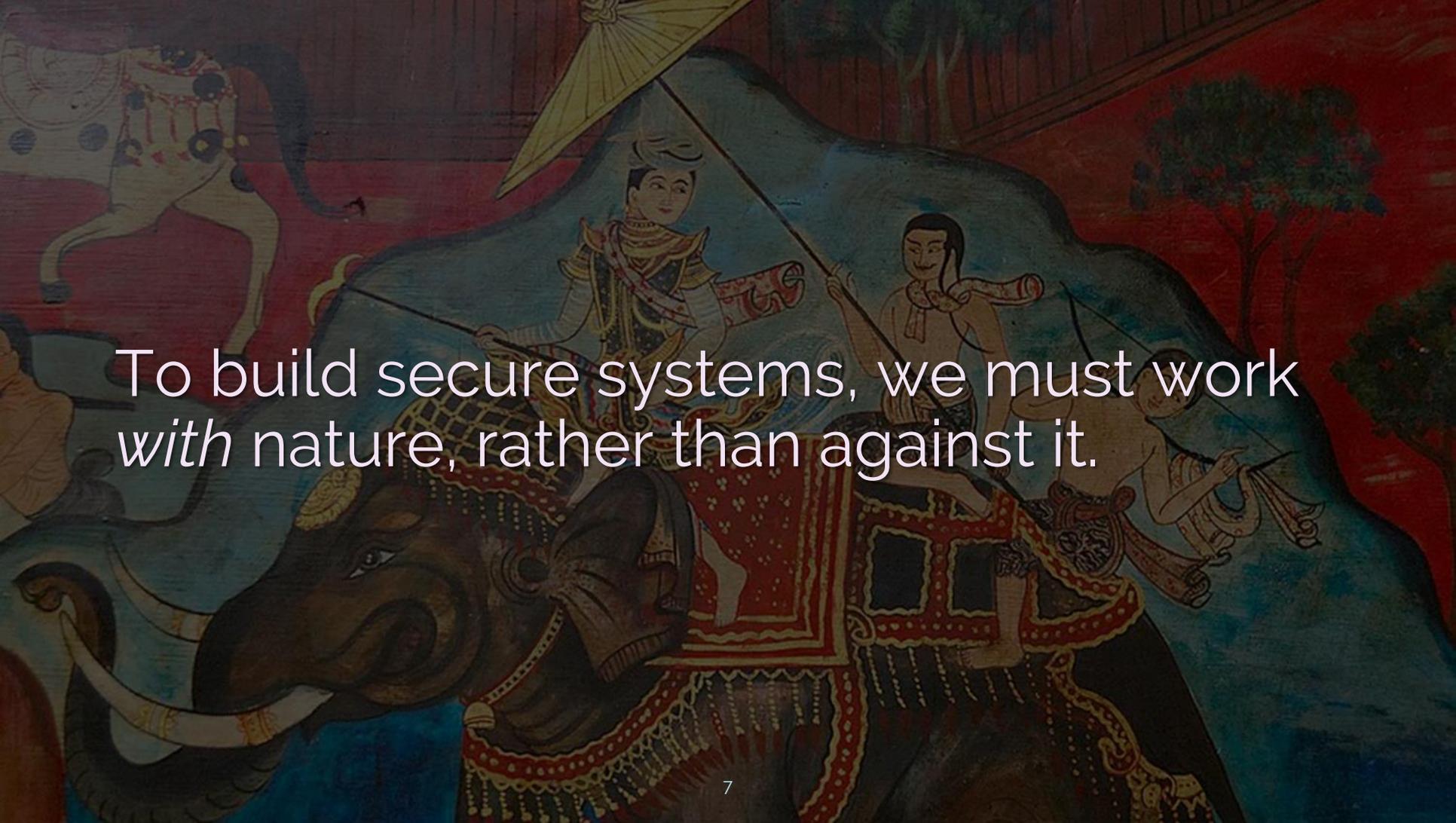
Humans make mistakes. It's part of our nature (it's mostly a feature, not a bug)

Infosec's mistake: operating as if you can force humans to never err





This forces us into a futile war against nature. We cannot bend it to our will.



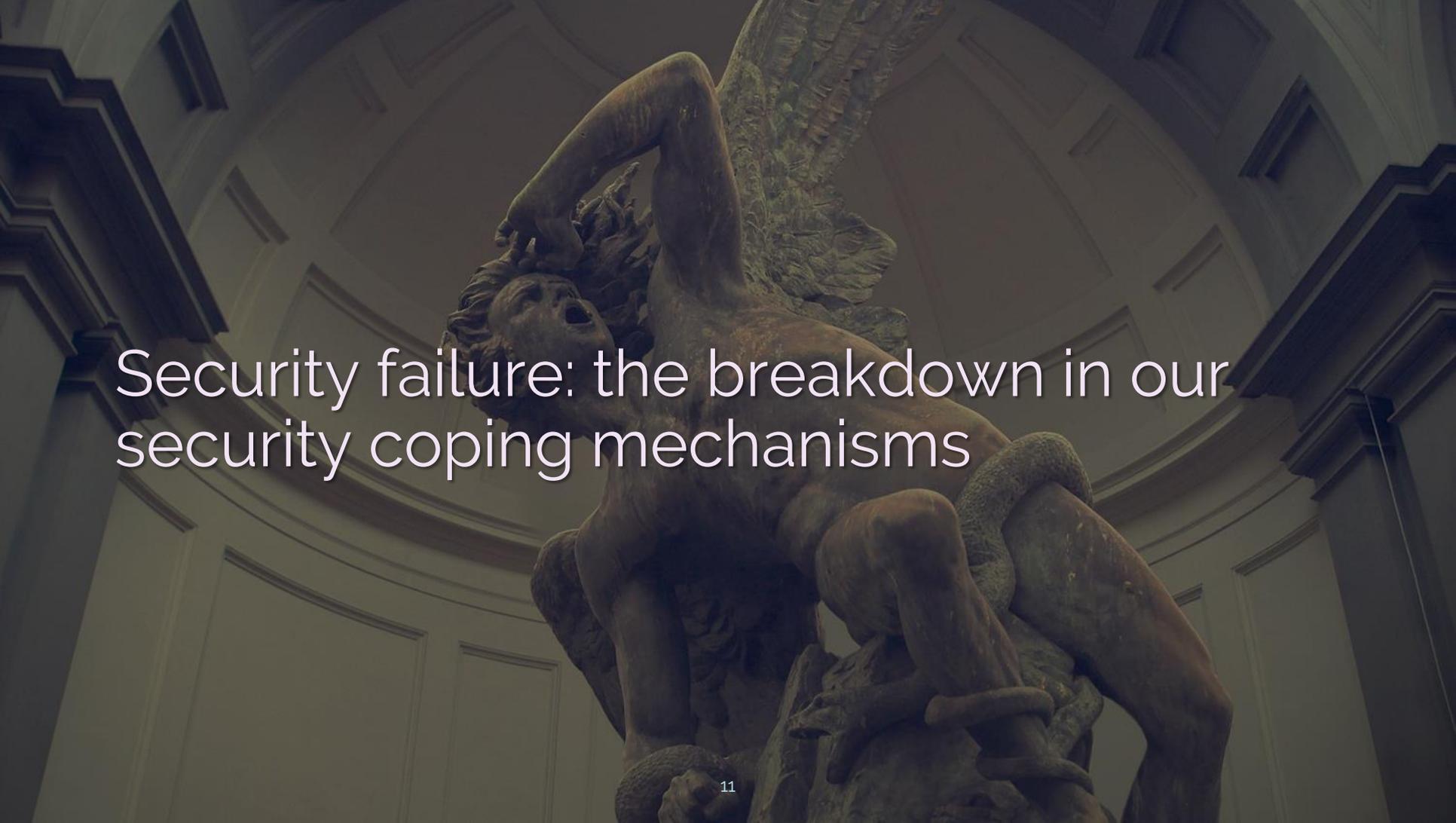
To build secure systems, we must work *with* nature, rather than against it.

1. Clearing the Err
2. Hindsight & Outcome Bias
3. Unhealthy Coping Mechanisms
4. Making Failure Epic

The background of the image is a reproduction of the painting 'The Starry Night' by the Dutch Impressionist painter J.M.W. Turner. The painting depicts a night scene with a turbulent, swirling sky filled with stars and a bright, glowing moon. The foreground shows a dark, silhouetted landscape with a prominent cypress tree on the left and a small town with a church spire in the distance. The overall mood is one of awe and wonder, capturing the beauty and mystery of the night sky.

Clearing the Err

Error: an action that leads to failure or that deviates from expected behavior



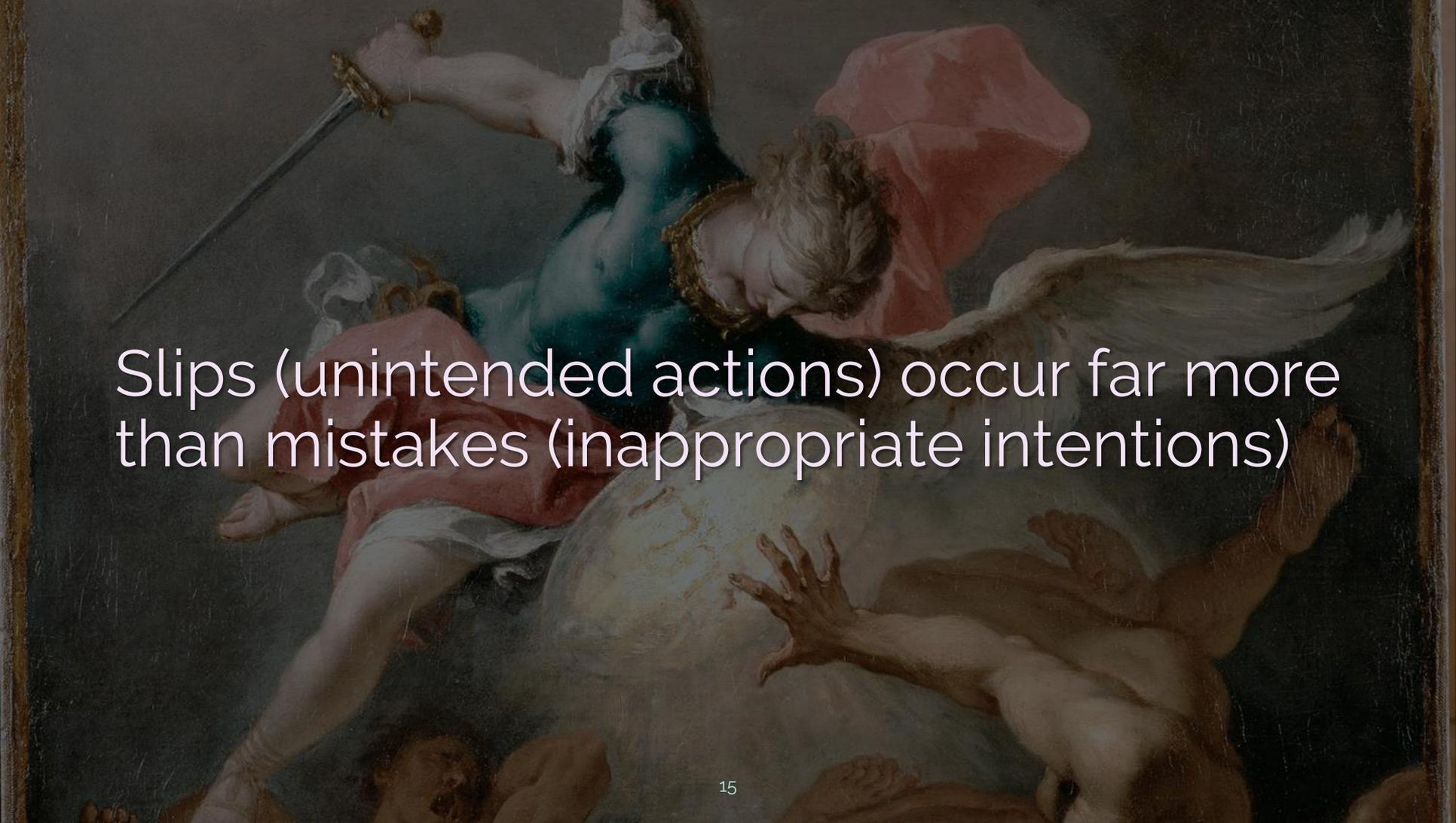
# Security failure: the breakdown in our security coping mechanisms

“Human error” involves subjective expectations, including in infosec

A Renaissance-style painting depicting Christ as a muscular, shirtless figure with a red cloak, standing on a large, multi-headed serpent. Christ holds a wooden staff in his right hand and a chain in his left. The serpent is coiled around his legs. In the foreground, a child in a Roman-style helmet and tunic holds a human skull. A banner with Latin text is draped across the scene. The background shows a landscape with trees, a distant city, and a crucifix. The overall tone is dramatic and allegorical.

Understanding why incidents happened is essential, but blame doesn't help

Aviation, manufacturing, & healthcare  
are already undergoing this revolution

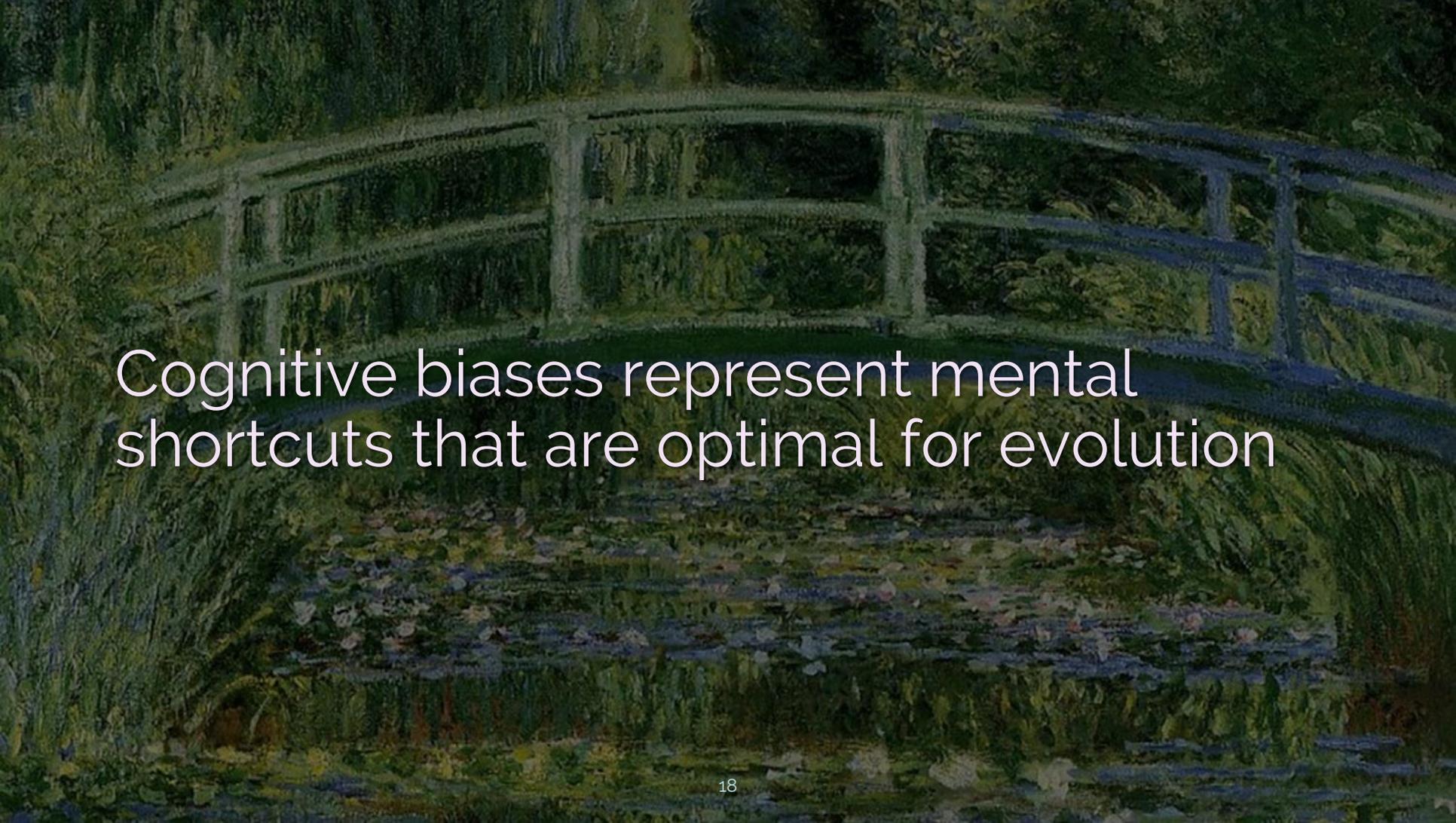


Slips (unintended actions) occur far more than mistakes (inappropriate intentions)

The term “human error” is less grounded to reality than we believe...

