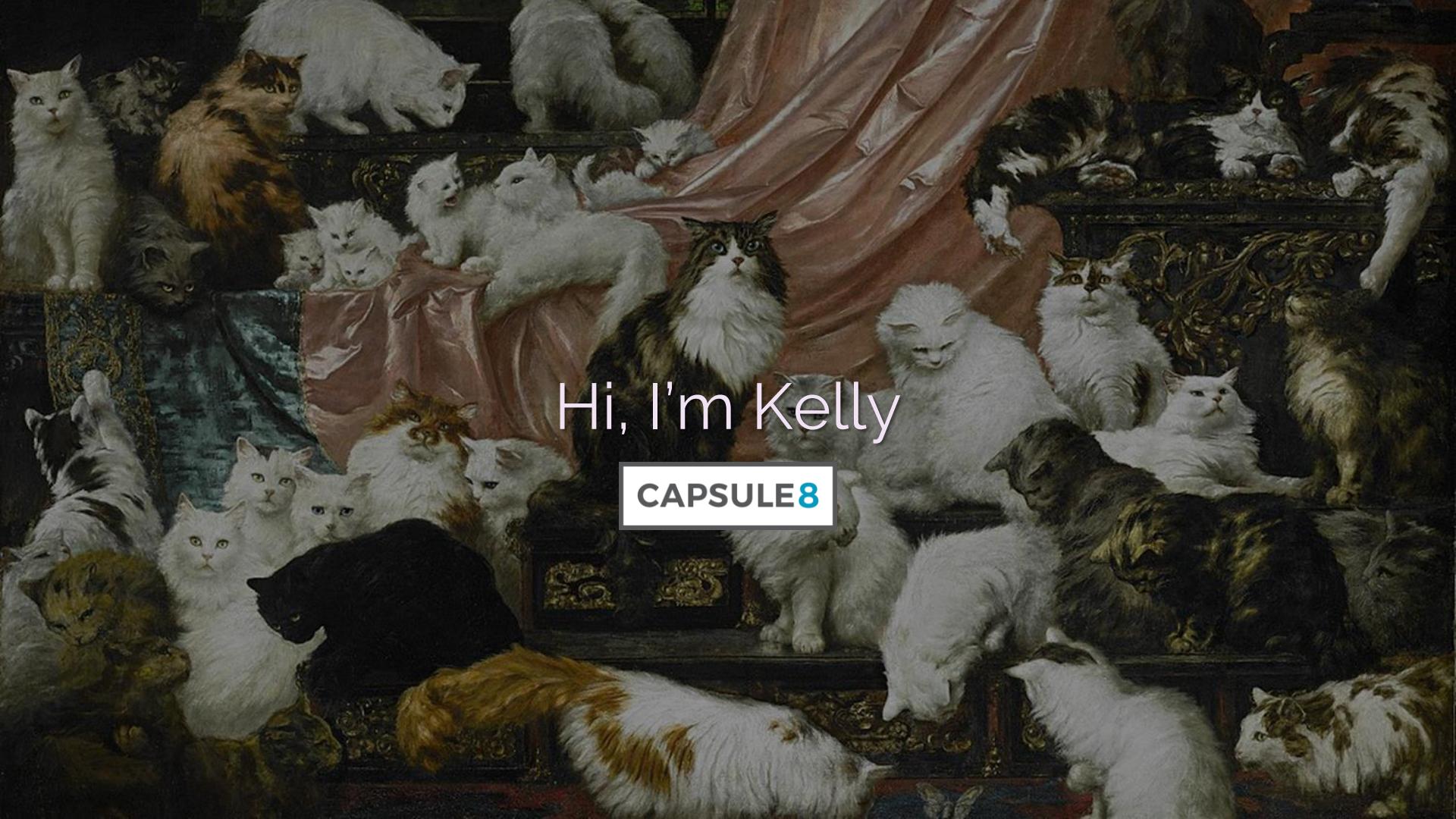
A painting of a man in a dark coat and hat standing on a rocky cliff edge, looking out over a vast, misty landscape.

To ERR IS HUMAN: The Complexity of Security Failures

Kelly Shortridge (@swagitda_)

Hacktivity 2019 Keynote

A painting depicting a room overflowing with numerous cats of various breeds and colors, including white, black, and calico. They are perched on furniture like a sofa and armchairs, and some are on the floor. A large, heavy red curtain hangs in the background.

Hi, I'm Kelly

CAPSULE8

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

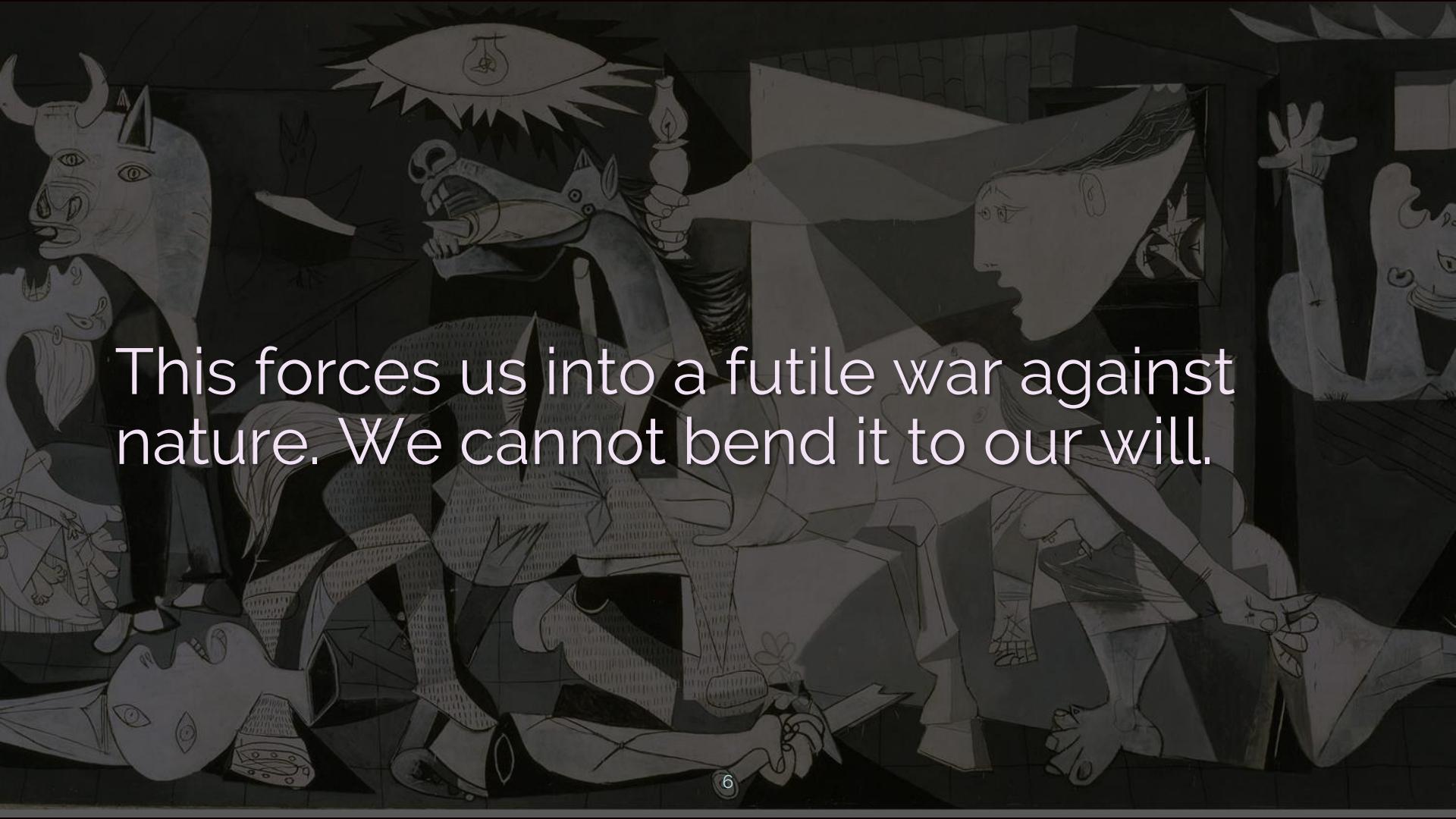


A dark, textured background featuring a close-up of a person's face and shoulders, possibly from a painting like the Mona Lisa.

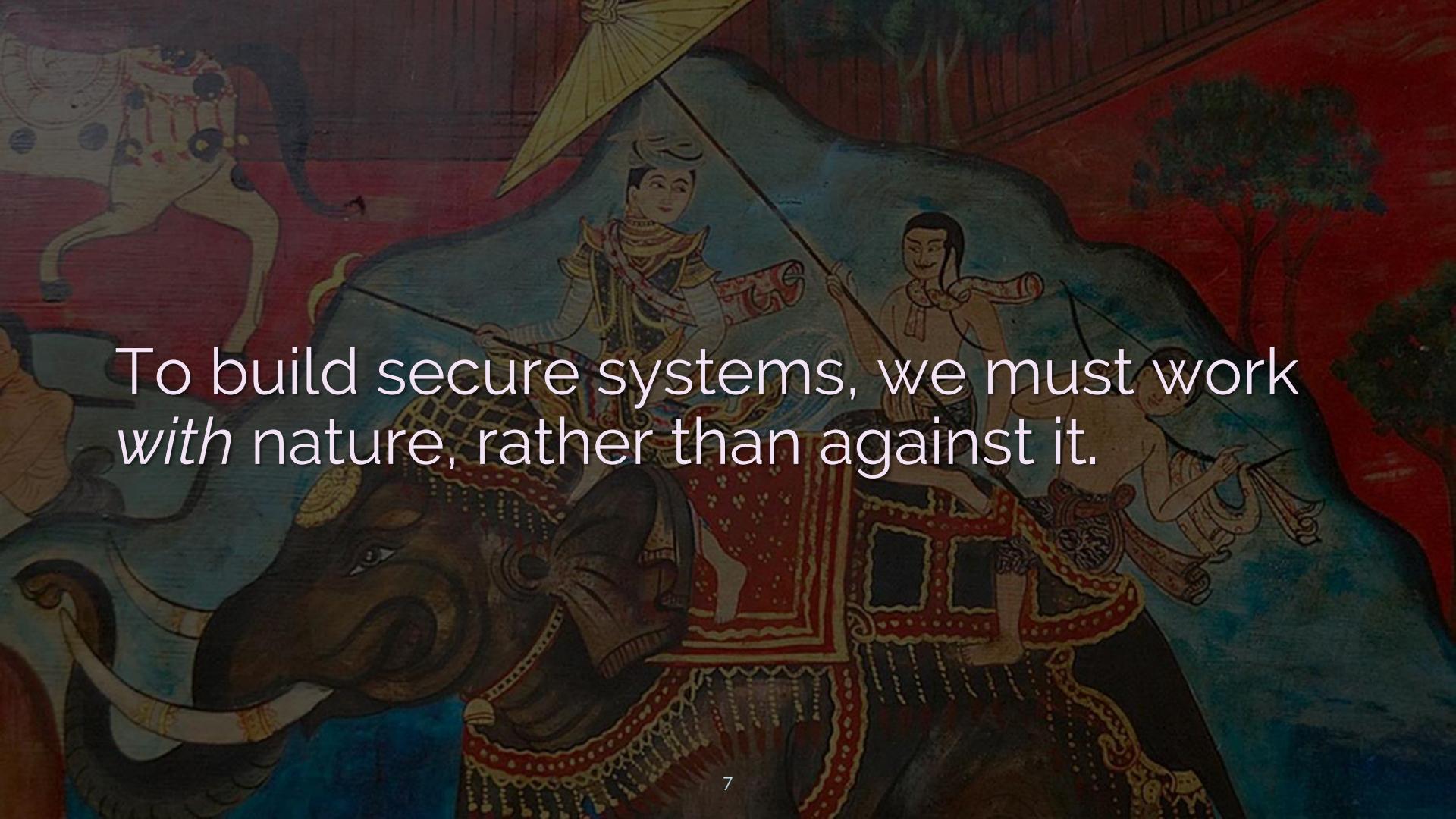
Humans make mistakes. It's part of our nature (it's mostly a feature, not a bug)

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.

A traditional East Asian painting, possibly a scroll or panel, depicting a scene with several figures and a large, stylized dragon or cloud creature. In the center, a figure in a light-colored robe and a tall, ornate hat holds a long staff or spear. To the right, another figure in a light robe stands near a large, dark, swirling dragon. The background features red and blue washes, and there are green trees on the right side. The overall style is characteristic of classical Chinese or Korean narrative art.

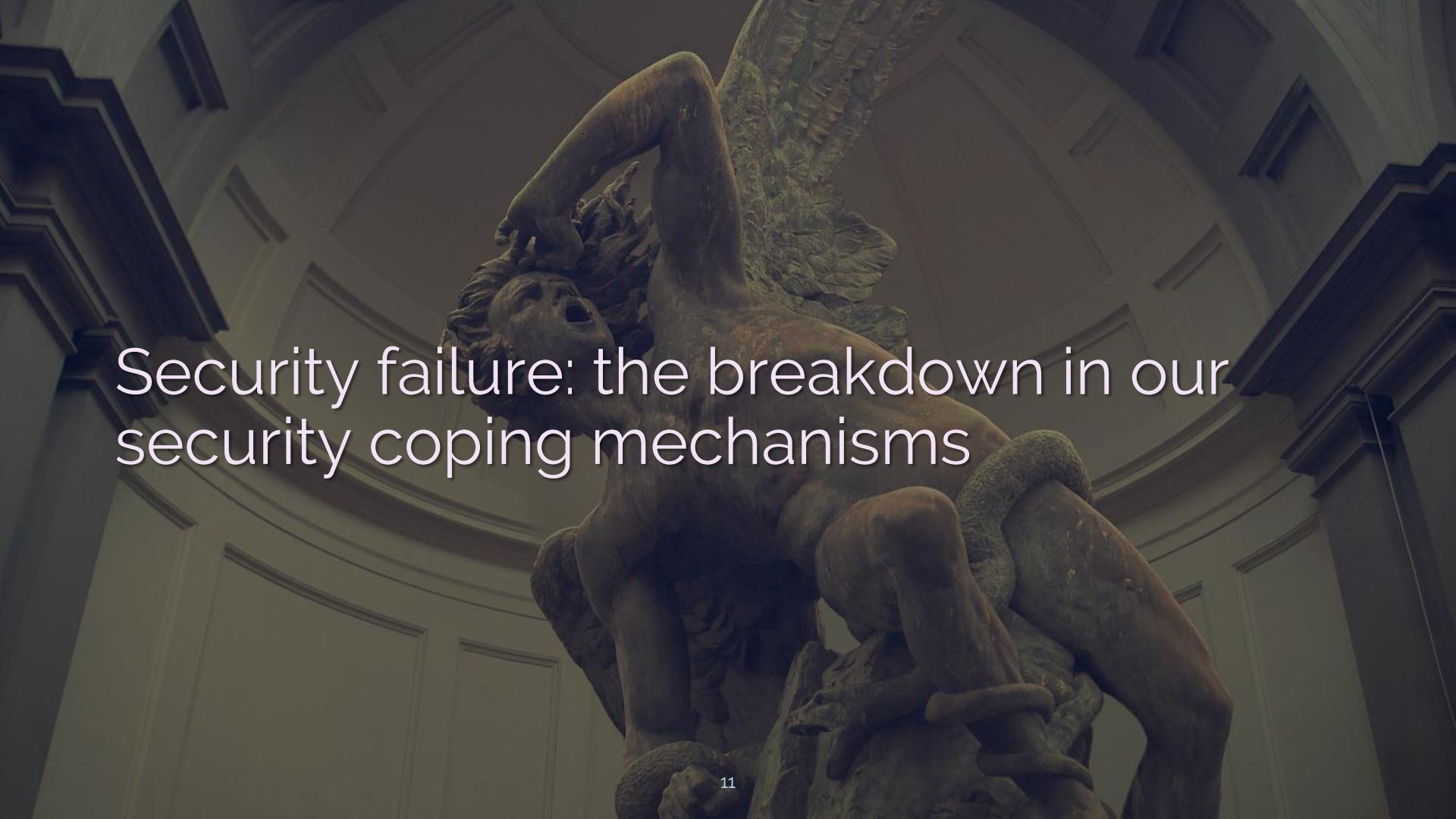
To build secure systems, we must work
with nature, rather than against it.

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

The background is a reproduction of Vincent van Gogh's painting "The Starry Night". It depicts a dark, swirling night sky filled with numerous small, yellow stars and a large, bright, yellow sun in the upper right corner. In the foreground, a dark, silhouetted town with several tall, thin church spires is visible on the left, while rolling hills and fields are on the right. The style is characterized by thick, expressive brushstrokes.