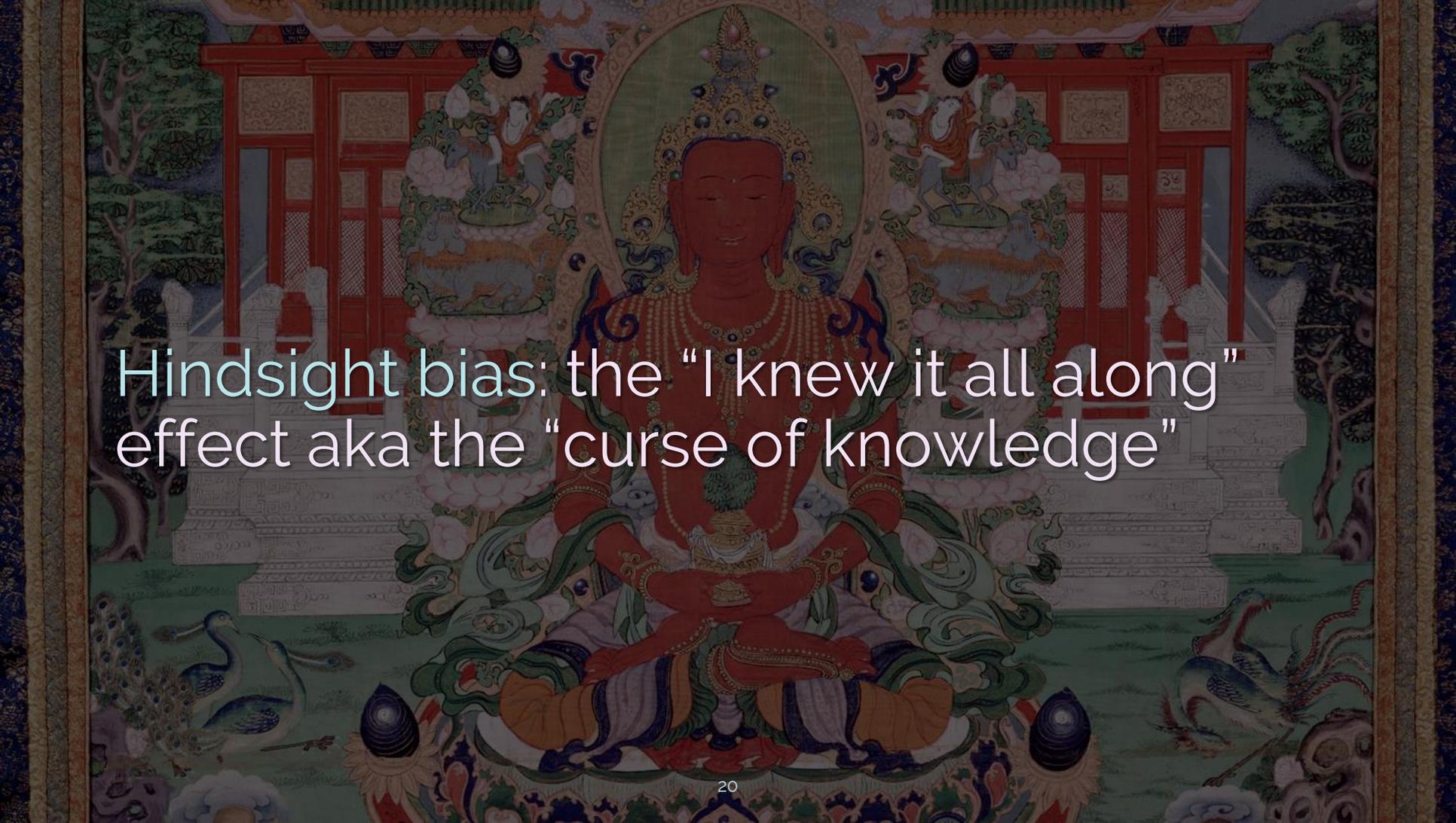


# Hindsight & Outcome Bias

The background is a painting of a stone bridge with a wooden railing, crossing a stream. The scene is surrounded by dense, lush green foliage and trees. The painting style is impressionistic, with visible brushstrokes and a rich, textured appearance. The overall color palette is dominated by various shades of green, with some brown and grey tones in the bridge and foliage.

Cognitive biases represent mental shortcuts that are optimal for evolution

We learn from the past to progress, but our “lizard brain” can take things too far

A traditional Tibetan Buddhist thangka painting. The central figure is a Buddha seated in a meditative posture (Padmasana) on a lotus throne. The Buddha has a serene expression, closed eyes, and is wearing a red robe with intricate gold jewelry. The background features a red wooden structure with white panels, possibly a palace or a temple. The scene is surrounded by lush greenery, trees, and various animals like peacocks and storks. The overall style is characteristic of traditional Tibetan art, with vibrant colors and detailed patterns.

Hindsight bias: the “I knew it all along”  
effect aka the “curse of knowledge”

People overestimate their predictive abilities when lacking future knowledge

e.g. skepticism of N.K. attribution for the Sony Pictures leak; now it is “obvious”



Outcome bias: judging a decision based on its eventual outcome

Instead, evaluate decisions based on what was known at that time

An ancient Egyptian painting depicting a domestic scene. A man on the left, wearing a blue and white headband and a patterned kilt, sits on the floor. A woman in the center, wearing a white dress and a headband, sits on a chair, looking towards the man. A child on the right, wearing a yellow headscarf and a patterned dress, sits on the floor. They are gathered around a low, ornate table with a red and white striped top. On the table and floor are various game pieces, including small wooden pegs and a black and white board. The background shows a wall with a floral pattern and a doorway leading to an outdoor area with trees.

All decisions involve some level of risk.  
Outcomes are largely based on chance.

We unfairly hold people accountable for events beyond their control



e.g. CapitalOne – did the breach really represent a failure in their strategy? (No.)

These biases change how we cope with failure...



# Unhealthy Coping Mechanisms



Unhealthy coping mechanism #1:  
Blaming “human error”

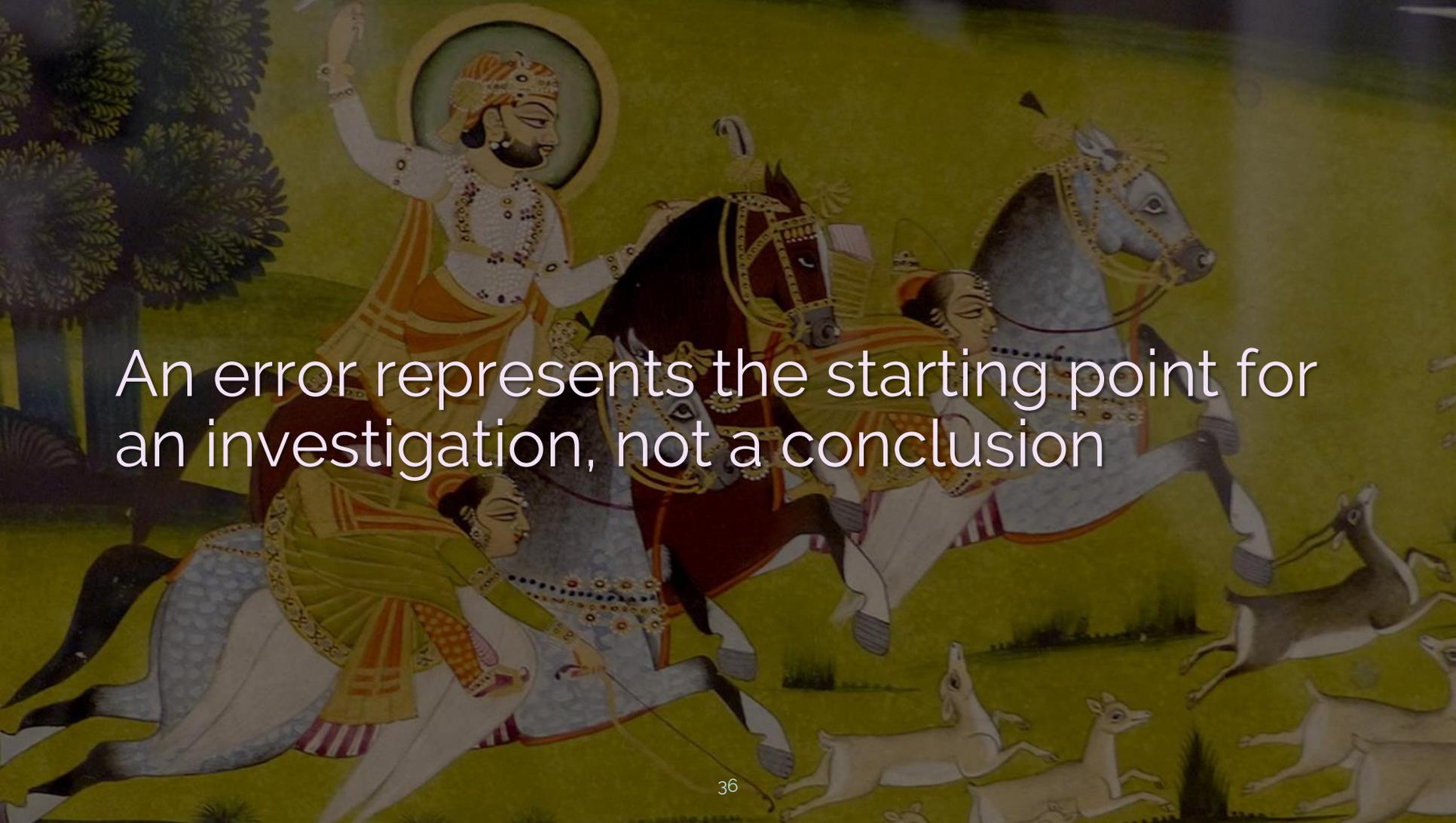
Infosec's fav hobbies: PICNIC & PEBKAC

This isn't about removing accountability  
— malicious individuals certainly exist

獲需  
以  
溪  
重

Fundamental attribution error: your actions reflect innate traits, mine don't

“You are inattentive, sloppy, & naïve for clicking a link. I was just super busy.”



An error represents the starting point for an investigation, not a conclusion

“Why did they click the link?”

“Why did clicking a link lead to pwnage?”

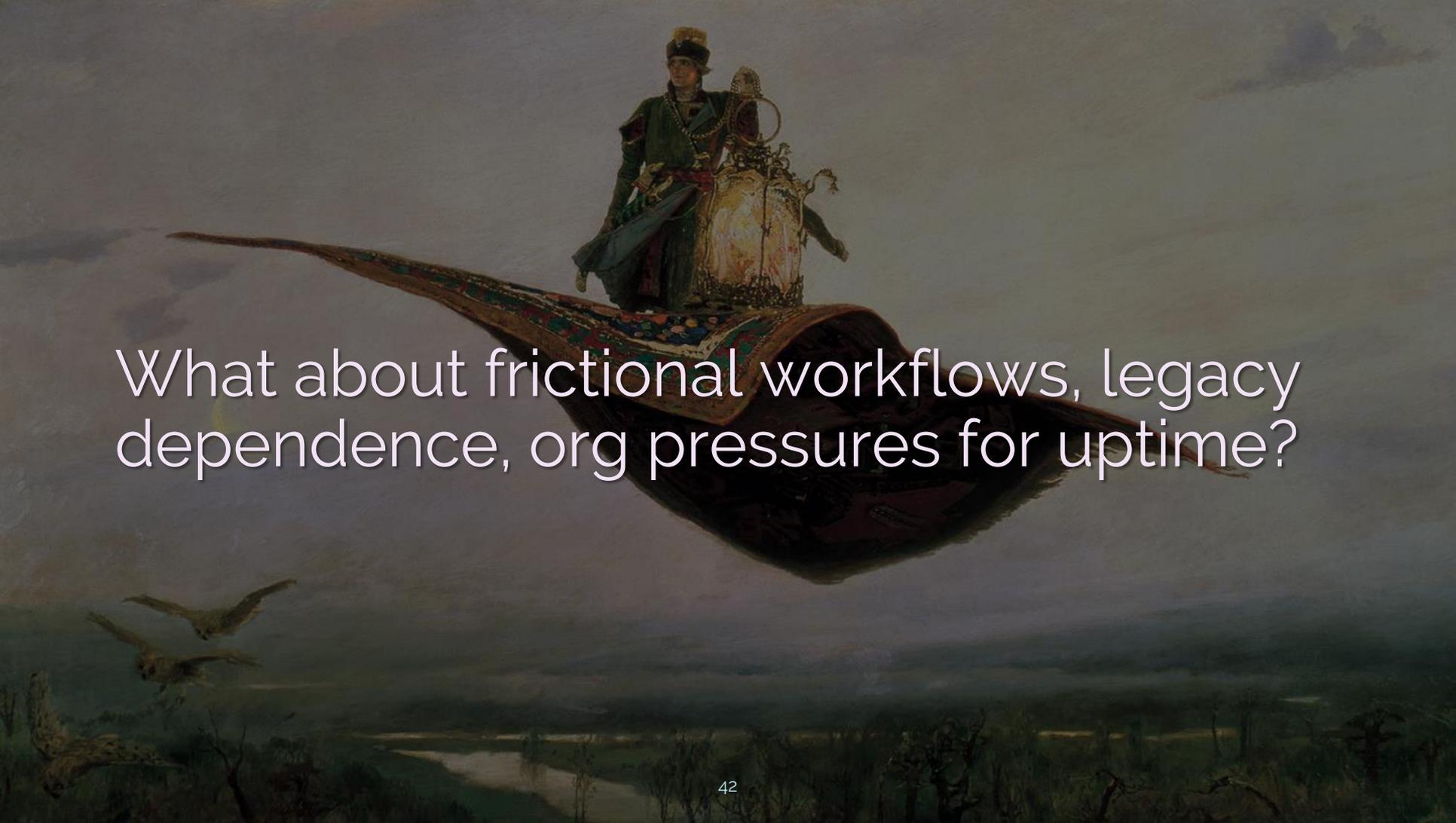
These questions go unanswered if we accept the “human error” explanation



e.g. training devs to “care about security”  
completely misses the underlying issue

A “5 Whys” approach is a healthy start

Equifax's ex-CEO blamed "human error" for the breach. He was wrong.