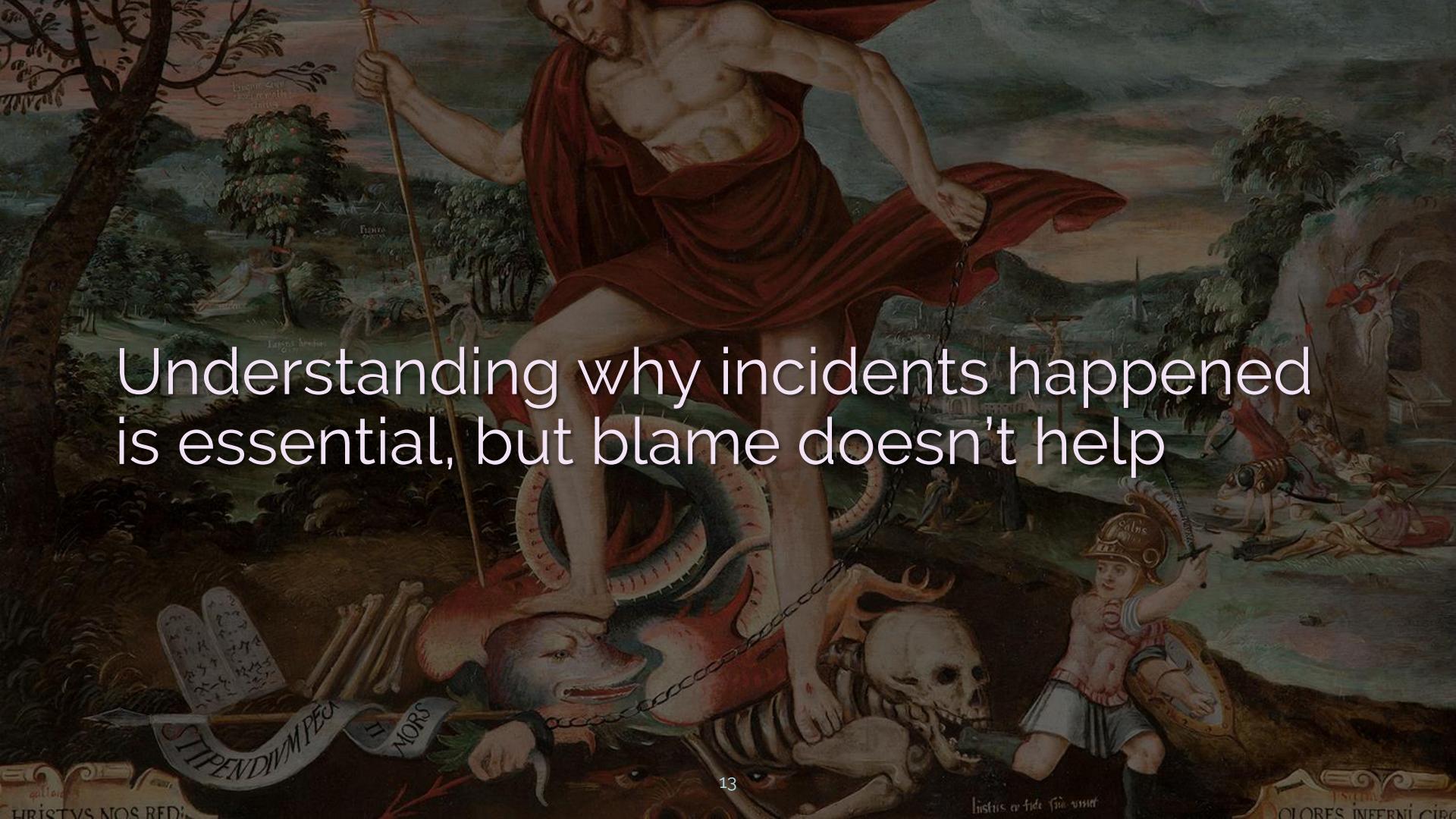
Clearing the Err

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



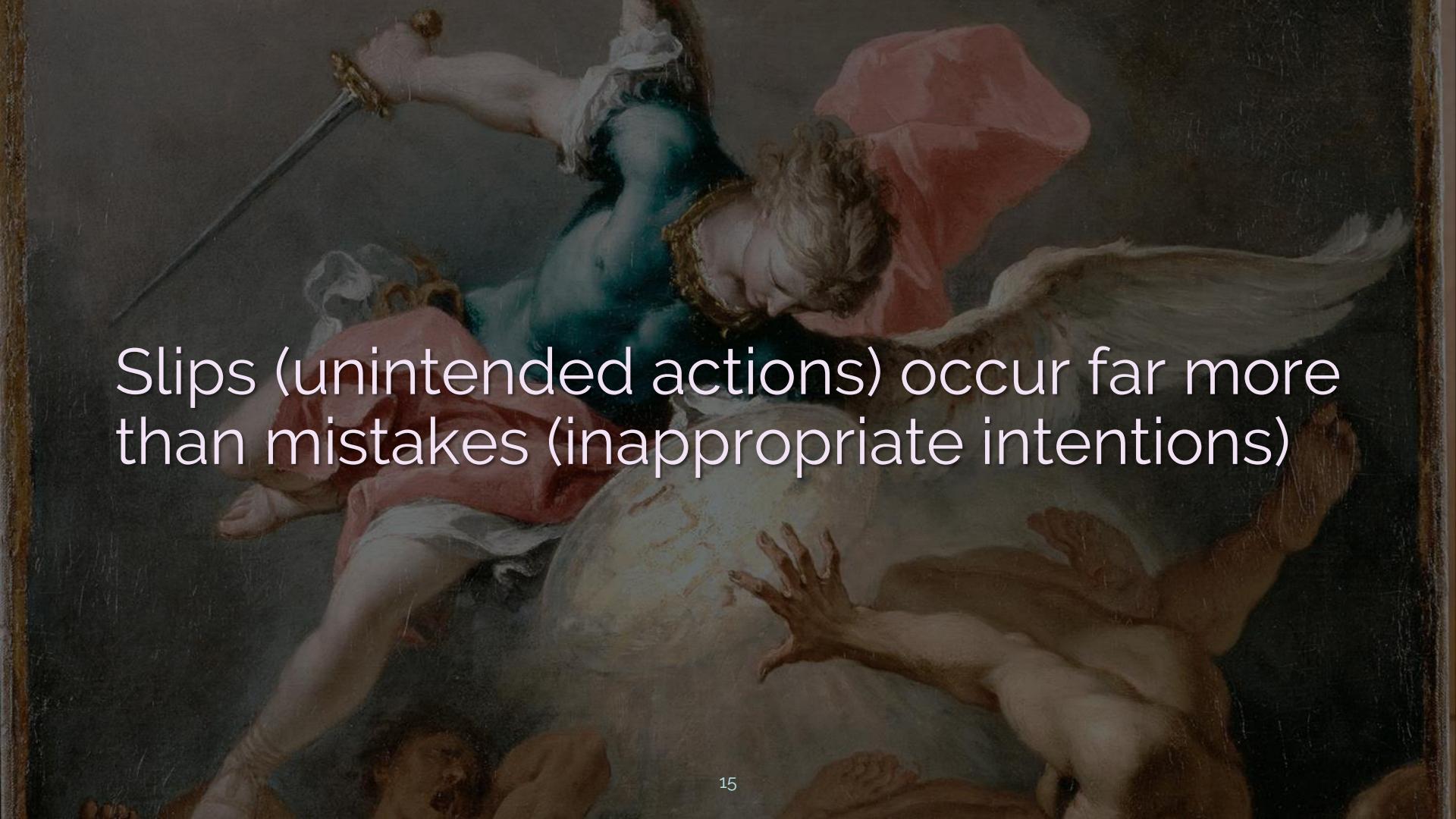
Security failure: the breakdown in our security coping mechanisms

“Human error” involves subjective expectations, including in infosec



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

Aviation, manufacturing, & healthcare
are already undergoing this revolution

A dramatic painting depicting a scene of violence or passion. A woman in a red dress is shown in mid-fall, her body angled downwards. She has a look of distress or agony on her face. A man in a blue robe is pulling her down, his hand gripping her arm. He holds a long, curved sword in his other hand, its hilt visible near the top left. The background is dark and smoky, suggesting a chaotic or divine setting.

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

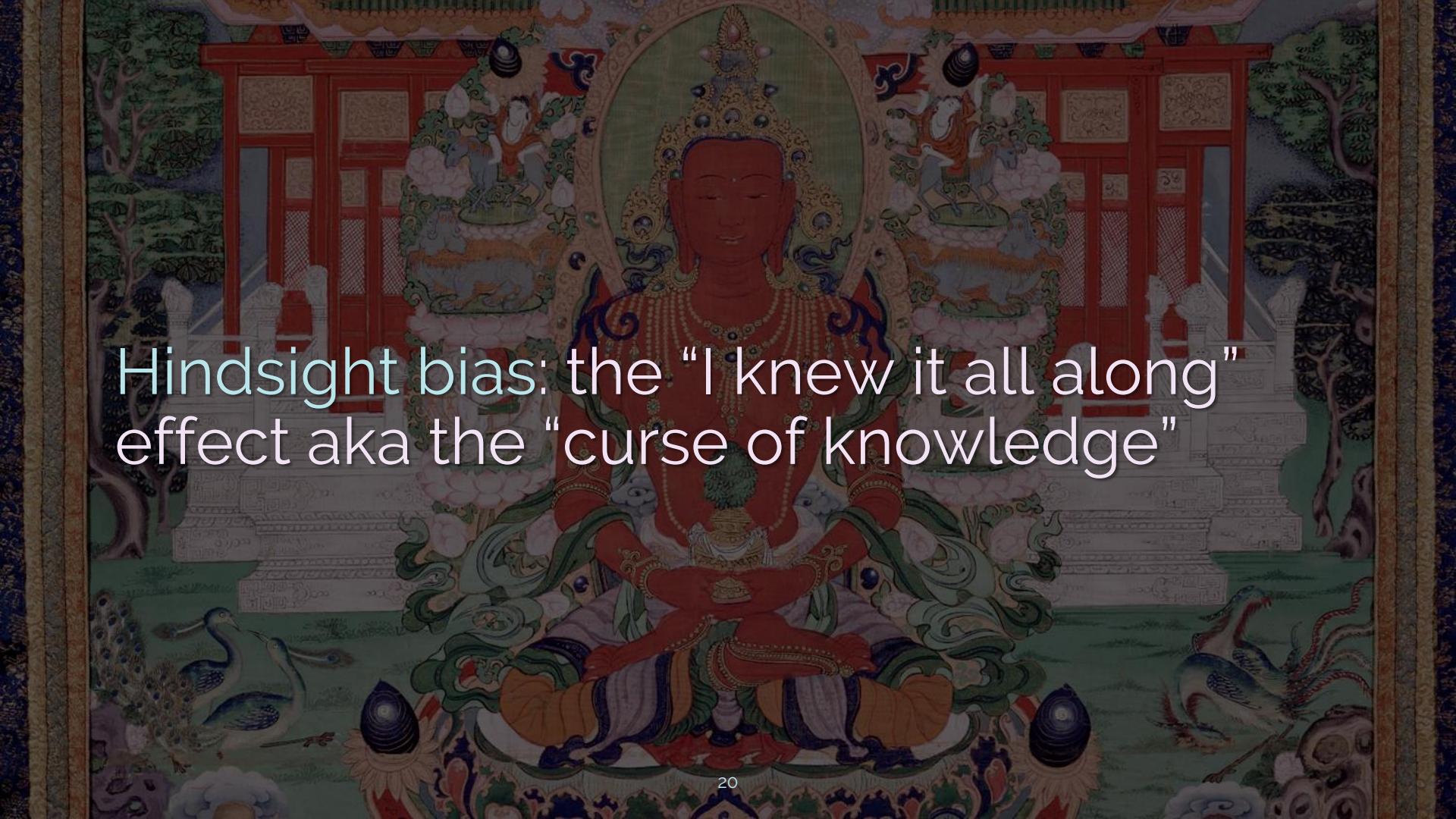
The term “human error” is less grounded to reality than we believe...

Hindsight & Outcome Bias

A landscape painting by Claude Monet, likely "The Path at Giverny" (1896). It depicts a winding path through a lush green garden, with a simple wooden fence visible in the background. The style is characteristic of Impressionism, with visible brushstrokes and a focus on light and color.

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



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”

A dark, atmospheric painting depicting a scholar's study or library. In the center, an elderly man with a long white beard sits at a desk, illuminated by a single candle. On the desk are several open books, a small still life arrangement, and a skull. Behind him, another figure is partially visible. The room is filled with tall stacks of books, a large vase with flowers, and various objects on shelves, creating a sense of a cluttered but scholarly environment.

Outcome bias: judging a decision based
on its eventual outcome

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

A painting depicting a woman in a traditional dress playing a harpsichord. She is looking down at the instrument. In the foreground, a small figure, possibly a child, is seated on the harpsichord's keyboard, reaching out towards the keys.

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

We unfairly hold people accountable for events beyond their control

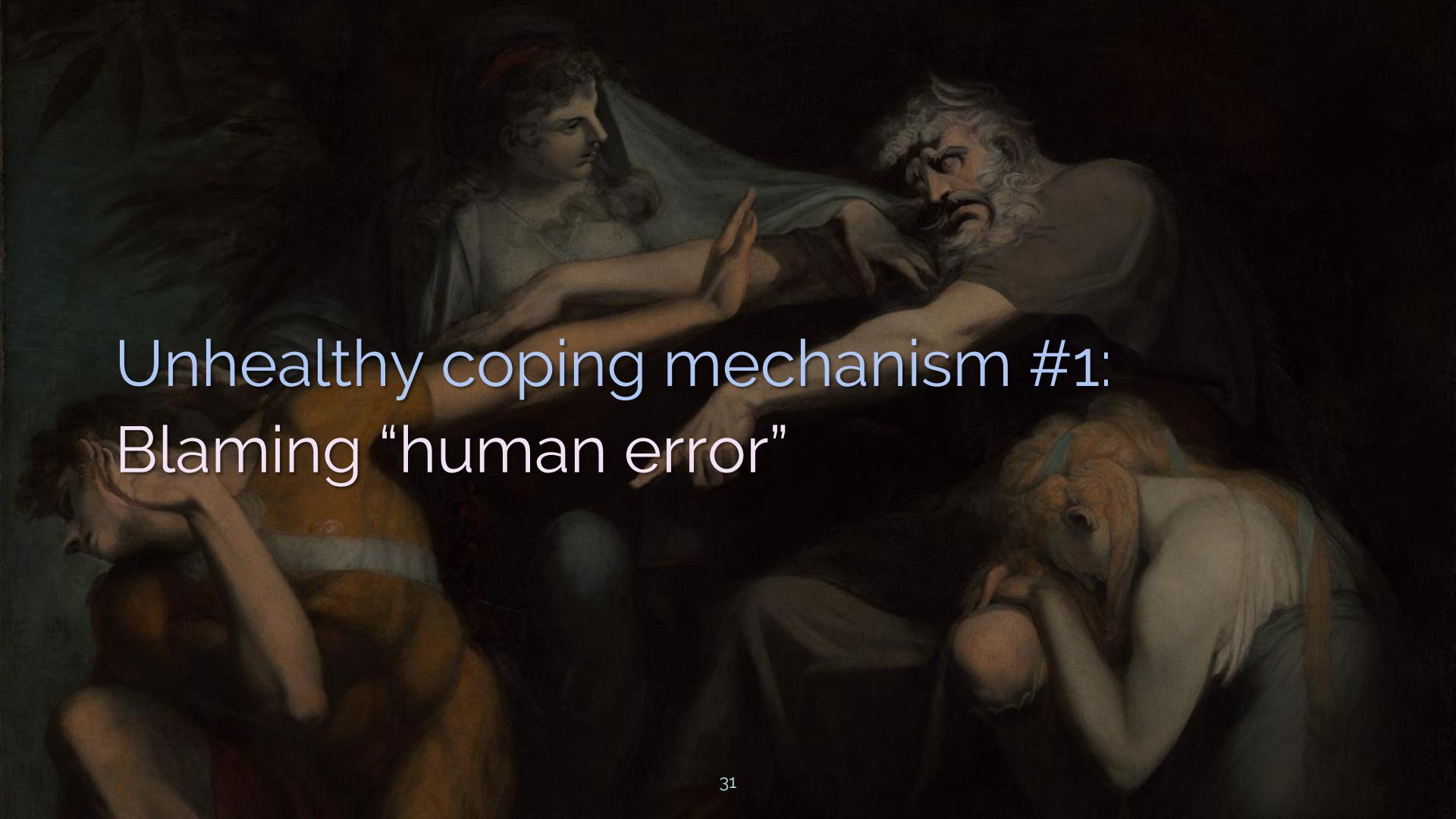


e.g. CapitalOne – did the breach really represent a failure in their strategy? (No.)

These biases change how we cope with failure...

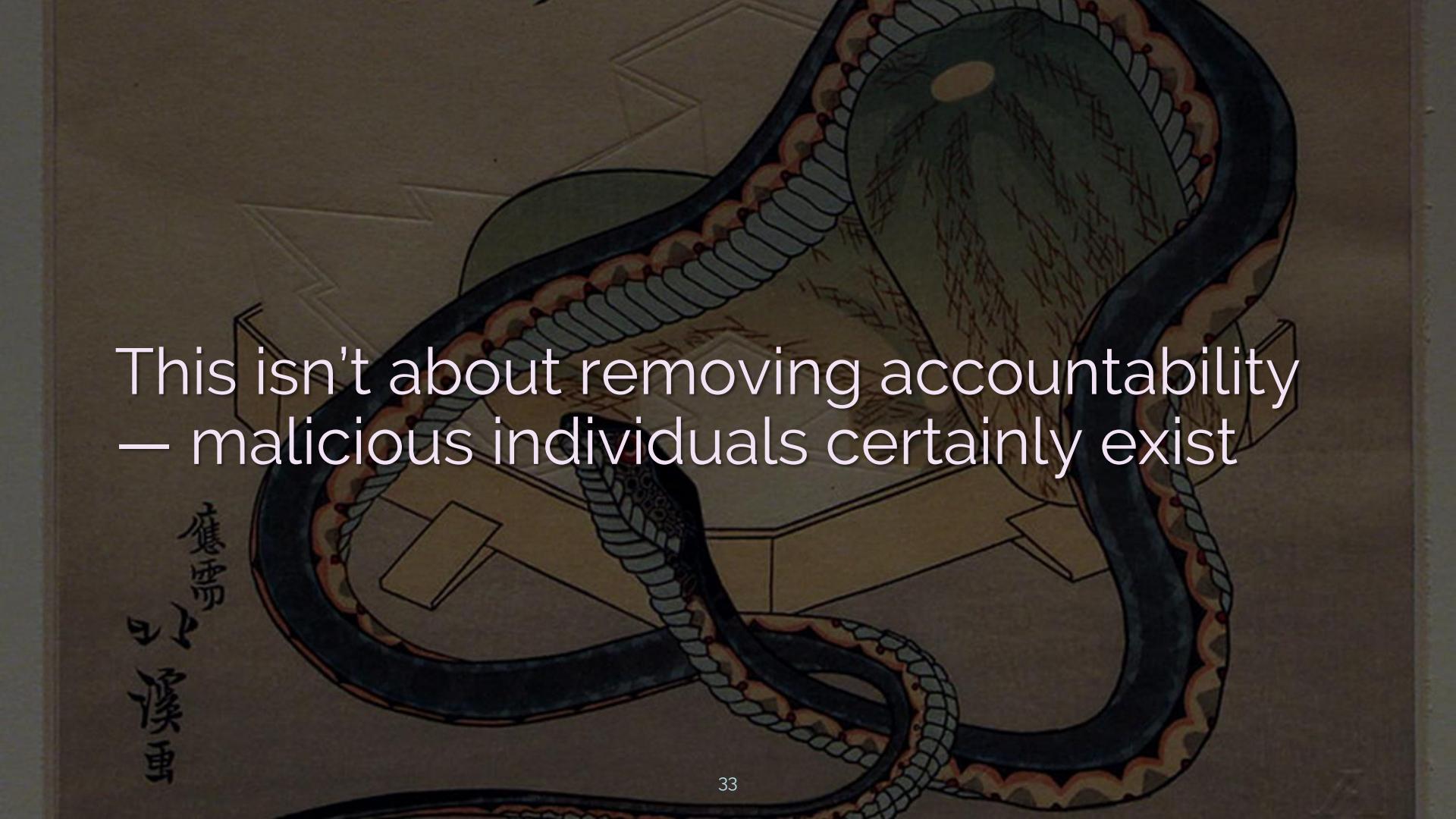
A dark, somber painting depicting a man in a suit holding a bloody hand, appearing distressed or in pain. Another figure is lying nearby, suggesting a scene of violence or suffering.

Unhealthy Coping Mechanisms

A dramatic painting depicting a group of figures in a dark, emotional scene. In the center, a man with long, curly hair and a beard is shown in a state of distress, holding his head in his hands. To his left, another figure is seen from behind, also appearing distressed. Above them, a woman looks down with a somber expression. The lighting is low, creating strong shadows and highlights that emphasize the emotional intensity of the scene.

Unhealthy coping mechanism #1:
Blaming “human error”

Infosec's fav hobbies: PICNIC & PEBKAC

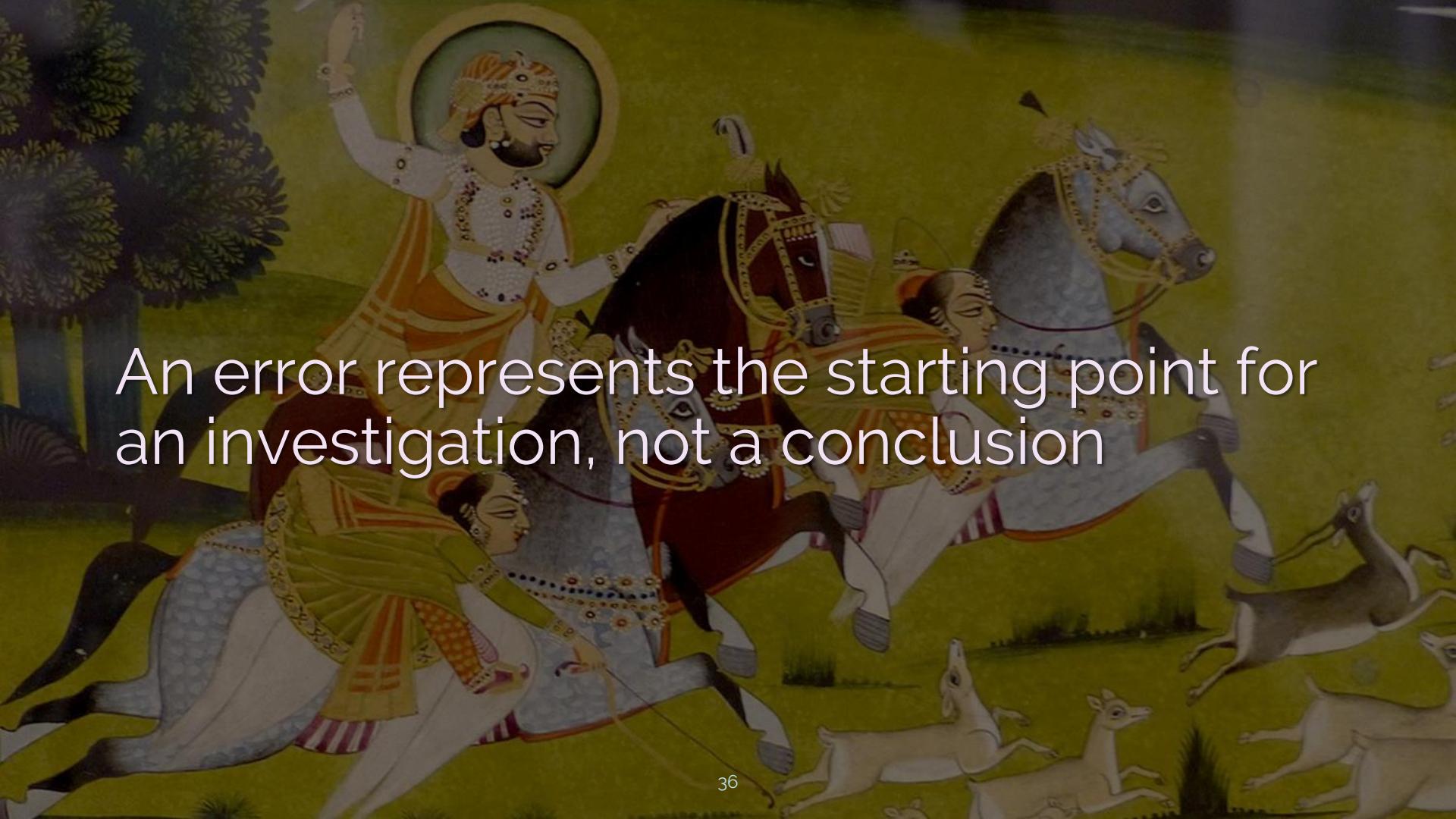


This isn't about removing accountability
– malicious individuals certainly exist

應需
水溪畫

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?”

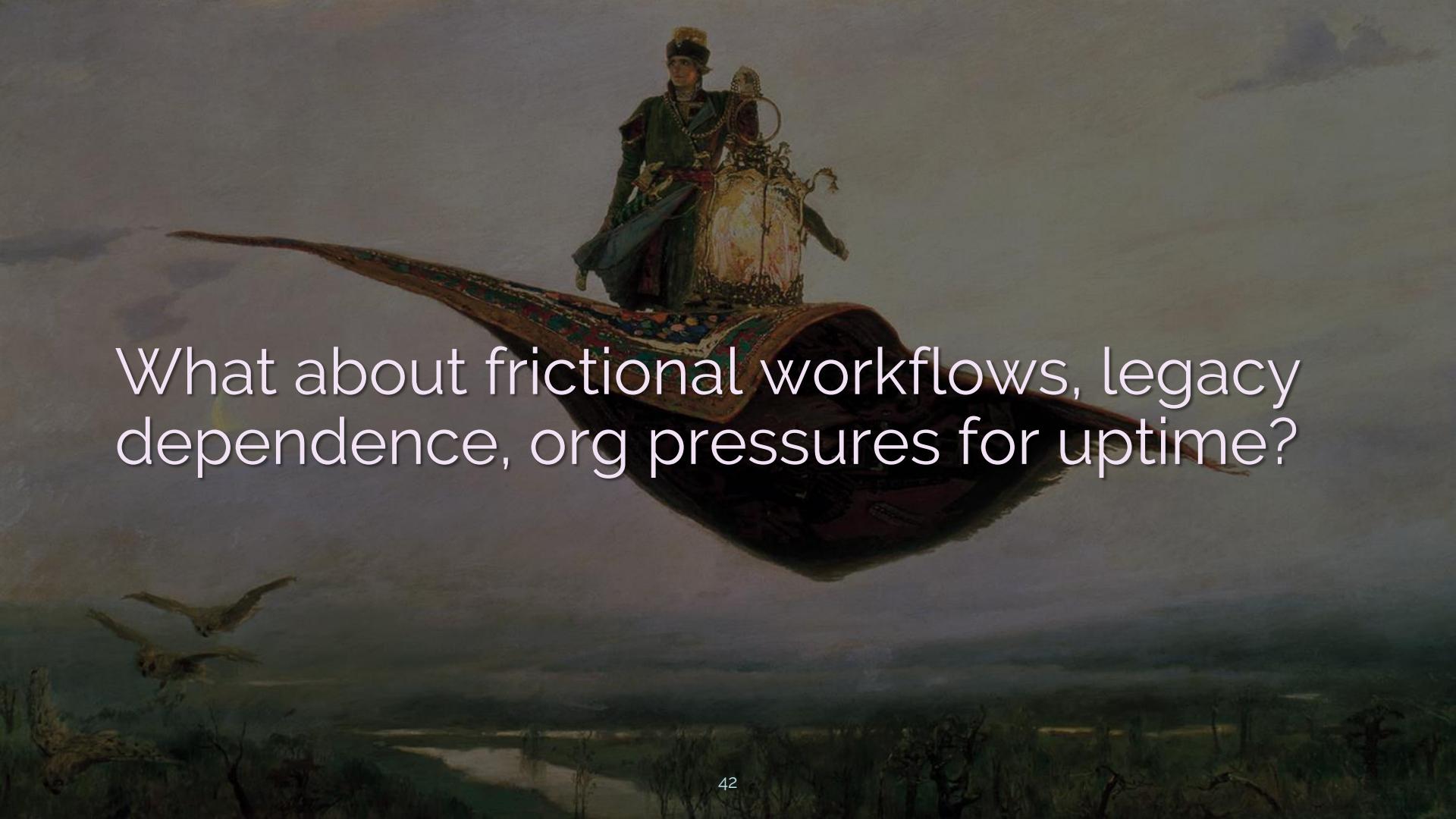
These questions go unanswered if we accept the “human error” explanation

A traditional Korean dragon (myeong) painting in the background. The dragon is green and yellow, with a fierce expression, sharp teeth, and a long, flowing tail. It is surrounded by swirling clouds and smoke, creating a dramatic and mythical atmosphere.