What about frictional workflows, legacy dependence, org pressures for uptime?

90% of breaches cite “human error” as the cause. That stat is basically useless.

A dark, dramatic painting depicting a man lying on his back, bound with chains, and being attacked by a large eagle. The man has a pained expression, and the eagle is perched on his chest, pecking at him. The background is a dark, stormy sky with jagged, dark rock formations. The overall mood is one of suffering and helplessness.

Bad theory: if humans are removed from the equation, error can't occur



Unhealthy coping mechanism #2:  
Behavioral control

“An approach aimed at the individual is the equivalent of swatting individual mosquitoes rather than draining the swamp to address the source of the problem.”

– Henriksen, et al.

“Policy violation” is a sneaky way to still  
rely on “human error” as an answer

A classical painting depicting a woman in a red and yellow dress holding a cornucopia, surrounded by an abundance of fruit and a man in a floral wreath. The scene is set in a lush, dark forest with a path leading into the distance. The woman is the central figure, holding a large, overflowing basket of fruit. The man is seated next to her, looking at her with a smile. The background shows a path leading into a wooded area with other figures in the distance. The overall mood is one of abundance and tranquility.

The cornucopia of security awareness  
hullabaloo is a direct result of this

Solely restricting human behavior will never improve security outcomes.

We focus on forcing humans to fit our ideal mold vs. re-designing our systems

A traditional Indian painting of the goddess Durga. She is depicted with five faces and ten arms. She wears a crown and is adorned with jewelry. Her arms hold various weapons: a trident (trishula), a sword (khadga), a mace (gada), a conch shell (shankha), a lotus flower, and a bow. She is surrounded by a dense background of peacock feathers. The text 'Formal policies are rarely written by those in the flow of work being policed' is overlaid on the image in white font.

Formal policies are rarely written by those in the flow of work being policed

Infosec is mostly at the “blunt” end of systems; operators are at the “sharp” end



People tend to blame whomever resides  
closest to the error

Operator actions “add a final garnish to a lethal brew whose ingredients have already been long in the cooking.”

– James Reason

e.g. Equifax's 48-hour patching policy  
that was very obviously not followed

Creating words on a piece of paper &  
expecting results is... ambitious

A painting of a long-haired goat with a red collar, standing in a desolate, rocky landscape. The background features rugged mountains under a cloudy sky. The text is overlaid on the image.

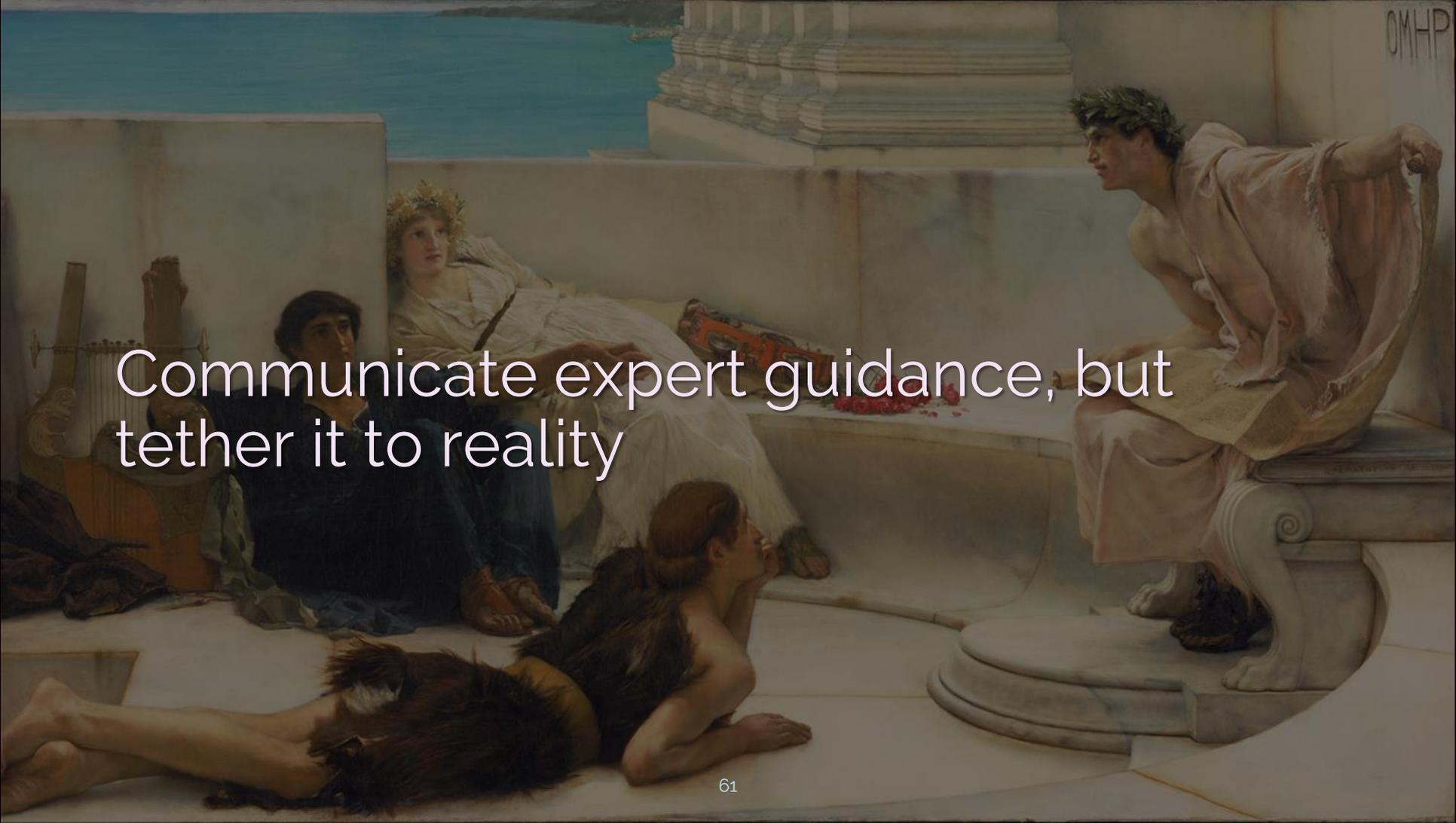
Discipline doesn't actually fix the "policy violation" cause (but it does scapegoat)

# Case study: SS&C & BEC



Solely implementing controls to regulate human behavior doesn't beget resilience

Post-W/WII analysis: Improved design of cockpit controls won over pilot training



Communicate expert guidance, but  
tether it to reality

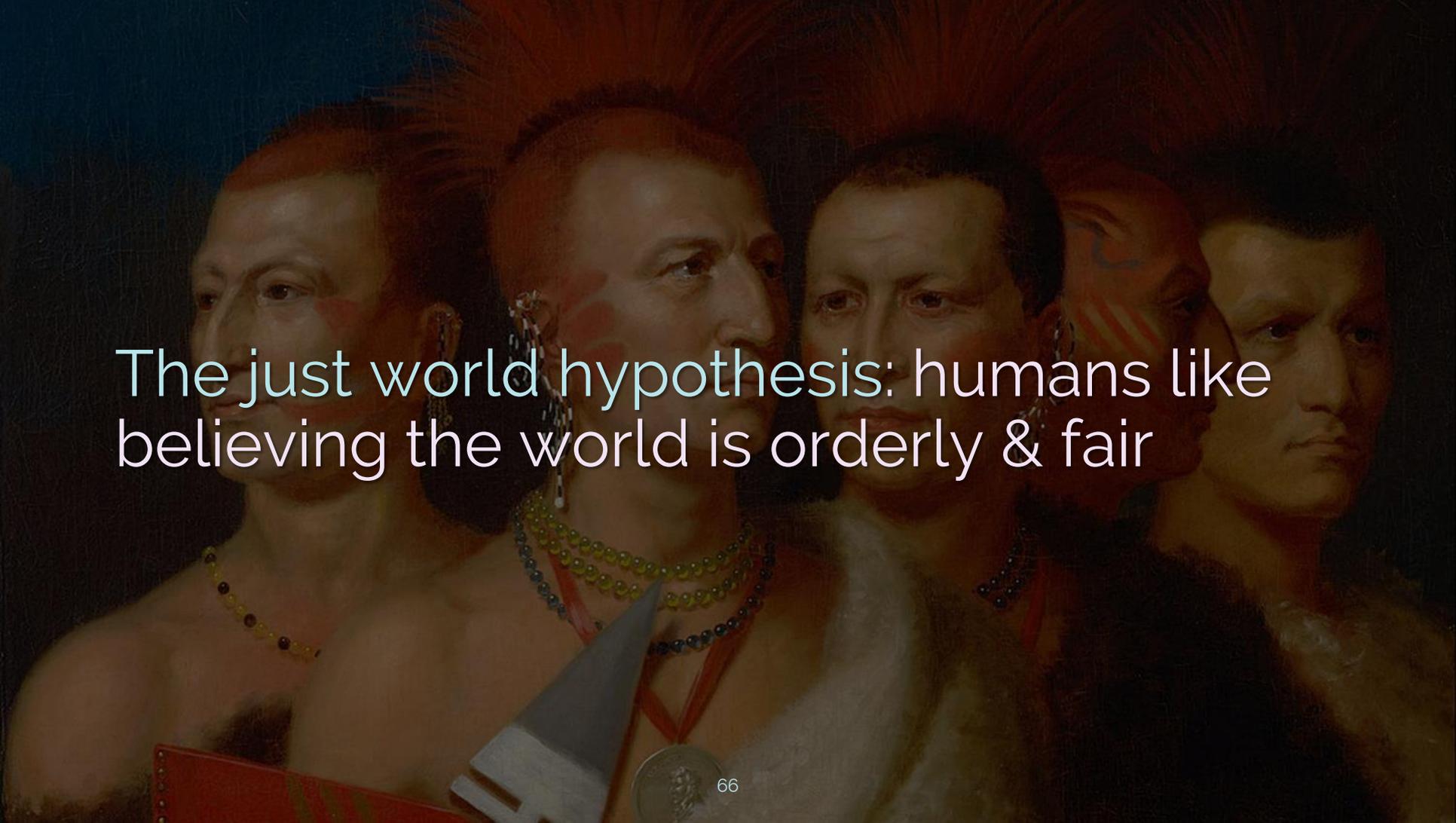
Checklists can be valuable aids *if* they're based on knowledge of real workflows

Policies must encourage safer contexts,  
not lord over behavior with an iron fist.



Unhealthy coping mechanism #3:  
The just-world hypothesis

Attempting to find the ultimate causal  
seed of failure helps us cope with fear

A detail from Hans Memling's painting 'The Ambassadors' (1480), showing five indigenous people from the Americas. They are depicted from the chest up, wearing various beaded necklaces and large feathered headdresses. The background is dark and textured. The text 'The just world hypothesis: humans like believing the world is orderly & fair' is overlaid in white on the left side of the image.

The just world hypothesis: humans like believing the world is orderly & fair

The fact that the same things can lead to both success & failure isn't a "just world"

A dramatic painting of a volcanic eruption. A massive plume of ash and smoke rises from a crater, filling the sky. In the foreground, two small figures stand on a rocky ledge, looking out over the scene. The background shows a valley with a lake and distant mountains under a hazy sky.

# Case Study: The Chernobyl disaster

Errors are really symptoms of pursuing goals while under resource constraints

How can security teams more productively deal with security failures?

# Making Failure Epic



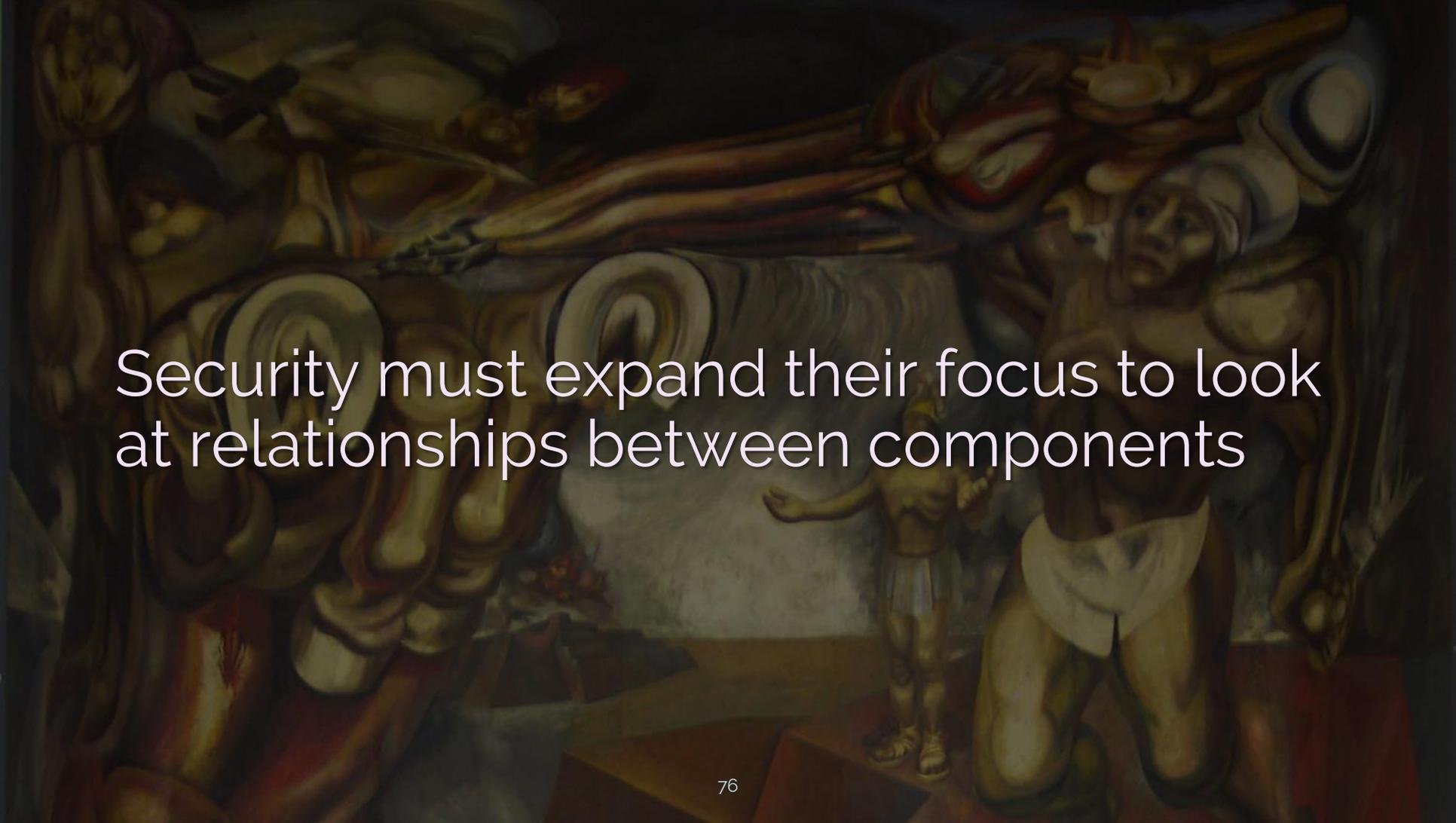
Infosec will progress when we ensure  
the easy way is the secure way

1. System perspective
2. Security UX
3. Chaos security engineering
4. Blameless culture

The background is a complex abstract painting. It features a variety of geometric shapes including rectangles, squares, circles, and triangles. A prominent red triangle points downwards from the top left. A large yellow rectangle is positioned in the center-left. To the right, there are several overlapping shapes in shades of blue, purple, and red. A thick black curved line sweeps across the right side. The background is filled with a mix of colors, including light blue, yellow, and brownish tones. There are also several thin black lines and a grid-like pattern of small squares in the lower right quadrant. The overall composition is dense and layered.