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.

A painting of a man in traditional attire, including a tall hat and a patterned robe, riding a large, ornate, flying carpet. The carpet is decorated with intricate patterns and has long, sweeping ends. They are flying over a landscape with rolling hills and birds in flight. The background is a dramatic sky with clouds.

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 dramatic painting depicting the mythological figure Prometheus being punished. He is shown from the waist up, lying on his back on a dark, rocky surface. His body is contorted in agony; his head is twisted back, his mouth is wide open as if screaming, and his arms are bent at the elbows with hands near his head. A large, dark, winged eagle with sharp talons is perched on his chest, tearing at his heart. The background is a dark, stormy sky with distant, jagged mountain peaks.

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 dress and a bearded man in a brown robe, surrounded by fruit and foliage.

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



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 goat standing in a vast, arid landscape. The goat is in the foreground, facing left, with its long, shaggy hair and long ears clearly visible. The background features rolling hills and mountains under a hazy sky.

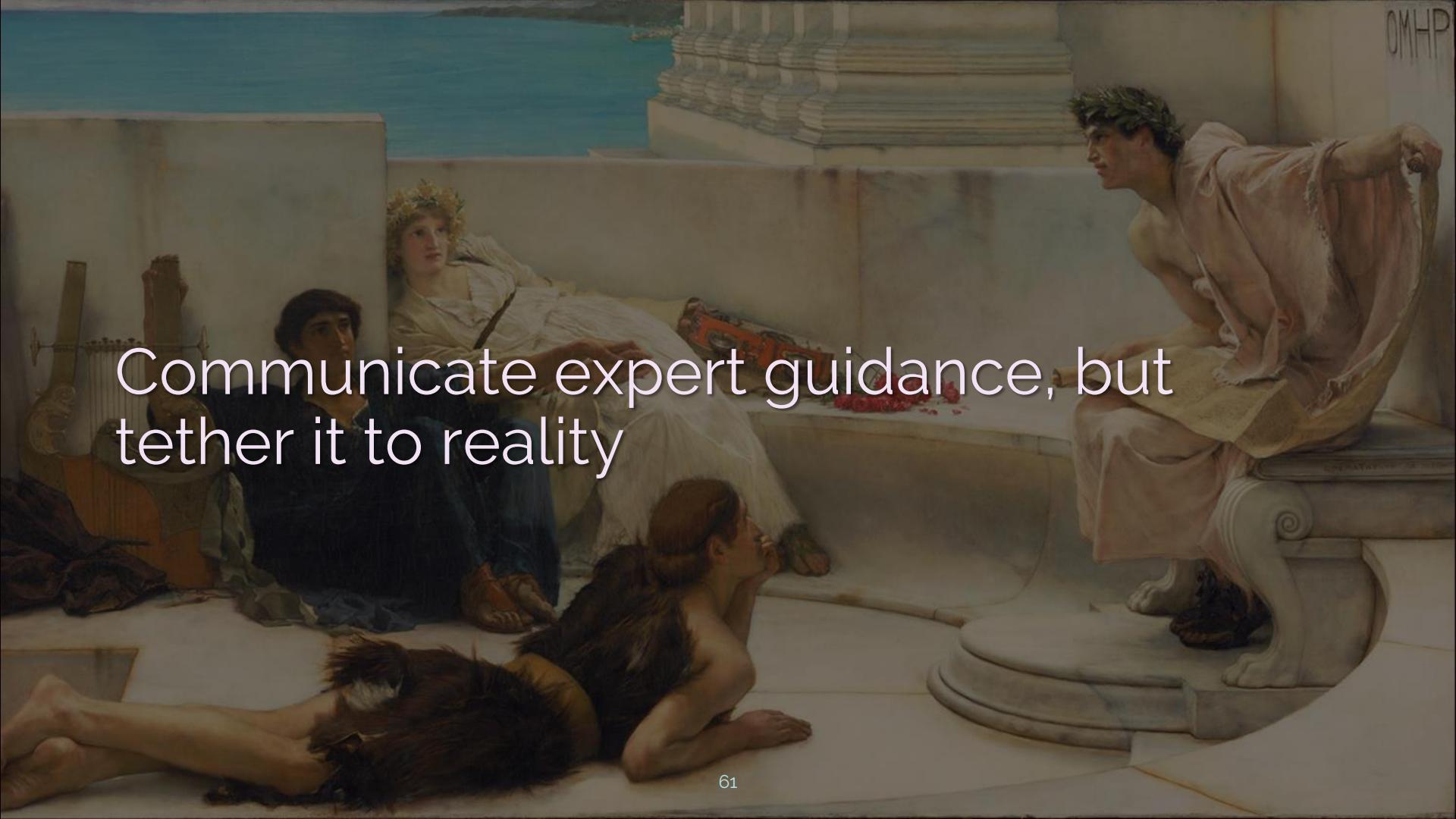
Discipline doesn't actually fix the “policy violation” cause (but it does scapegoat)

Case study: SS&C & BEC

A dramatic painting depicting a scene of physical struggle or control. A woman in a red dress is shown from the waist up, her head tilted back and eyes closed as if in distress or unconsciousness. Another woman, wearing a yellow dress and a gold bracelet, is holding her down, her hands gripping the other's arms. The lighting is dramatic, with strong highlights and shadows. The background is dark and indistinct.

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

Post-WWII analysis: Improved design of cockpit controls won over pilot training

A classical painting depicting a scene of guidance and reality. In the foreground, a figure with long dark hair, wearing a lion's skin, lies on the ground, looking up at a man who is kneeling on a large column. The kneeling man is holding a scroll and appears to be giving guidance. In the background, a woman with a laurel wreath lies on a bed, looking down at the scene. A harp is visible on the left side of the painting.

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.

A classical painting featuring three female figures. In the center, a woman in a white robe holds a sword and looks down. To her left, another woman in a blue robe holds a staff and looks towards the center. To her right, a woman in a red robe holds a balance scale and looks upwards. The scene is set against a background of red curtains and green foliage.

Unhealthy coping mechanism #3: The just-world hypothesis

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



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"



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



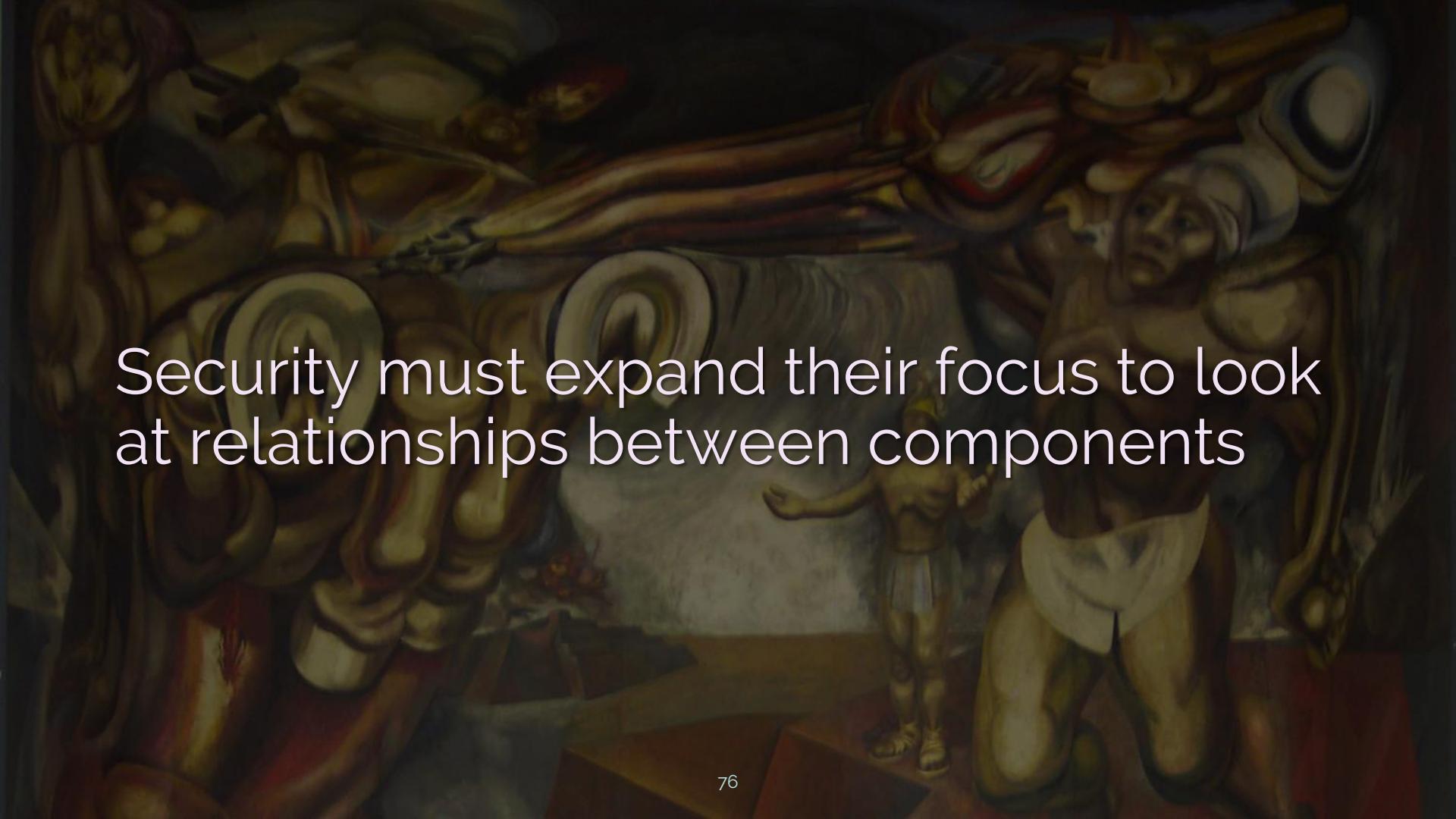
Infosec will progress when we ensure
the easy way is the secure way

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

An abstract painting in the style of Wassily Kandinsky. It features a variety of geometric shapes like circles, squares, and rectangles in shades of yellow, blue, red, and purple. The composition includes several radiating lines from a central point, some with small circles at their ends. In the lower right, there are two dark purple shapes containing smaller, multi-colored squares. The overall effect is dynamic and organic.

System perspective

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

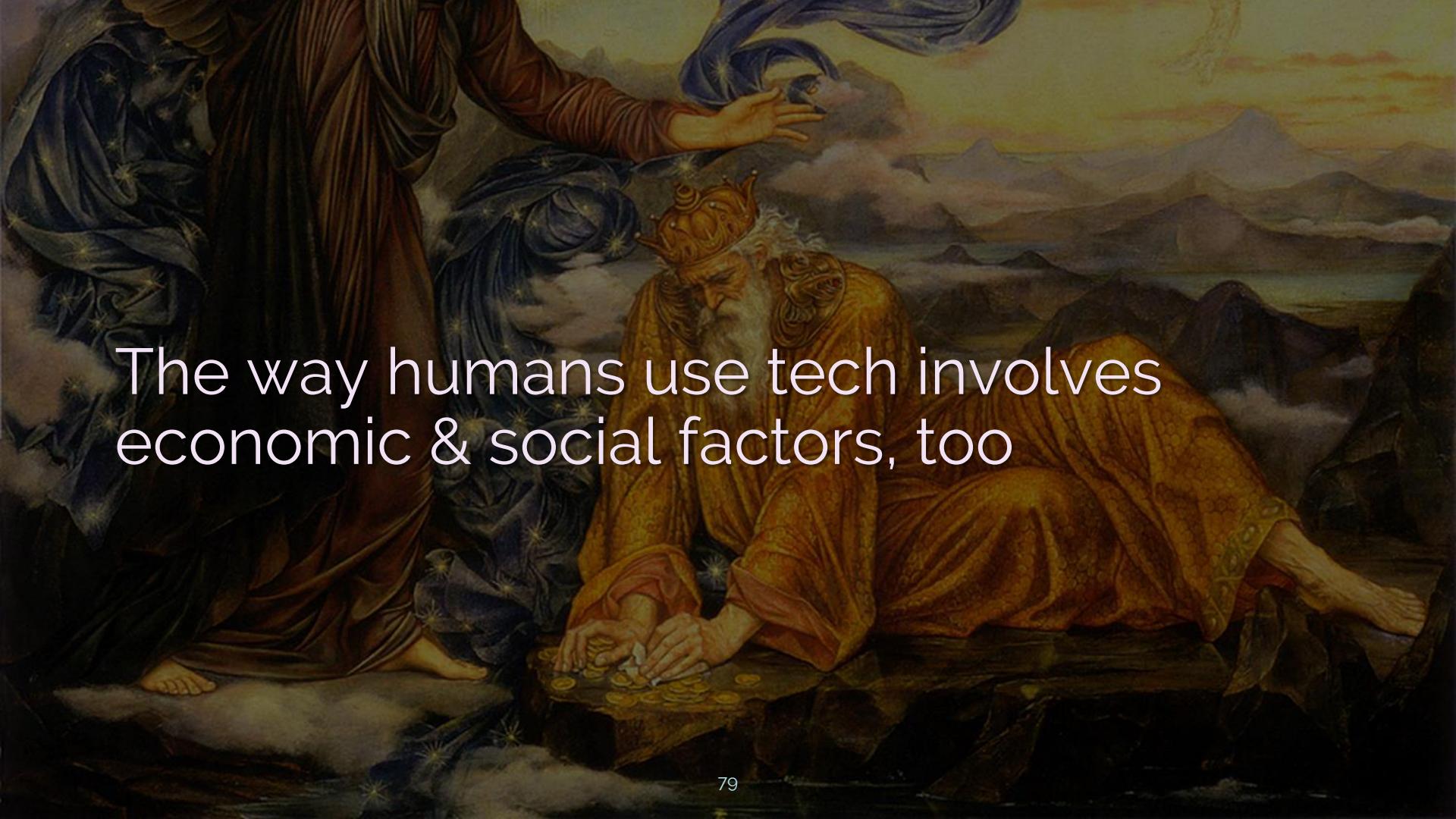


Security must expand their focus to look at relationships between components

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

A painting depicting a king in a golden robe and crown, sitting on a large rock. He is surrounded by a dark, star-filled sky and distant mountains. A hand reaches down from the top left, holding a small object. The king is looking down at a pile of gold coins on the ground.

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

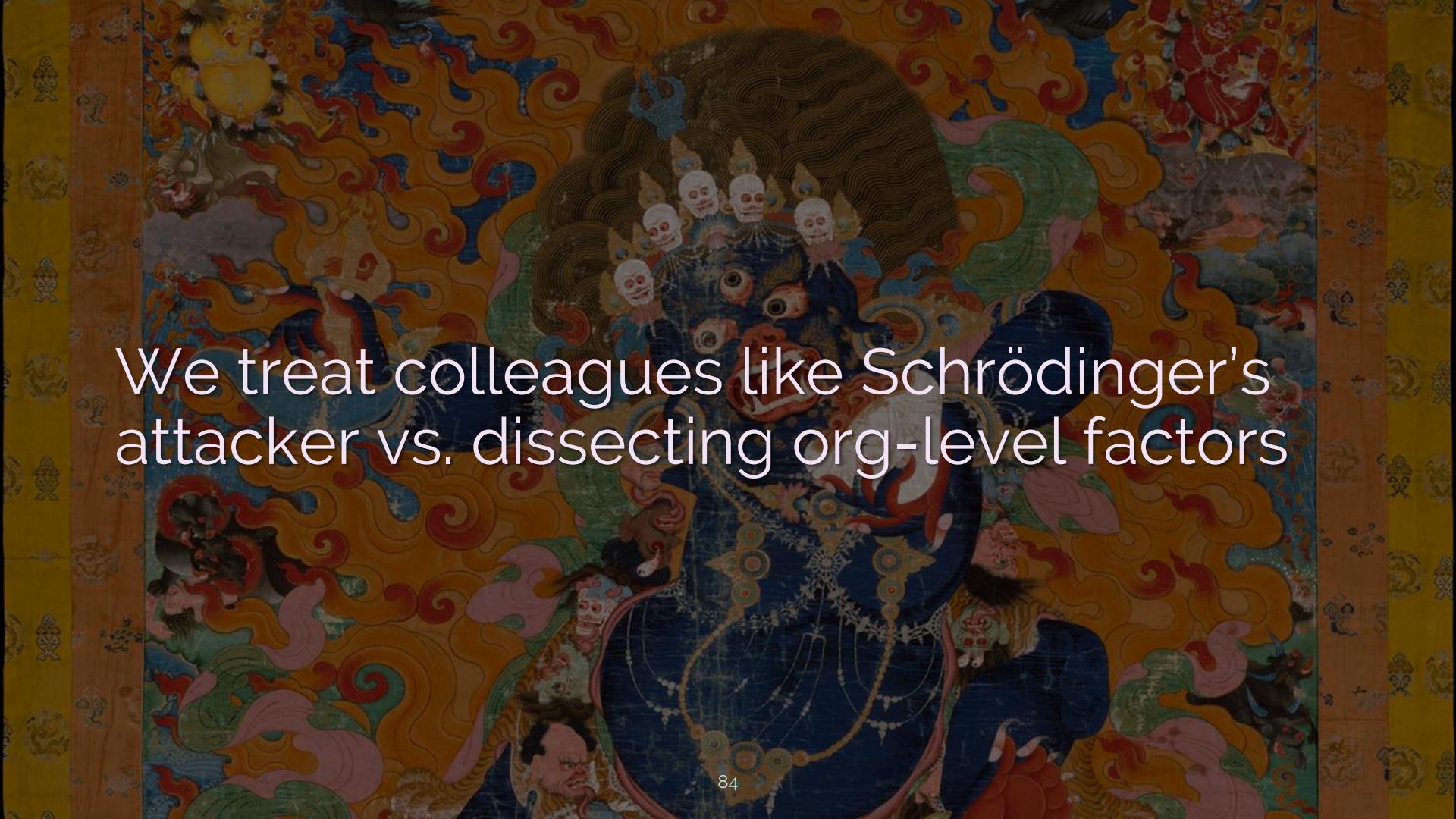
Economic factors: revenue & profit goals,
compensation schemes, budgeting, etc.

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



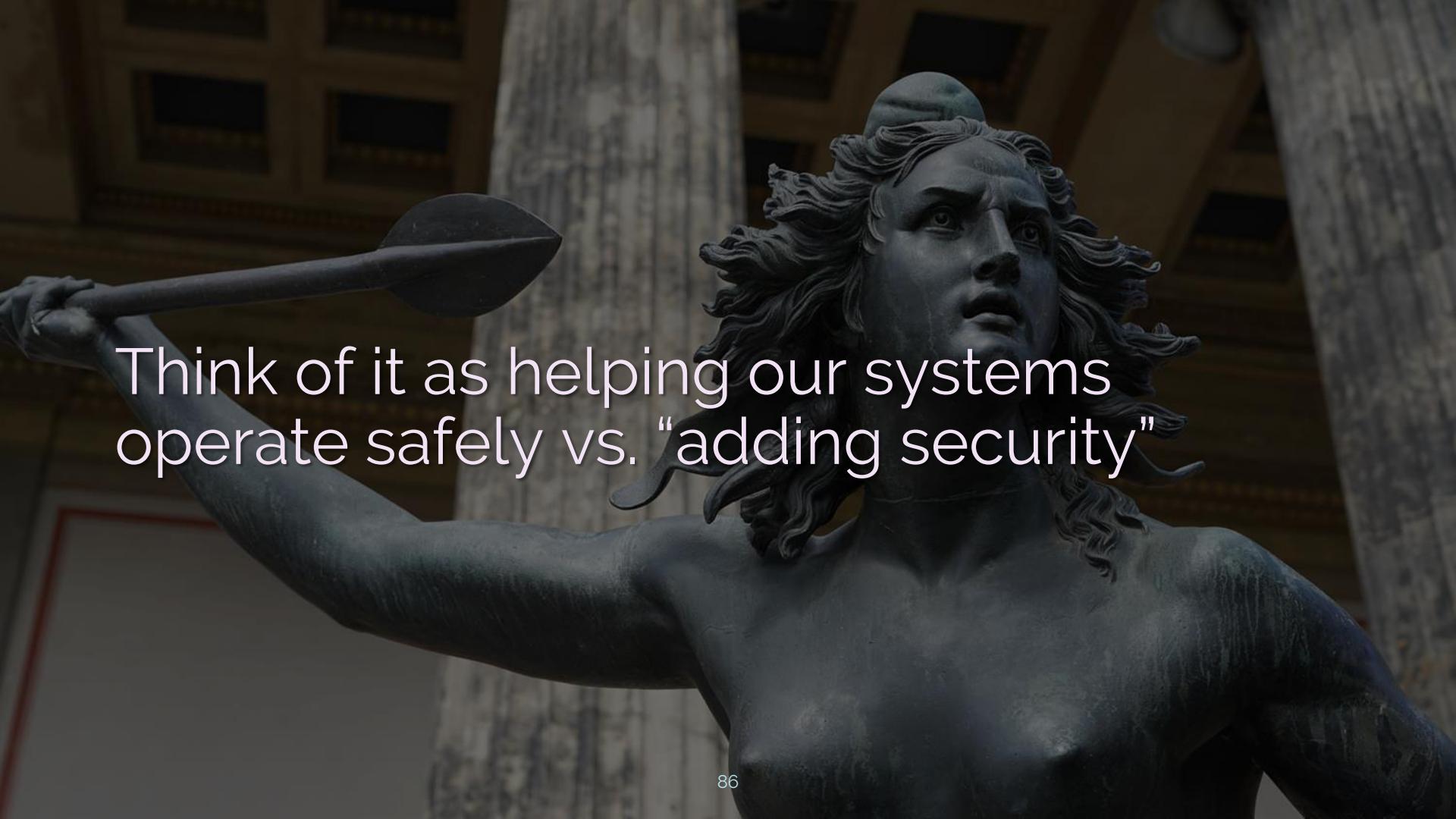
Pressure to do more work, faster is a vulnerability. So is a political culture.