System perspective

Security failure is never the result of one factor, one vuln, or one dismissed alert

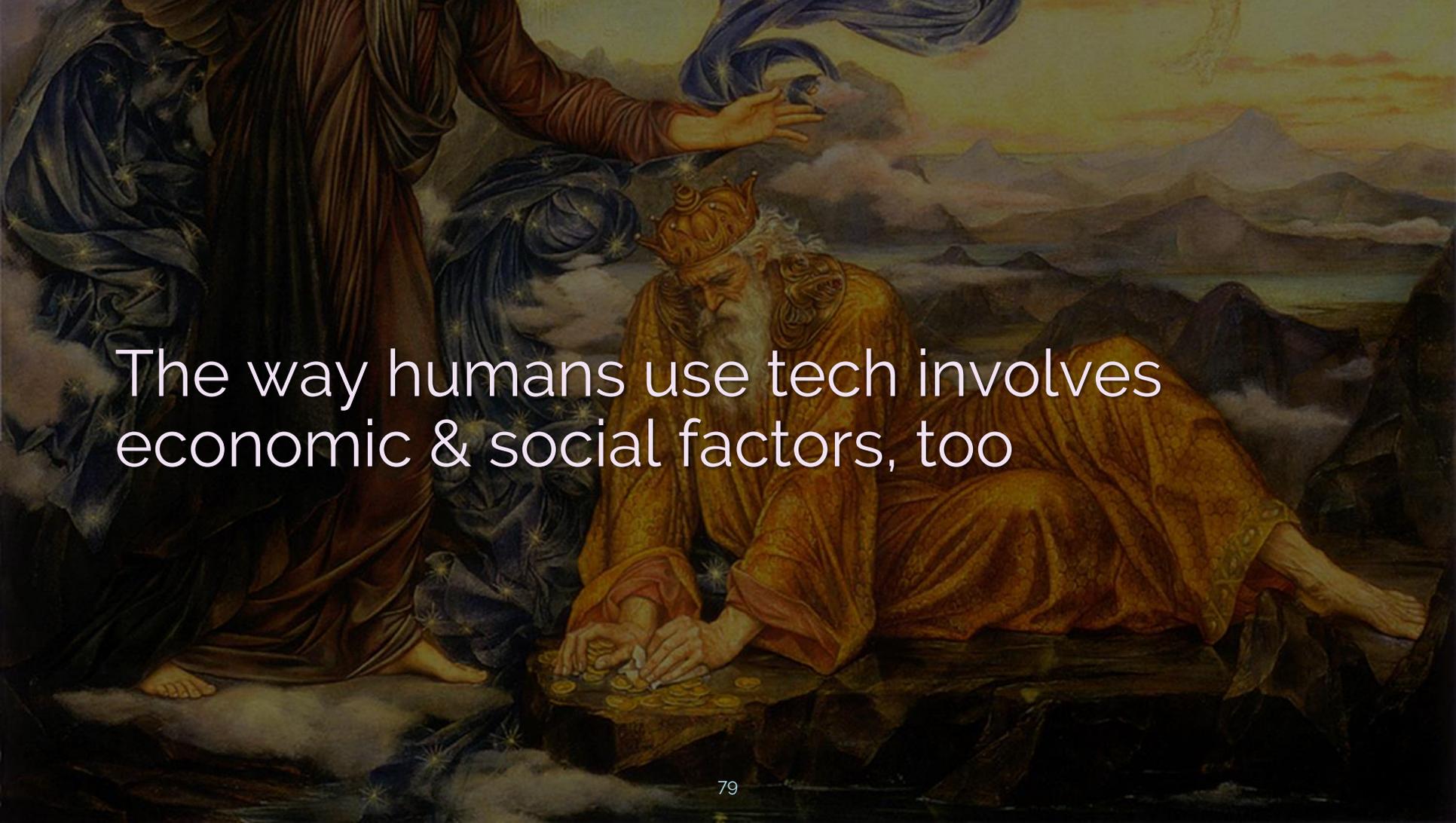
The background is a dark, textured image of a complex, abstract painting. It features several figures, including a prominent one on the right wearing a white headwrap and a white loincloth. The painting has a dense, layered appearance with swirling patterns and various colors like yellow, brown, and white. The overall mood is somber and intricate.

Security must expand their focus to look at relationships between components

A system is “a set of interdependent components interacting to achieve a common specified goal.”

“A narrow focus on operator actions, physical component failures, and technology may lead to ignoring some of the most important factors in terms of preventing future accidents”

– Nancy Leveson



The way humans use tech involves economic & social factors, too

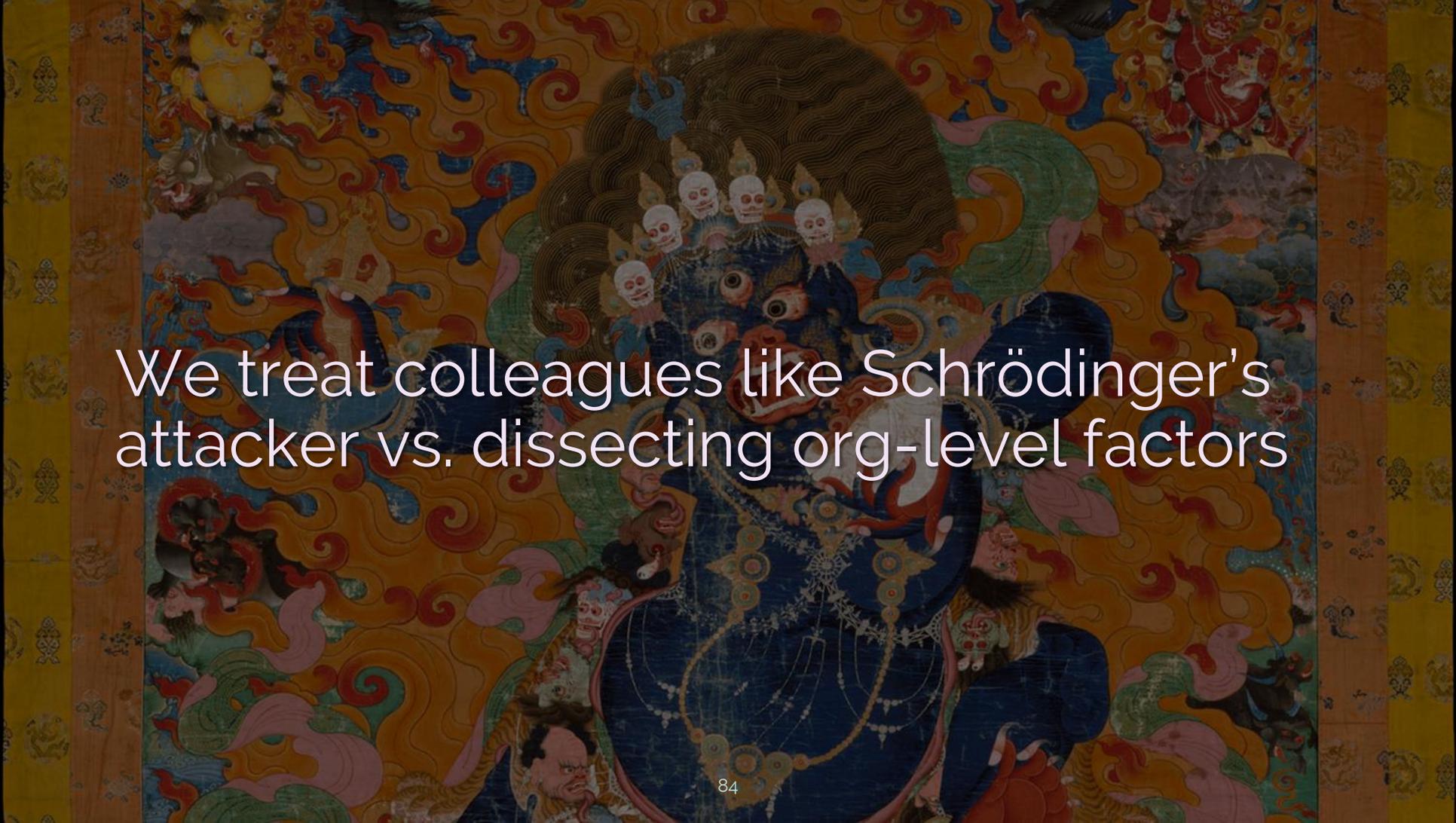
Economic factors: revenue & profit goals, compensation schemes, budgeting, etc.

Social factors: KPIs, expectations, what behavior is rewarded or punished, etc.



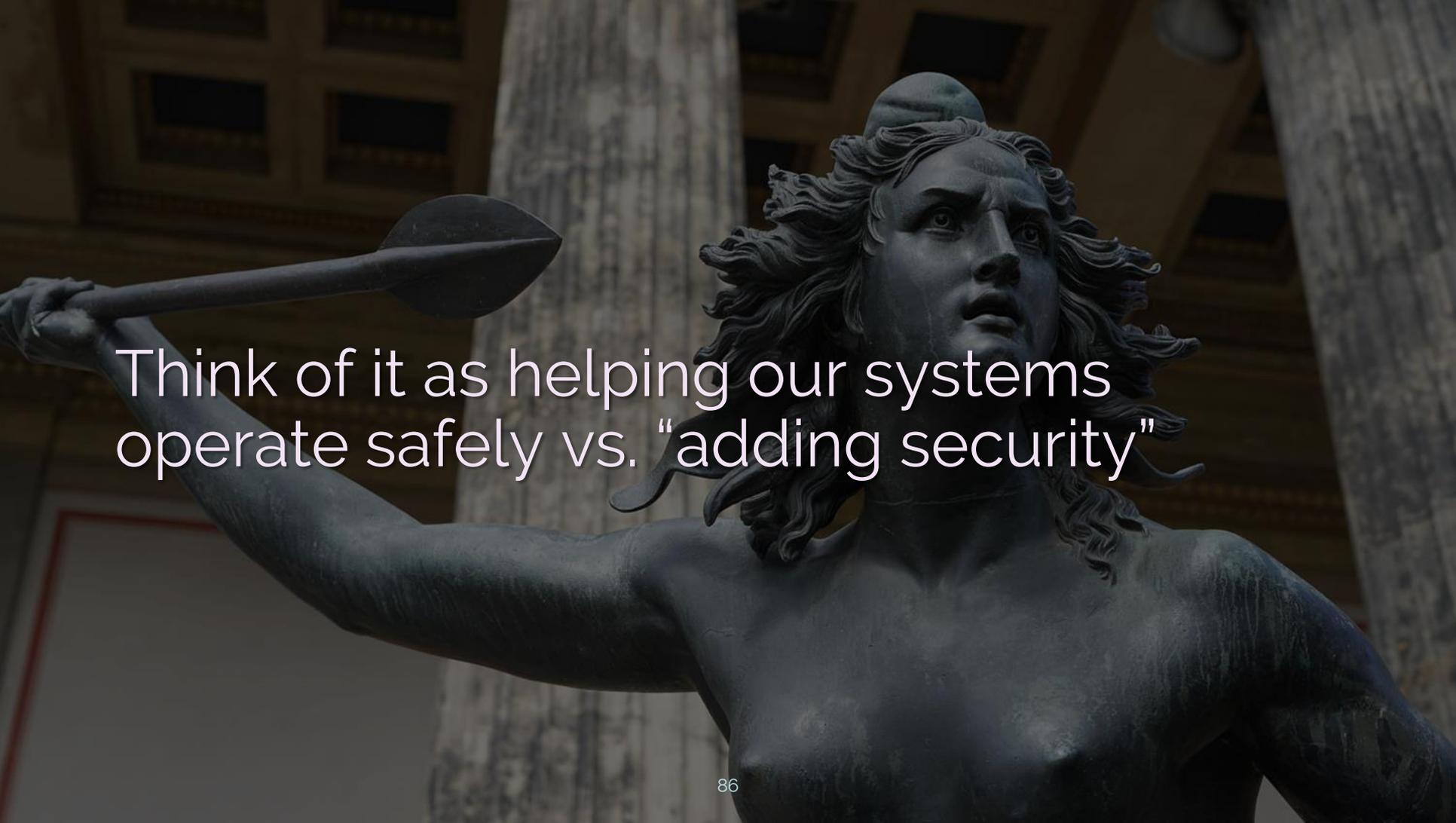
Pressure to do more work, faster is a vulnerability. So is a political culture.

Non-software vulns don't appear in our threat models, but also erode resilience



We treat colleagues like Schrödinger's  
attacker vs. dissecting org-level factors

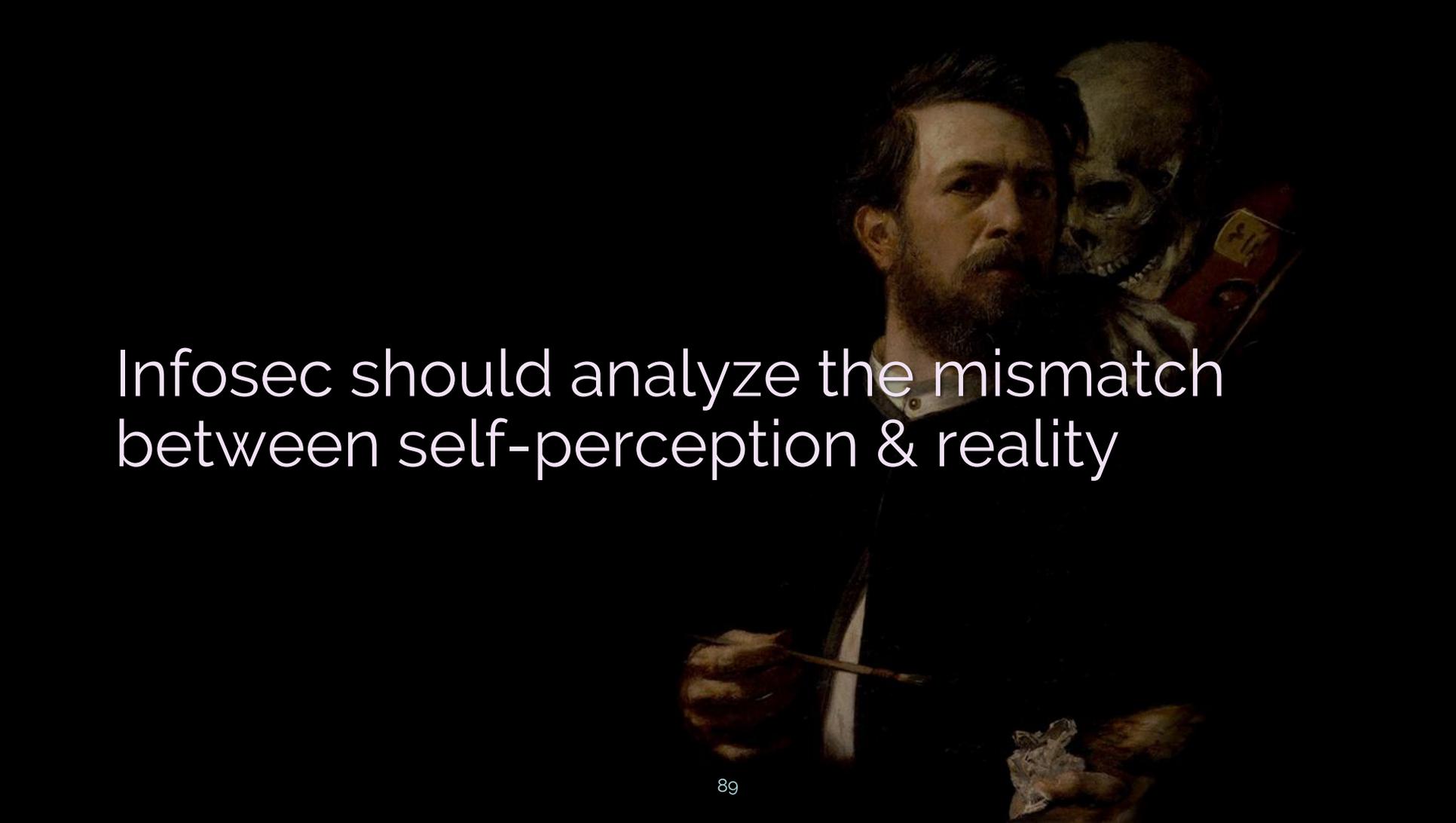
**Security is something a system does,  
not something a system has.**



Think of it as helping our systems  
operate safely vs. “adding security”

Health & “security vanity” metrics don’t say whether systems are *doing* security

Number of vulns found matters less than their severity & how quickly they're fixed



Infosec should analyze the mismatch  
between self-perception & reality

Alternative analysis for defenders is basically just user research...

Security UX



The pressure to meet competing goals  
is a strong source of security failure

What drives their promotion or firing?  
What are their performance goals?

A painting depicting three individuals seated on a wooden bench in a hallway. On the left, a Black woman in a white, off-the-shoulder dress looks down at a small object in her hands. In the center, a young girl with dark hair in braids, wearing a grey dress with a white collar and a necklace, looks down at a fan. On the right, a young man in a dark suit and cap looks down at a card or document. The background shows a hallway with a green railing and a plain wall. The overall mood is one of quiet concentration and individual focus.

Human attention is a finite & precious resource, so you must compete for it

User research can help you determine how to draw attention towards security



**Caitie McCaffrey**

@caitie

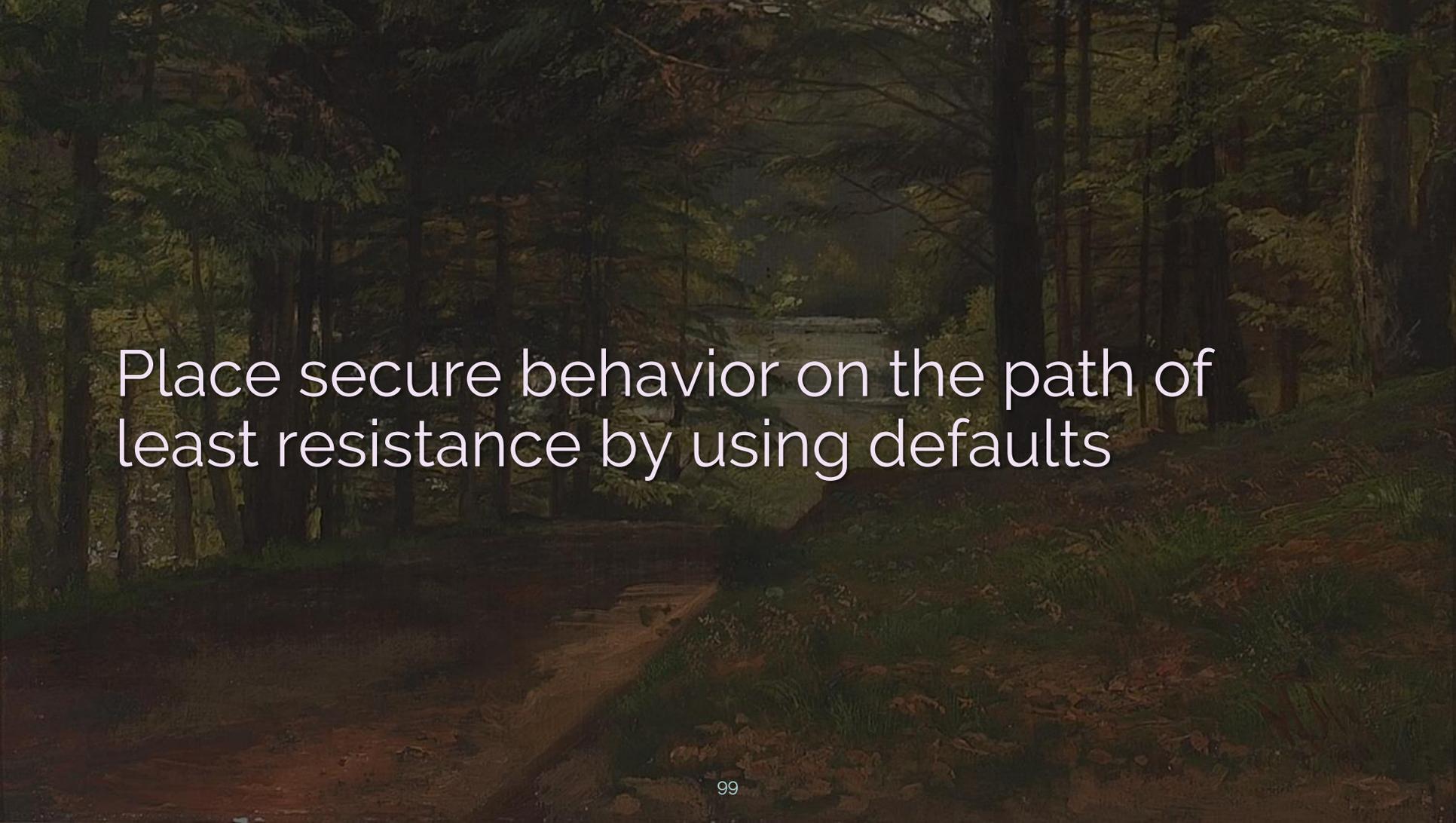


Daily Reminder for Devops & Infosec people designing tools: Alerts that always show up red don't make your systems more reliable or secure. They just teach people to ignore alerts.

WARNING: CYBER ANOMALY

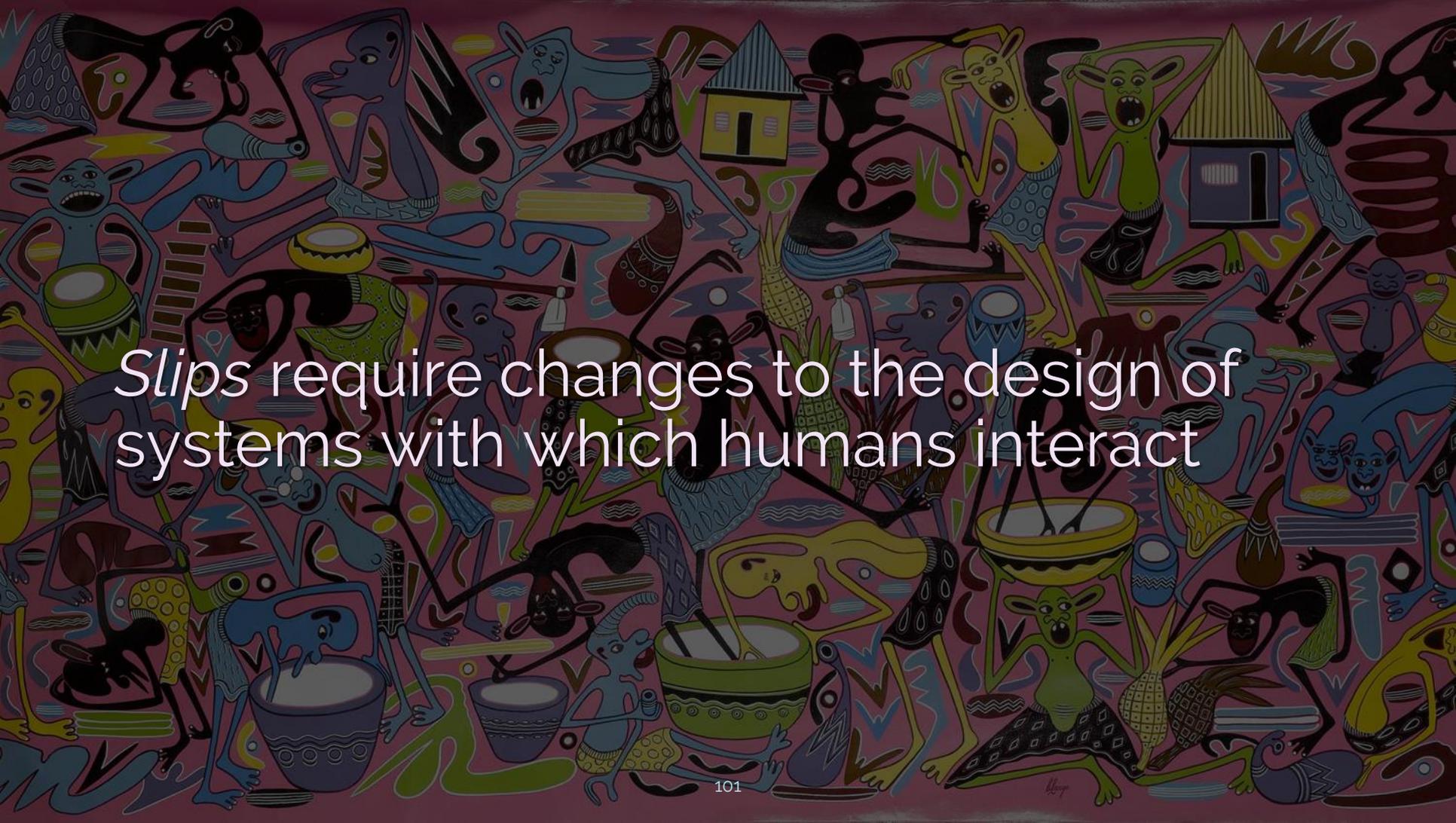
(thanks Raytheon)

Choice architecture: organizing the context in which people make decisions

A dark, atmospheric forest scene with a dirt path leading through tall trees towards a body of water in the distance. The lighting is low, creating a moody and somewhat mysterious atmosphere. The path is the central focus, leading the viewer's eye from the foreground into the depths of the forest.

Place secure behavior on the path of  
least resistance by using defaults

e.g. Requiring 2FA to create an account,  
security tests in CI/CD pipelines



*Slips* require changes to the design of systems with which humans interact

Checklists, defaults, eliminating  
distractions, removing complexity...



Strong security design anticipates user workarounds & safely supports them

e.g. Self-service app approvals with a Slackbot to confirm the run request



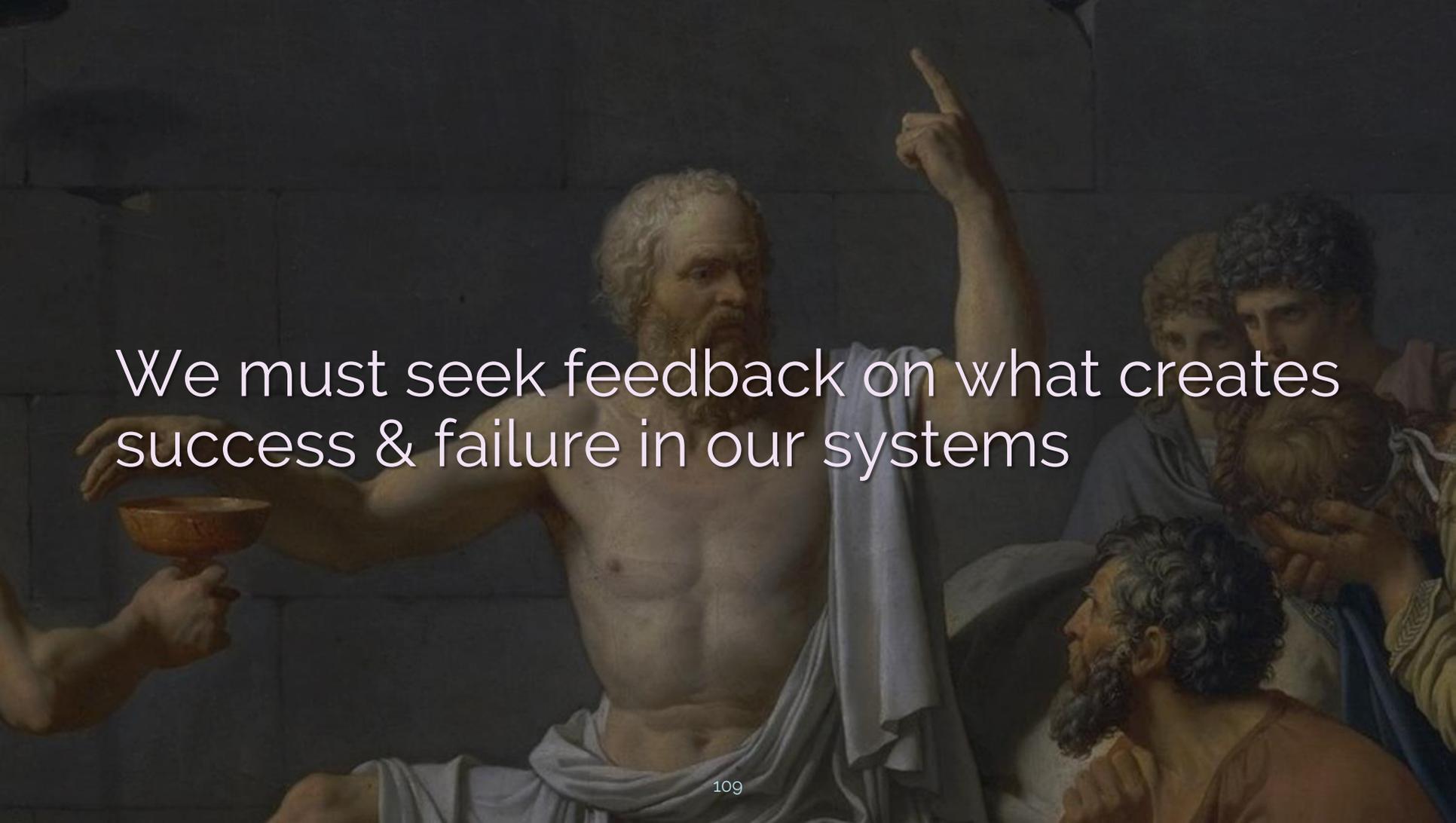
Think in terms of acceptable tradeoffs –  
create secure alternatives, not loopholes

How else can you better understand your systems & the context they create?