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

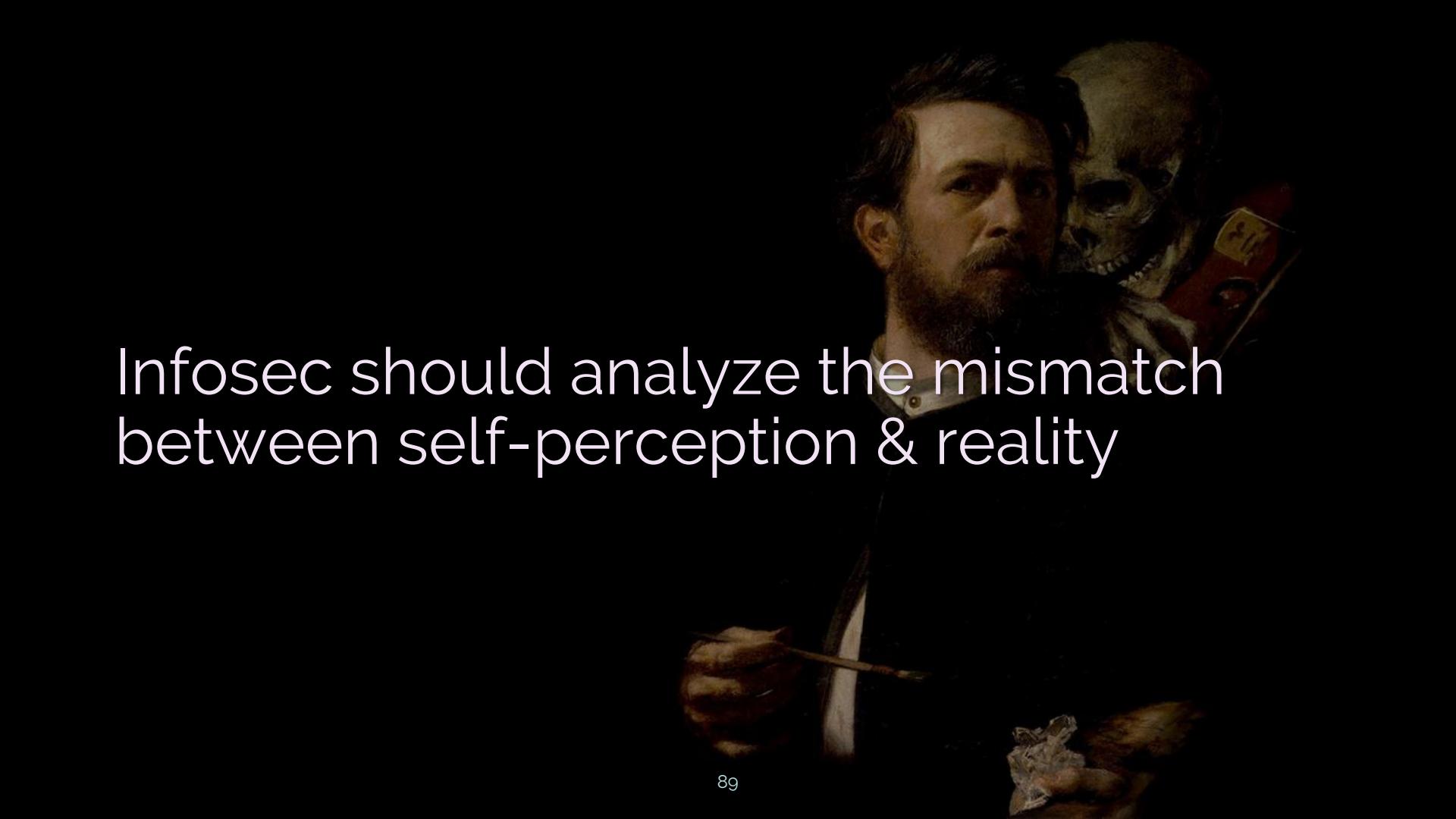
**Security is something a system does,
not something a system has.**



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

A dark, chiaroscuro painting by Georges de la Tour. It depicts a man with a beard and mustache, wearing a dark cap and a light-colored shirt. He is shown from the chest up, looking slightly to his right. Resting his head against his shoulder is a skull. In his left hand, he holds a paintbrush and a palette, which is partially visible. His right hand rests on a dark, crumpled object. The background is dark and indistinct.

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?



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

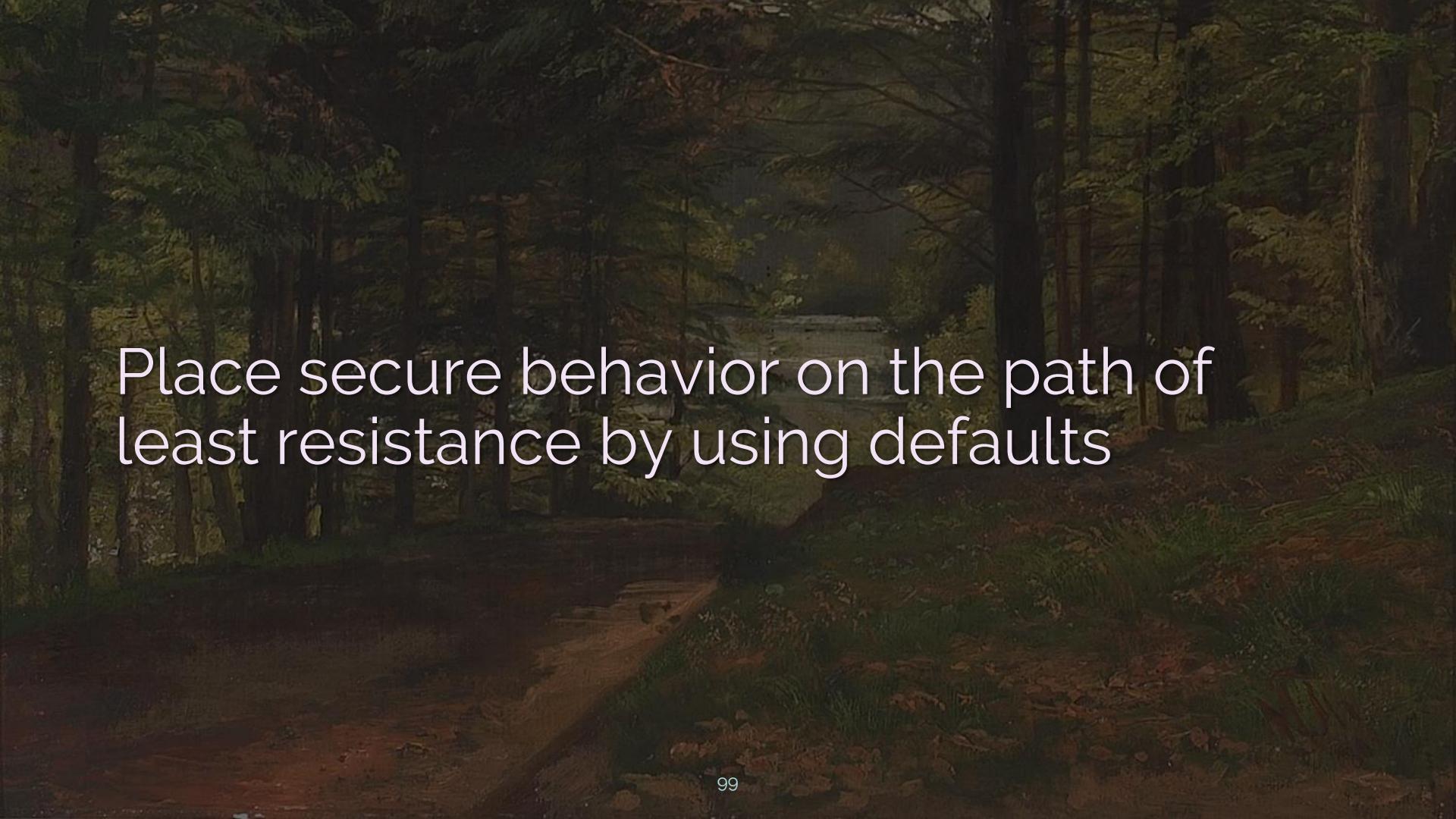


Daily Reminder for Devops & Infosec people designing tools: Alerts that always show up red don't make your systems more reliable or secure. They just teach people to ignore alerts.