The background of the image is a detailed reproduction of Hieronymus Bosch's painting 'Ship of Fools'. The central focus is a large, grotesque face with a wide, open mouth, which serves as the hull of a ship. Inside the mouth, a group of people is seated under a red canopy, appearing to be in a state of revelry or a theatrical performance. The ship itself is filled with various scenes of human folly and vice, including people drinking, gambling, and engaging in other chaotic activities. The background features a dark, stormy sea and a sky filled with flying creatures and a large, dark, spherical object on the left. The overall tone is dark and satirical, reflecting the chaotic nature of the subject matter.

# Chaos Security Engineering

We will never be able to eliminate the potential for error.



We must seek feedback on what creates success & failure in our systems

“Enhancing error tolerance, error detection, and error recovery together produce safety.”

– Woods, et al

**Error tolerance:** the ability to not get totally pwned when compromise occurs

Error detection: the ability to spot unwanted activity

Error recovery: the ability to restore systems to their intended functionality

Highest ROI: anticipating how the potential for failure evolves

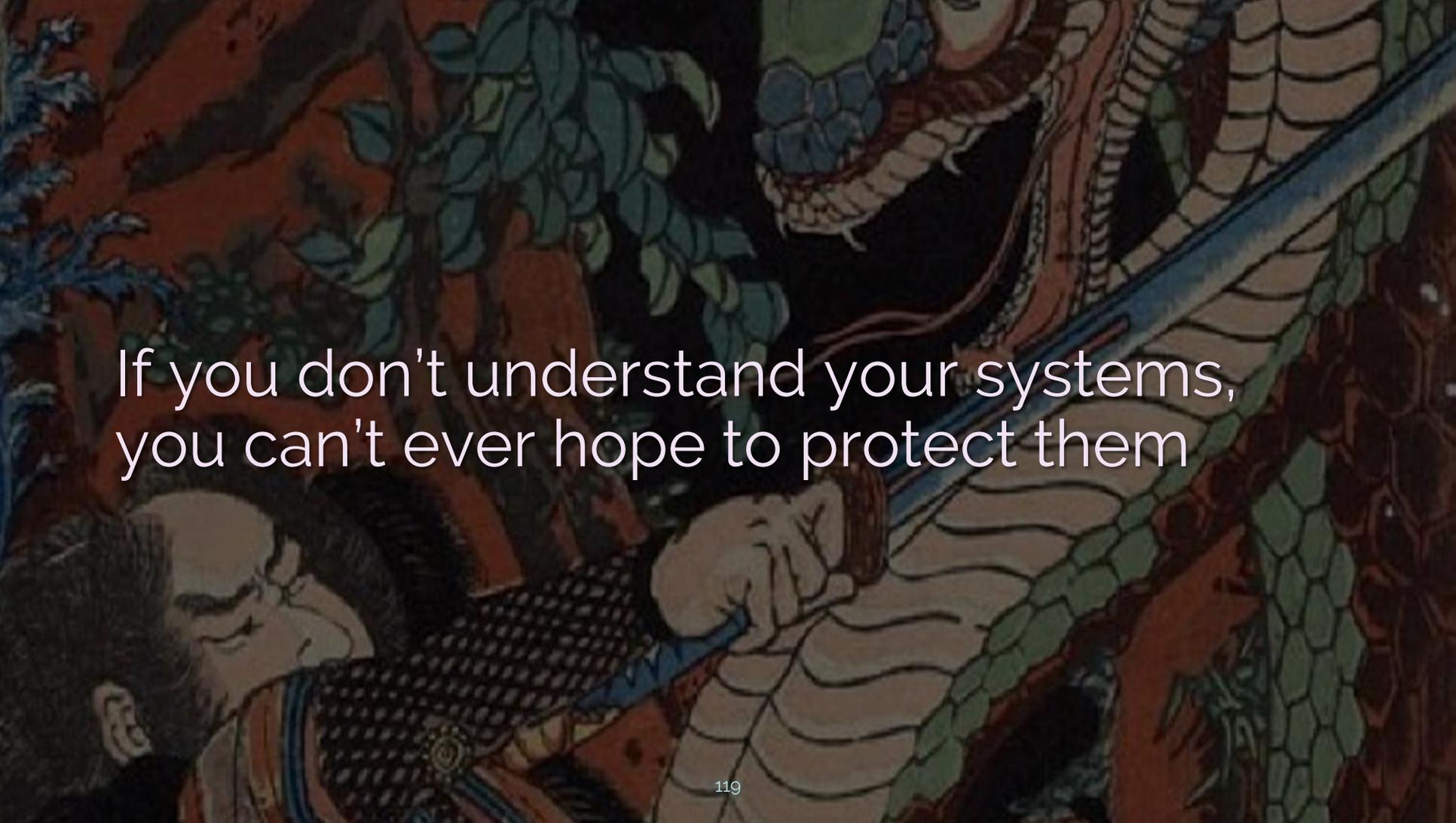
Chaos eng: continual experimentation to evaluate response to unexpected failure

e.g. Retrograding: inject old versions of  
libs, containers, etc. into your systems

A painting by Edgar Degas titled "The Ballet Rehearsal in the Dressing Room". It depicts a ballerina in a white tutu being supported by a man in a top hat in a dimly lit room. The scene is captured with visible brushstrokes, emphasizing the dynamic and somewhat chaotic nature of the rehearsal. The lighting is dramatic, with strong highlights on the ballerina's dress and the man's face, contrasting with the dark background.

Chaos engineering assumes existing knowledge hangs in a delicate balance

The potential for hazard is constantly changing, creating new blindspots



If you don't understand your systems,  
you can't ever hope to protect them

Chaos security engineering requires a blameless culture...

The image shows a close-up of a rock wall covered in numerous handprints. The handprints are of various sizes and colors, including red, orange, and white. They are scattered across the surface, some overlapping. The rock itself is a mix of brown and tan tones, with some darker spots. The overall appearance is that of an ancient or prehistoric site.

Blameless Culture



A blameless culture balances safety and accountability – not absolution

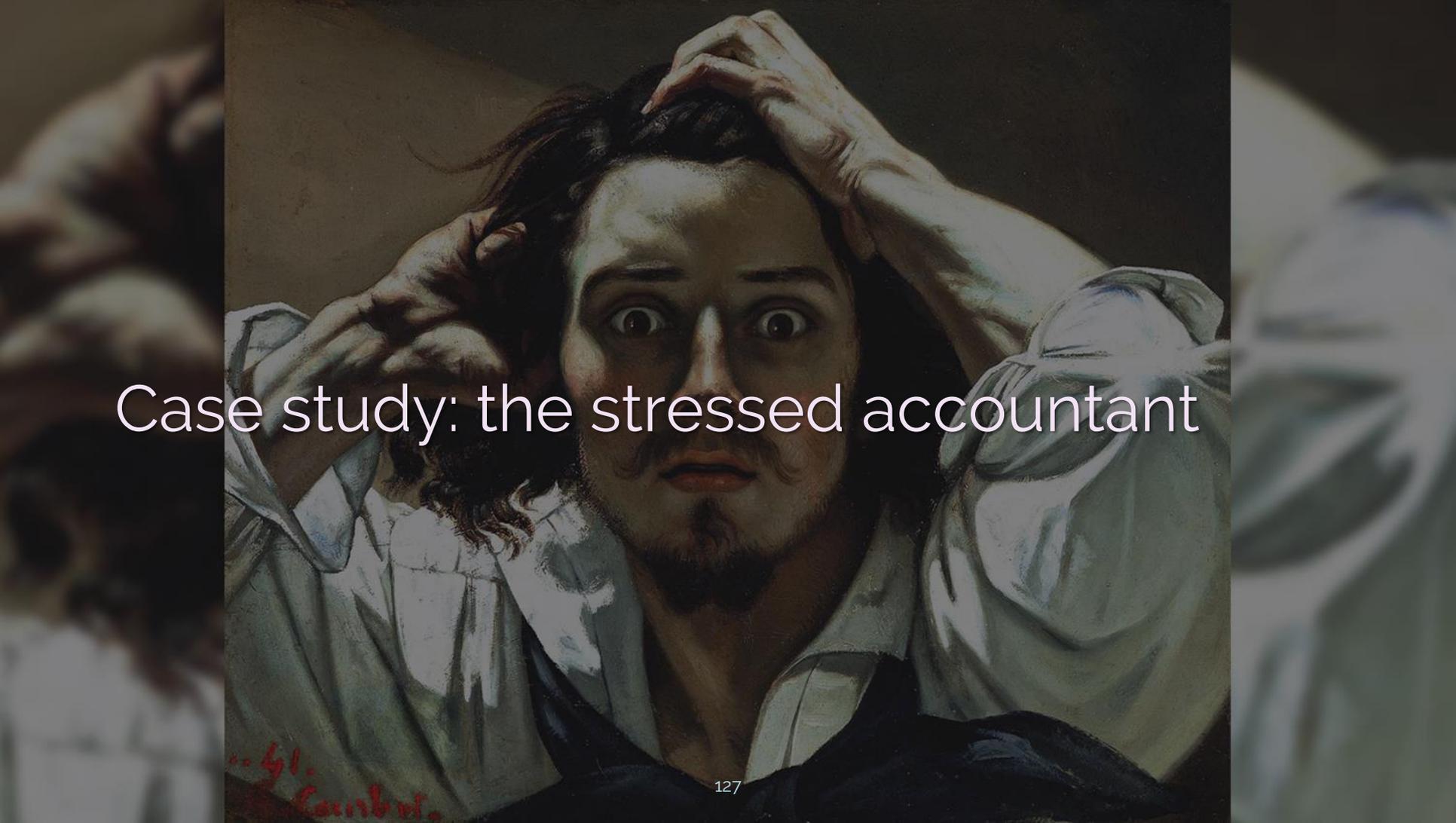
Supports a perpetual state of learning, in which critical info isn't suppressed



Asking the right questions is the first step towards a blameless culture

Neutral questions prevent bias from seeping into our incident review

Ask other practitioners what they would do in the same original context

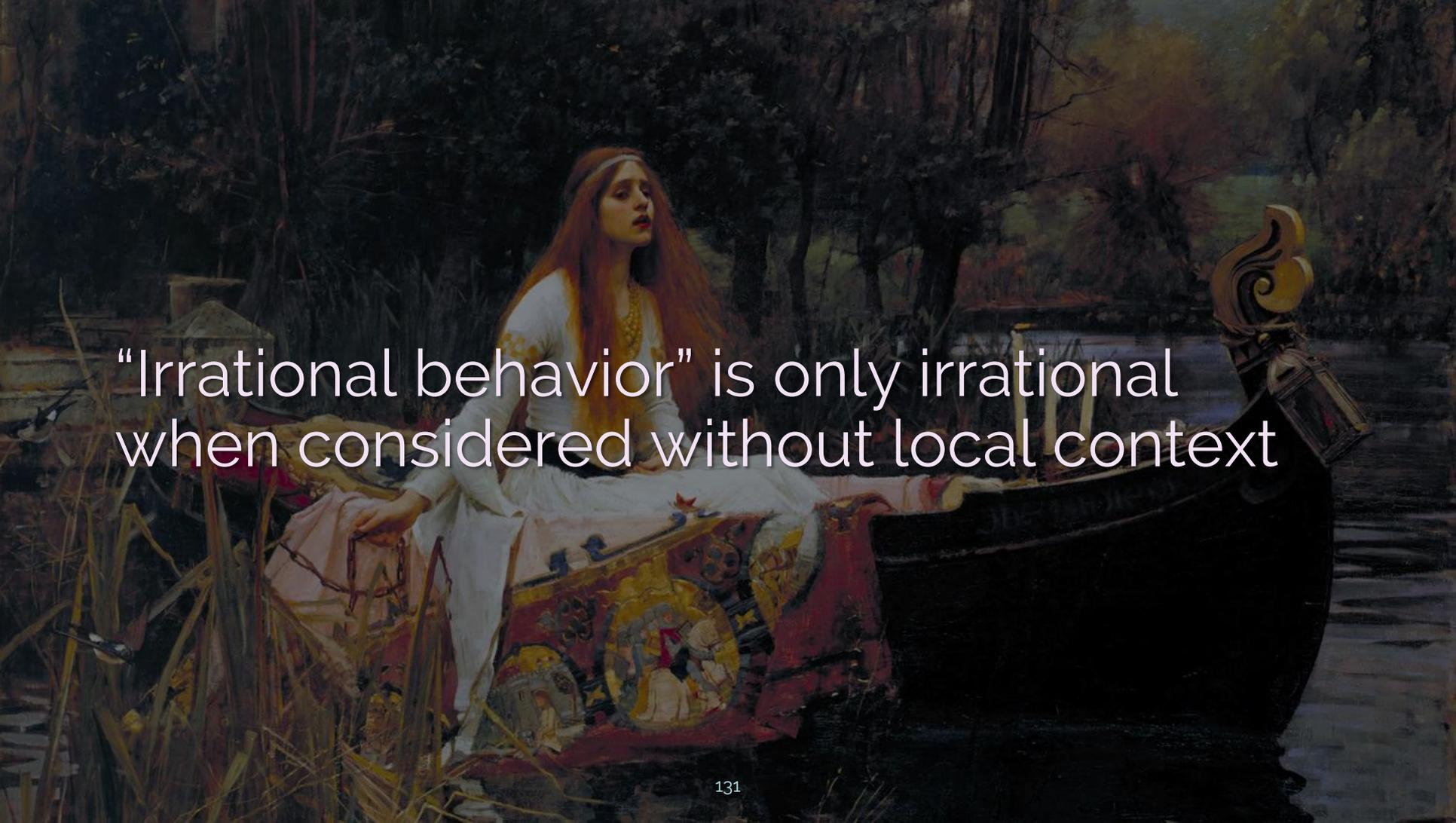
A detailed oil painting of a man with long, dark, wavy hair and a goatee. He has a wide-eyed, shocked expression, with his mouth slightly open and his hands pressed against his temples. He is wearing a light-colored, possibly white, shirt with ruffled cuffs. The background is dark and indistinct. The overall mood is one of intense stress or mental anguish.

Case study: the stressed accountant

“Human error” becomes a reasonable action given the human’s circumstances



Neutral practitioner questions help  
sketch a portrait of local rationality

A painting of a woman with long red hair, wearing a white dress with gold embroidery, sitting in a dark boat on a river. She is looking upwards and to the right. The boat has a decorative golden prow. The background shows a dense forest of trees. The text "Irrational behavior" is only irrational when considered without local context is overlaid in white on the image.

“Irrational behavior” is only irrational  
when considered without local context

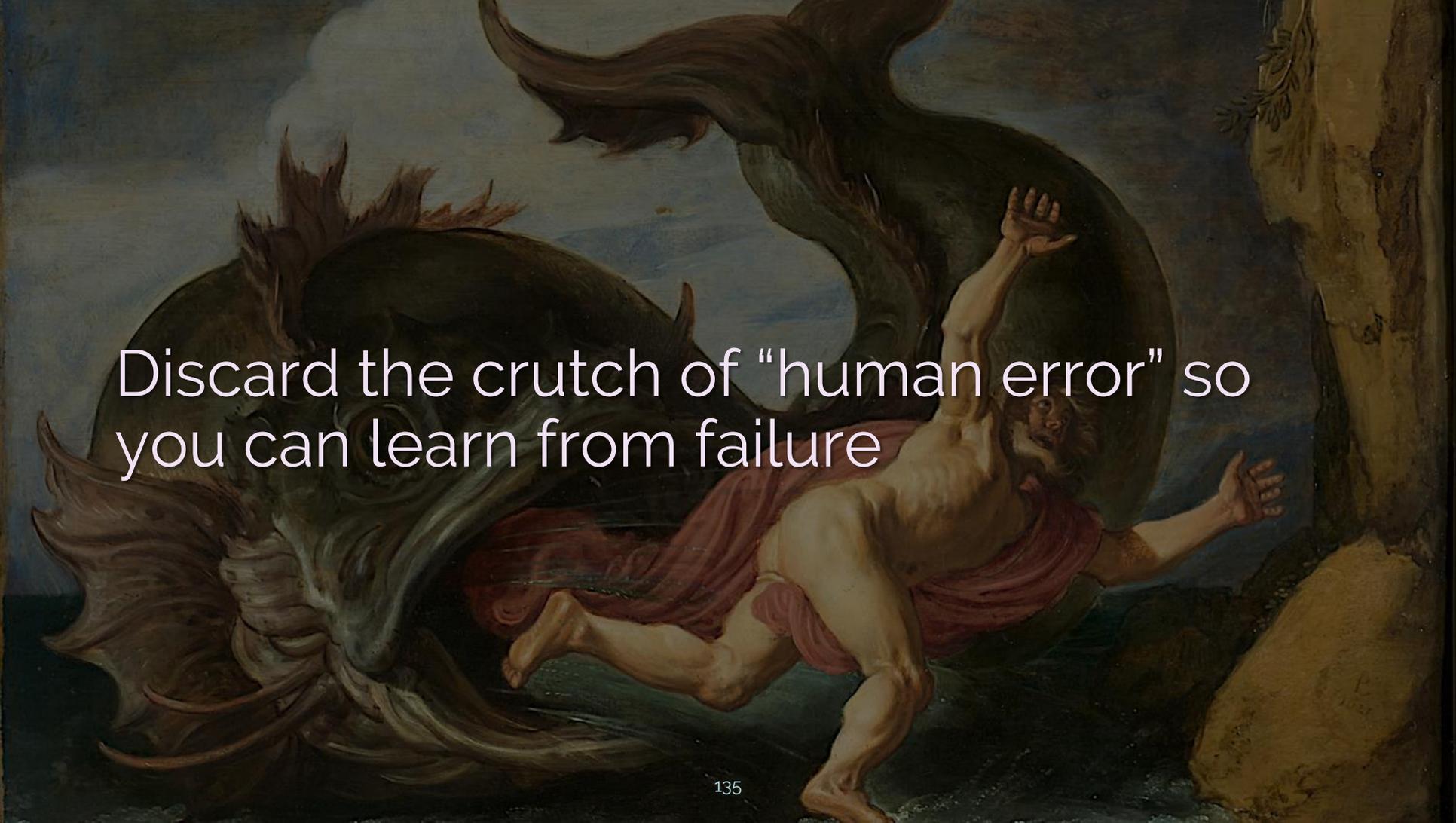
Our goal is to change the *context* of decision-making to promote security



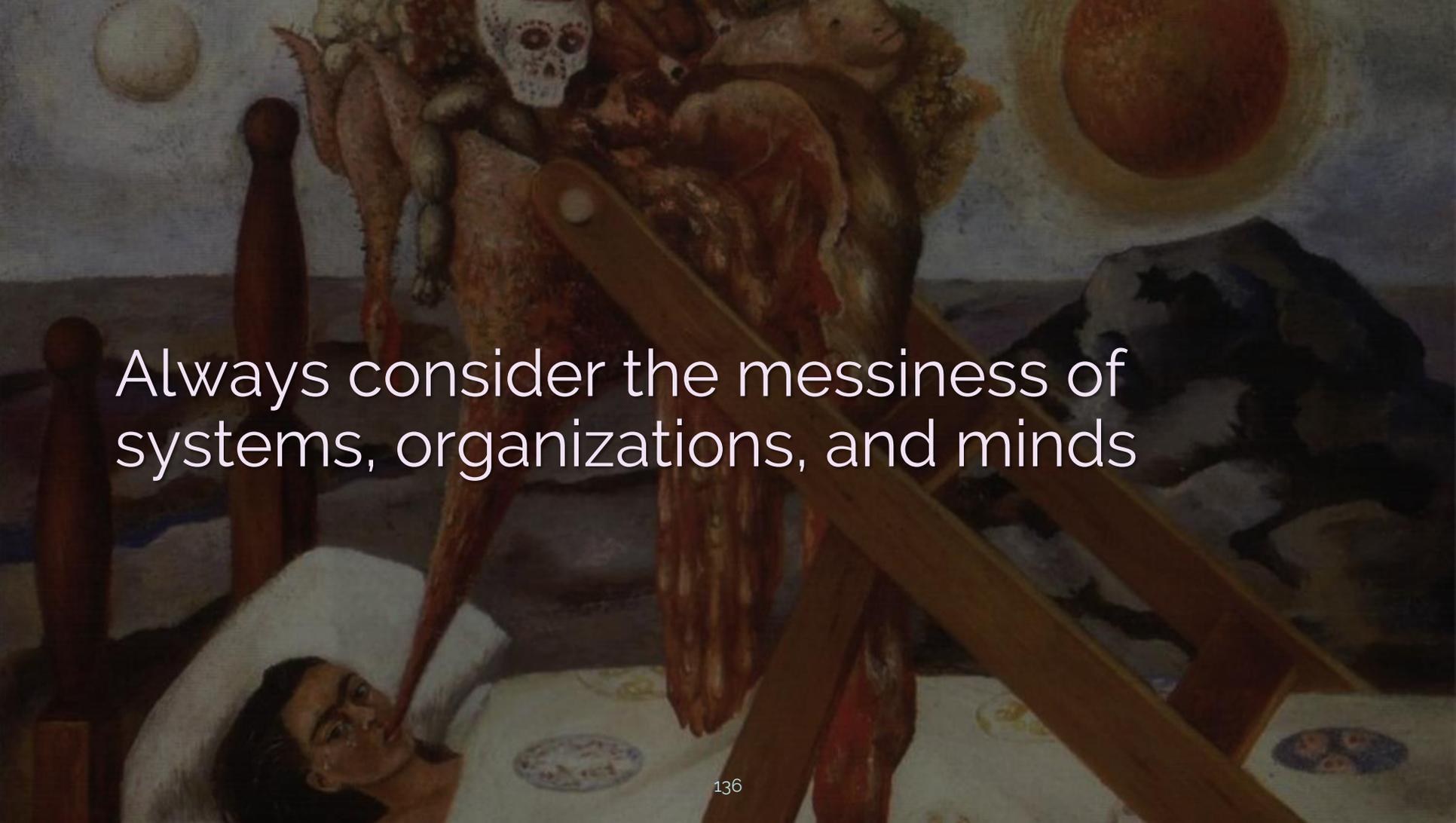
If you're using an ad-hominem attack in incident review, you've veered astray

A detailed oil painting of Napoleon Bonaparte on a white horse, wearing a red cape and a black bicorne hat with gold trim. He is pointing his right hand towards the sky. The background is a dramatic, cloudy sky. The text "In Conclusion" is overlaid in white serif font on the left side of the image.

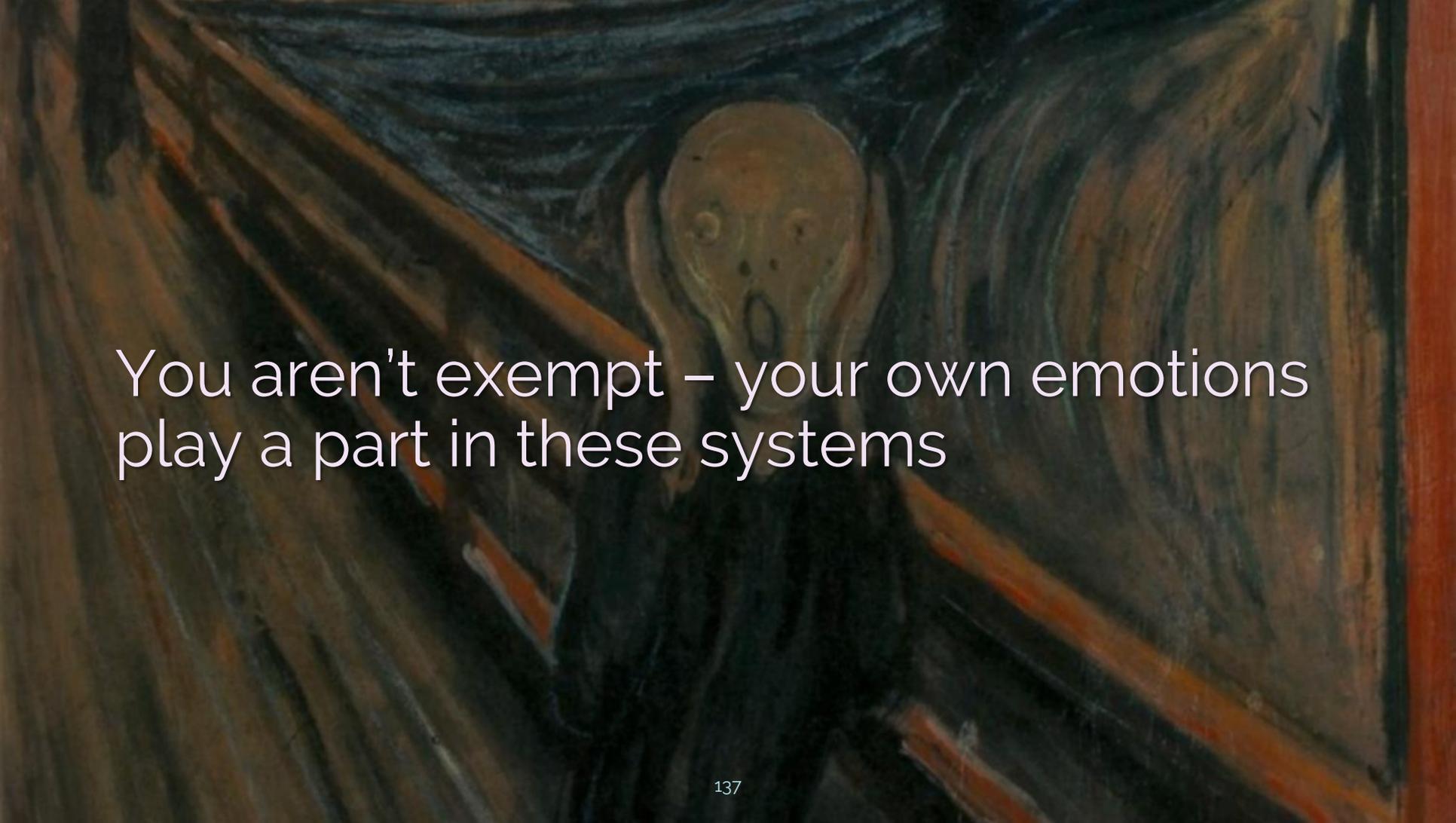
In Conclusion



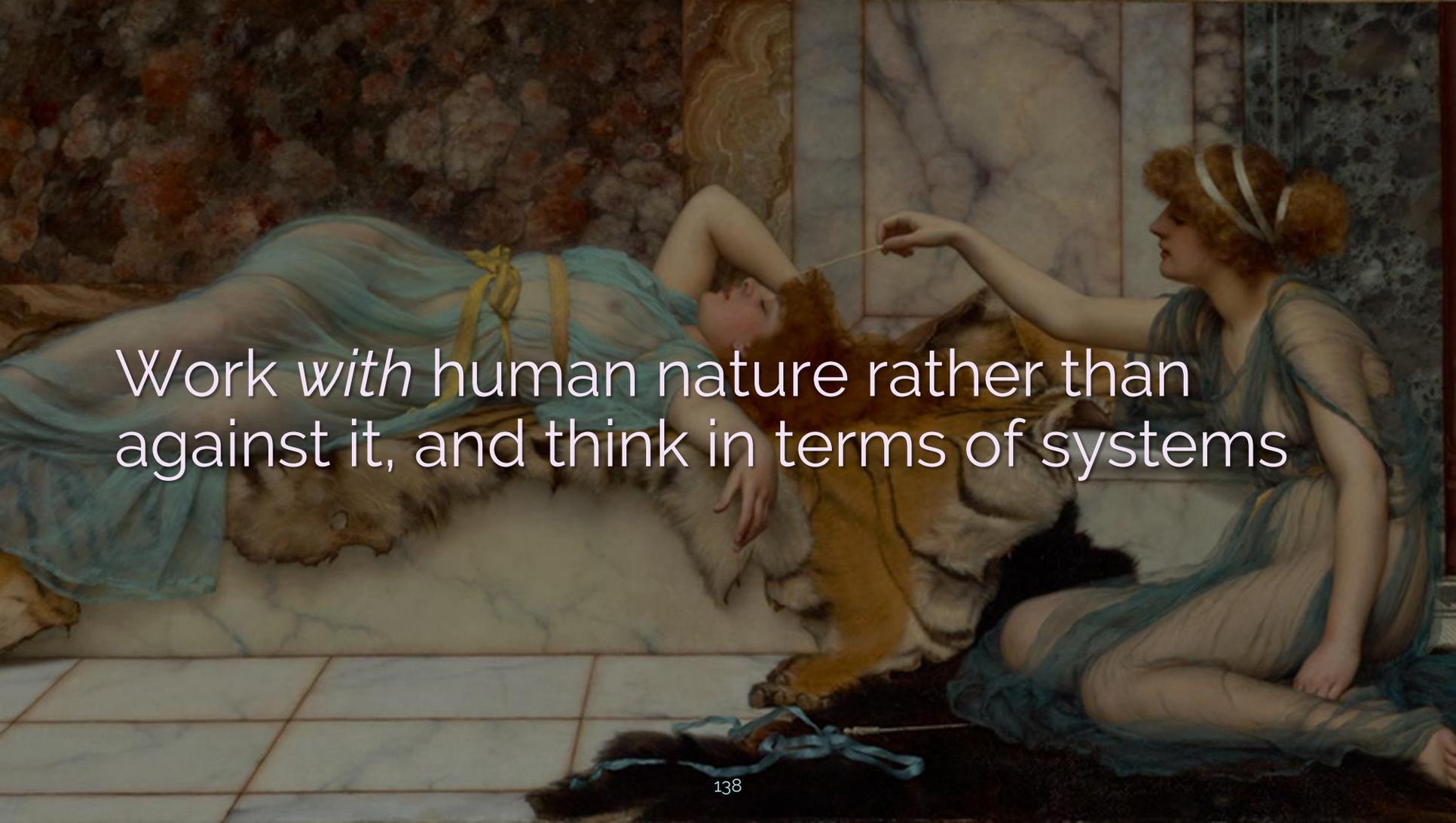
Discard the crutch of “human error” so  
you can learn from failure



Always consider the messiness of  
systems, organizations, and minds

The background of the slide is a reproduction of the painting 'The Scream' by Edvard Munch. It depicts a figure in the center, likely Christ the Redeemer, with a pale, almost featureless face, set against a dark, swirling, and turbulent background. The overall mood is one of intense emotional distress or suffering.

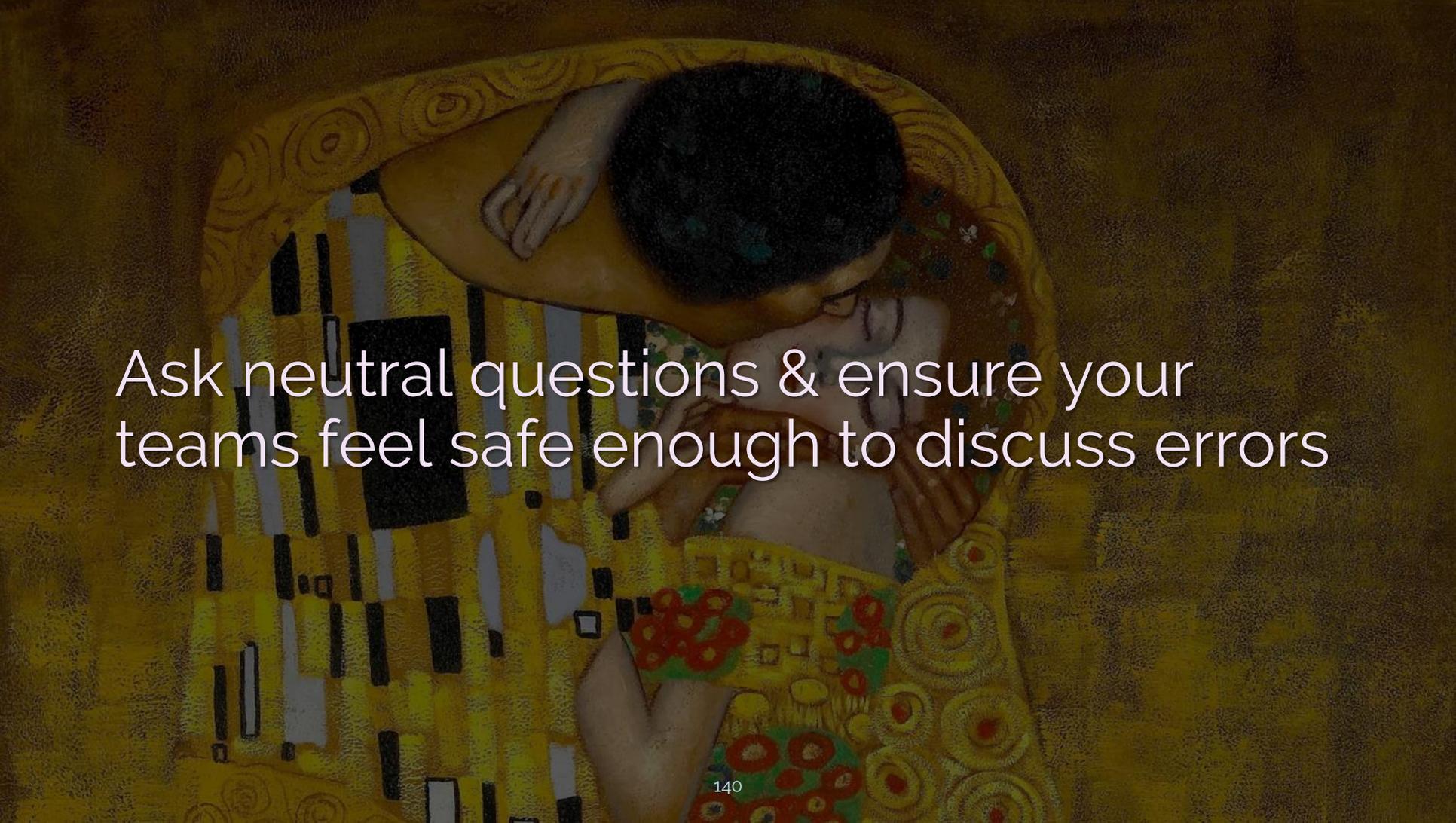
You aren't exempt – your own emotions  
play a part in these systems



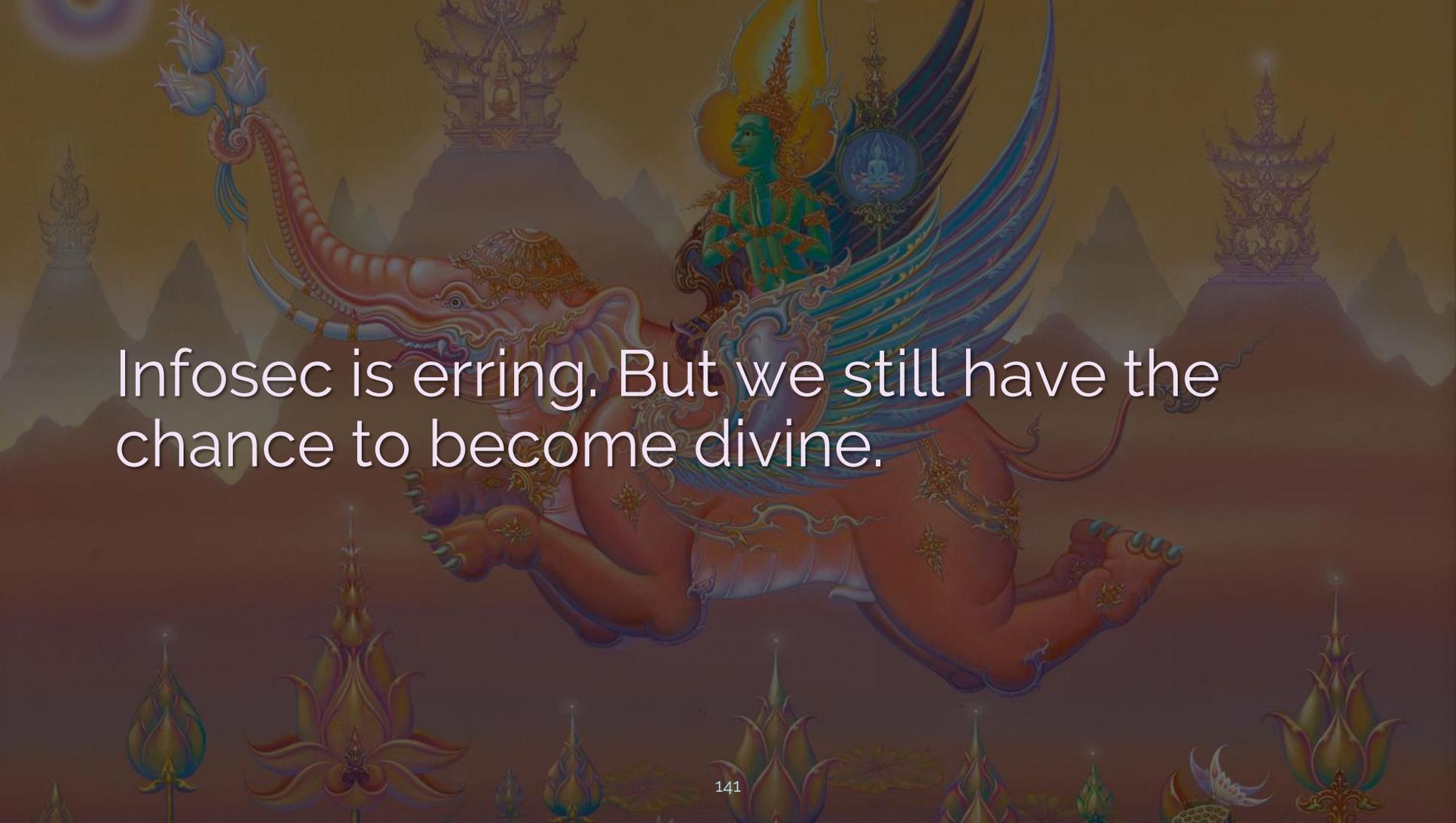
Work *with* human nature rather than against it, and think in terms of systems



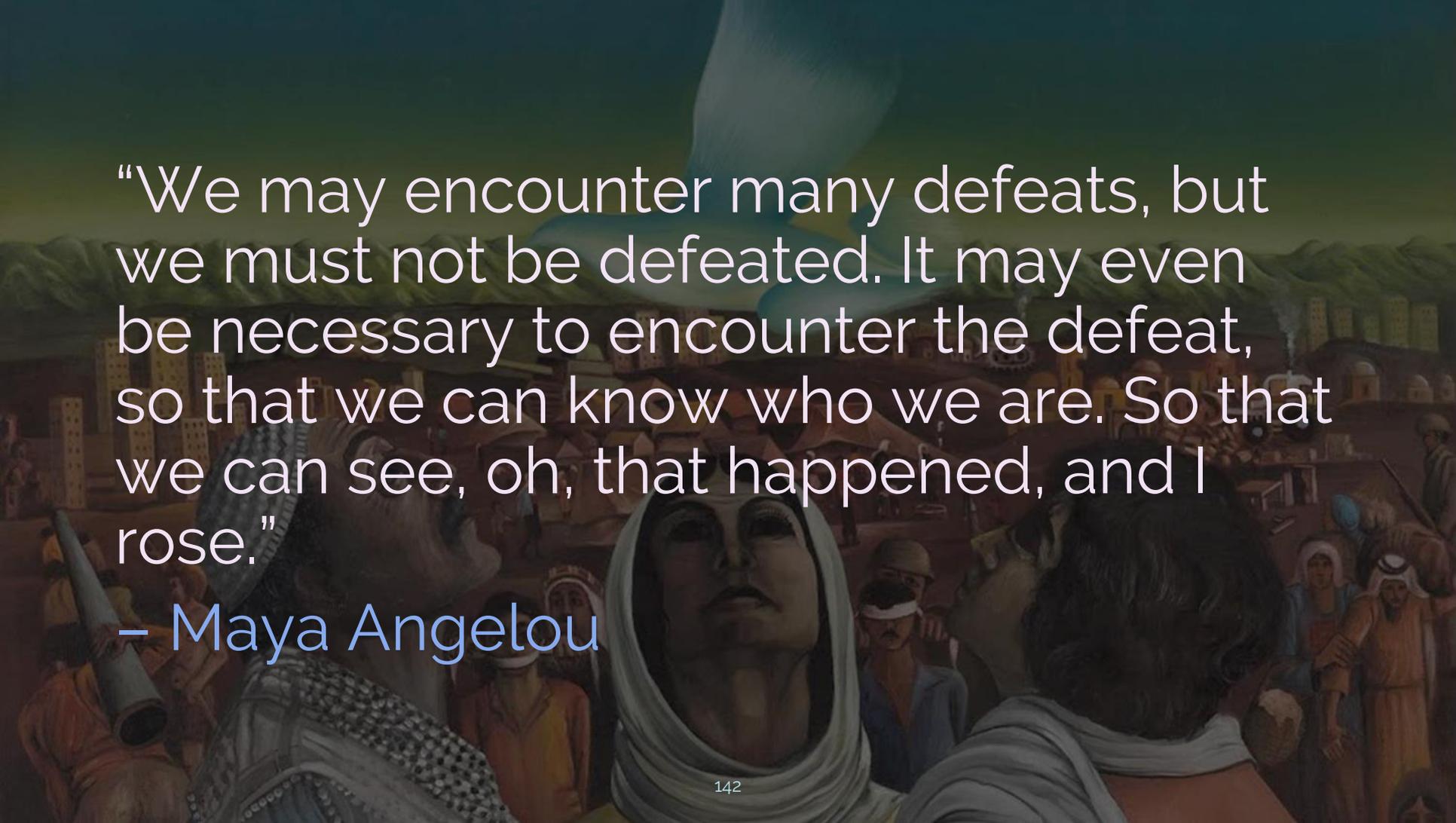
Leverage UX & chaos eng to improve  
the context your systems engender

The background of the slide is a reproduction of Gustav Klimt's painting 'The Kiss'. It depicts a man and a woman in a close embrace, surrounded by intricate golden patterns and symbols. The man is on the left, leaning towards the woman on the right. The scene is set against a dark, textured background with a prominent golden archway above them. The overall mood is intimate and romantic.

Ask neutral questions & ensure your teams feel safe enough to discuss errors



Infosec is erring. But we still have the chance to become divine.

A painting depicting a dense crowd of people in a city. In the foreground, a woman with a white headscarf looks upwards with a determined expression. To her right, another woman is seen from the back, looking towards the crowd. The background is filled with many other figures, some holding spears, suggesting a scene of conflict or a significant public gathering. The overall tone is somber and historical.

“We may encounter many defeats, but we must not be defeated. It may even be necessary to encounter the defeat, so that we can know who we are. So that we can see, oh, that happened, and I rose.”

– Maya Angelou



@swagitda\_



/in/kellyshortridge



kelly@greywire.net

# Suggested Reading

- “The evolution of error: Error management, cognitive constraints, and adaptive decision-making biases.” Johnson, D., et al.
- “Hindsight bias impedes learning.” Mahdavi, S., & Rahimian, M. A.
- “Outcome bias in decision evaluation.” Baron, J., & Hershey, J. C.
- “Human error.” Reason, J.
- “Behind human error.” Woods, D., et al.
- “People or systems? To blame is human. The fix is to engineer.” Holden, R.J.
- “Understanding adverse events: a human factors framework.” Henriksen, K., et al.
- “Engineering a safer world: Systems thinking applied to safety.” Leveson, N.
- “‘Going solid’: a model of system dynamics and consequences for patient safety.” Cook, R., Rasmussen, J.
- “Choice Architecture.” Thaler, R. H., Sunstein, C.R., Balz, J.P.
- “Blameless PostMortems and a Just Culture.” Allspaw, J.