WARNING: CYBER ANOMALY

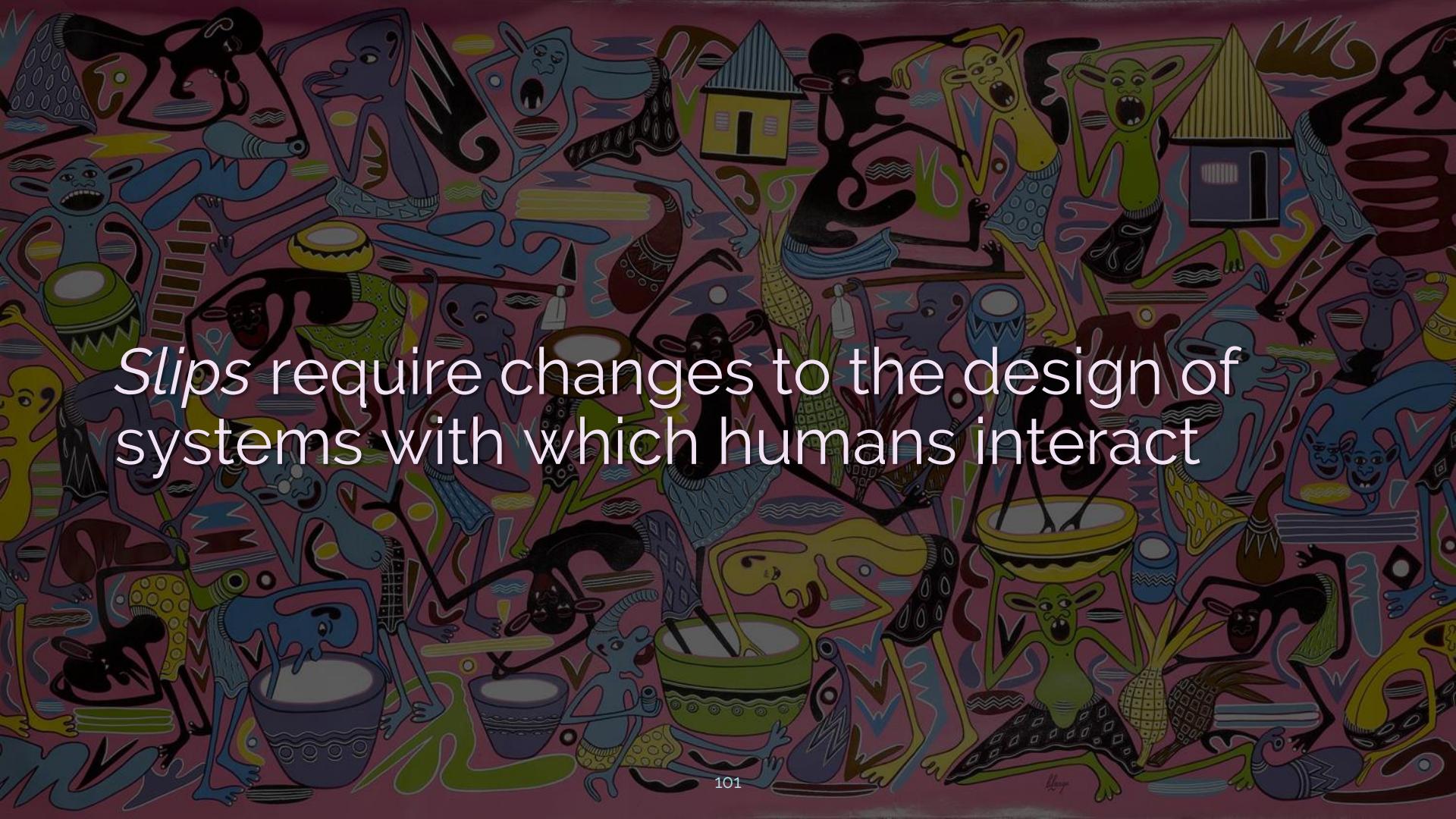
(thanks Raytheon)

Choice architecture: organizing the context in which people make decisions

A dark, atmospheric painting of a path through a forest at night or in low light. The scene is dominated by dark green and brown tones, with silhouettes of trees and branches against a lighter, possibly moonlit sky. A narrow path or stream bed leads from the foreground towards the center of the composition.

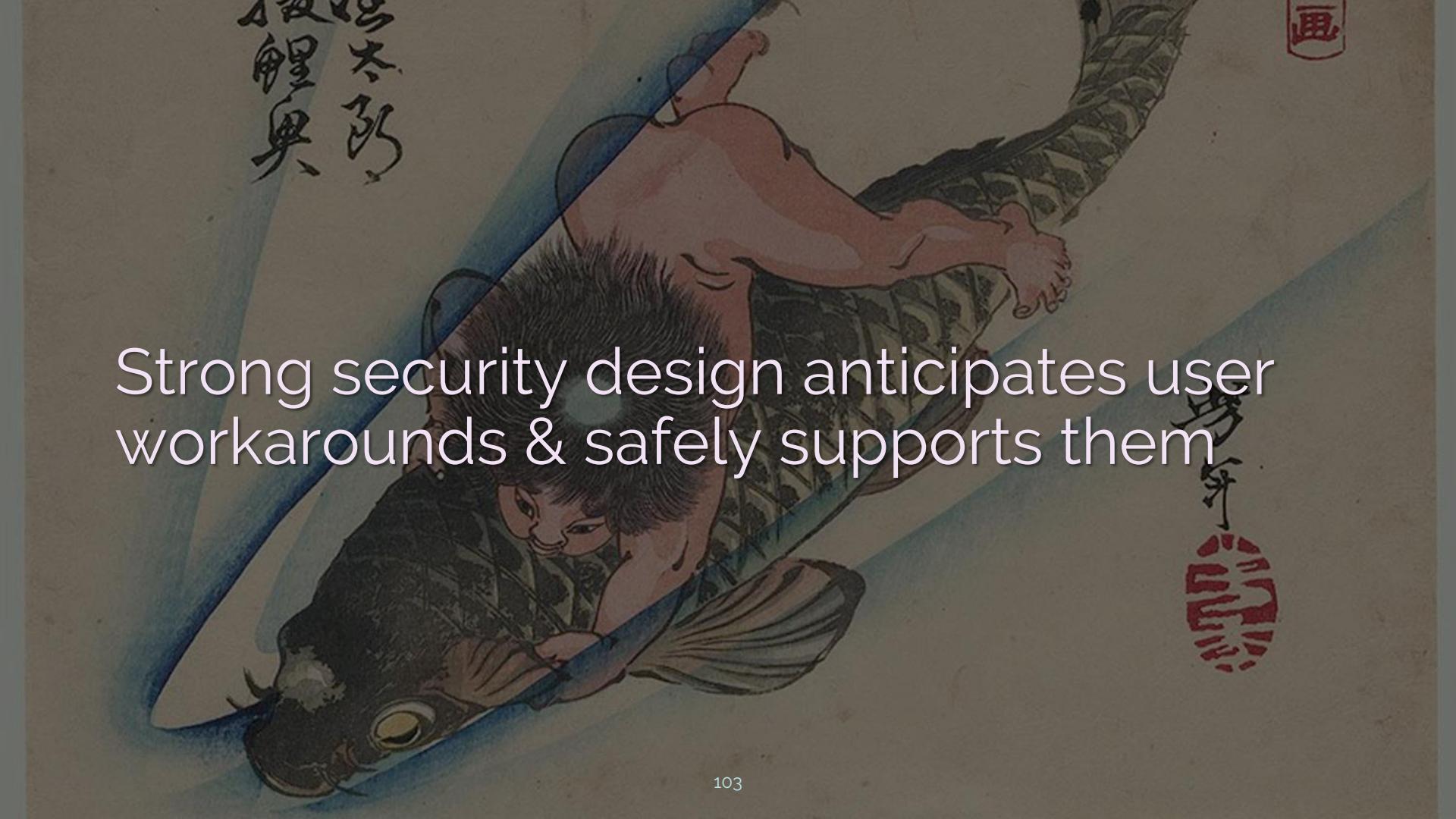
Place secure behavior on the path of least resistance by using defaults

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

A painting depicting Cleopatra VII of Egypt in an ornate, Egyptian-themed setting. She is shown reclining on a red sofa, wearing a traditional Egyptian headdress and a blue and gold patterned dress. A large, pink lotus flower is visible above her head. In the foreground, a large, spotted cat lies on the floor. Several other figures are present, some in traditional Egyptian clothing, others in more modern or Western-style attire. The background features tall, decorated columns and lush greenery.

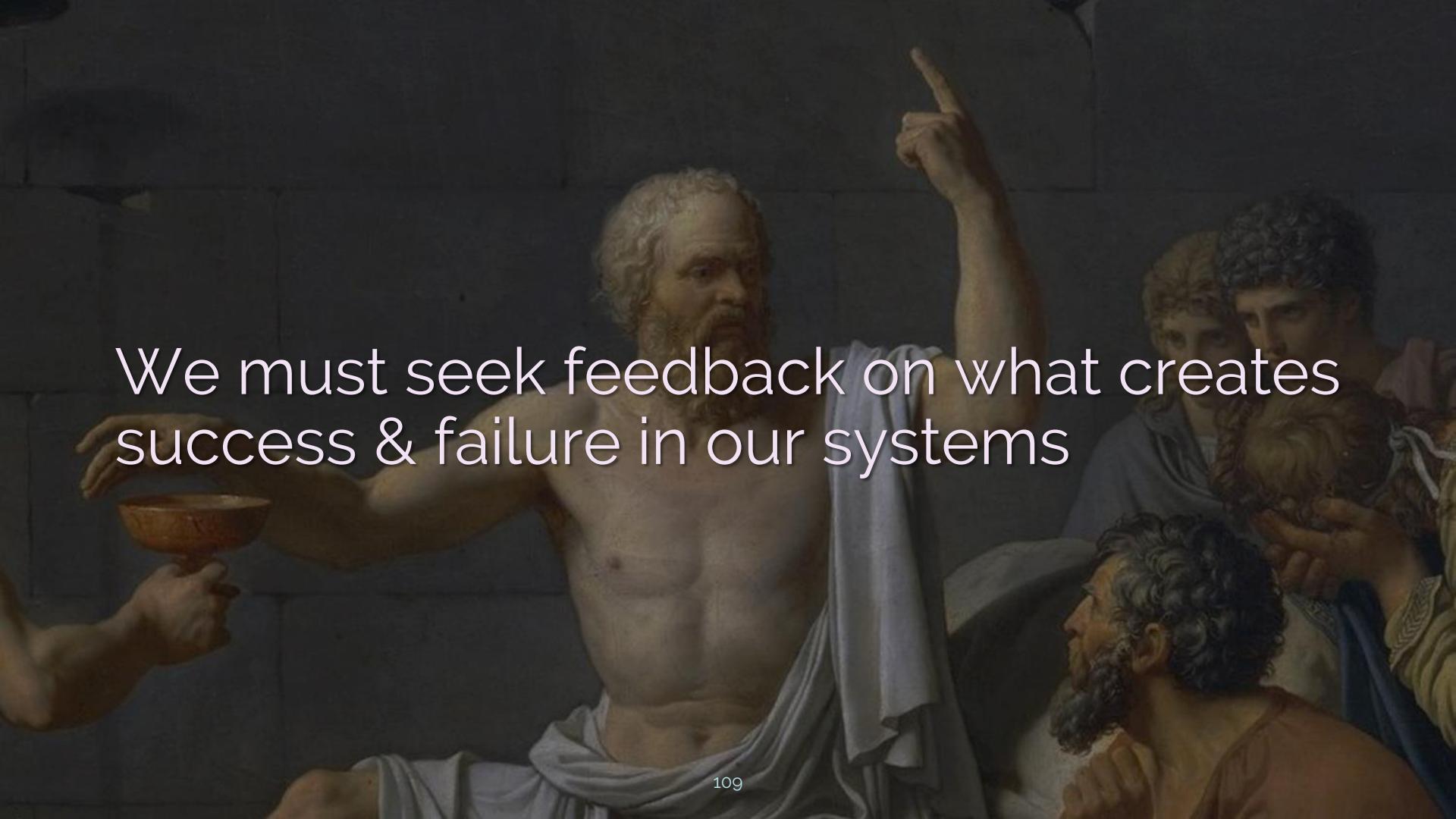
Think in terms of acceptable tradeoffs –
create secure alternatives, not loopholes

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

The background of the image is a reproduction of Hieronymus Bosch's 'The Garden of Earthly Delights'. It depicts a chaotic and fantastical scene filled with various figures, including naked men and women, animals, and mythical creatures, all set against a backdrop of distorted architecture, floating islands, and a dark, turbulent sky.

Chaos Security Engineering

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

A classical painting depicting the philosopher Socrates in the center, shown from the chest up, with his right arm raised and index finger pointing upwards. He has a beard and curly hair. To his left, another figure holds a golden bowl. In the foreground, the head of a man with dark, curly hair and a beard is visible. The background is dark.

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

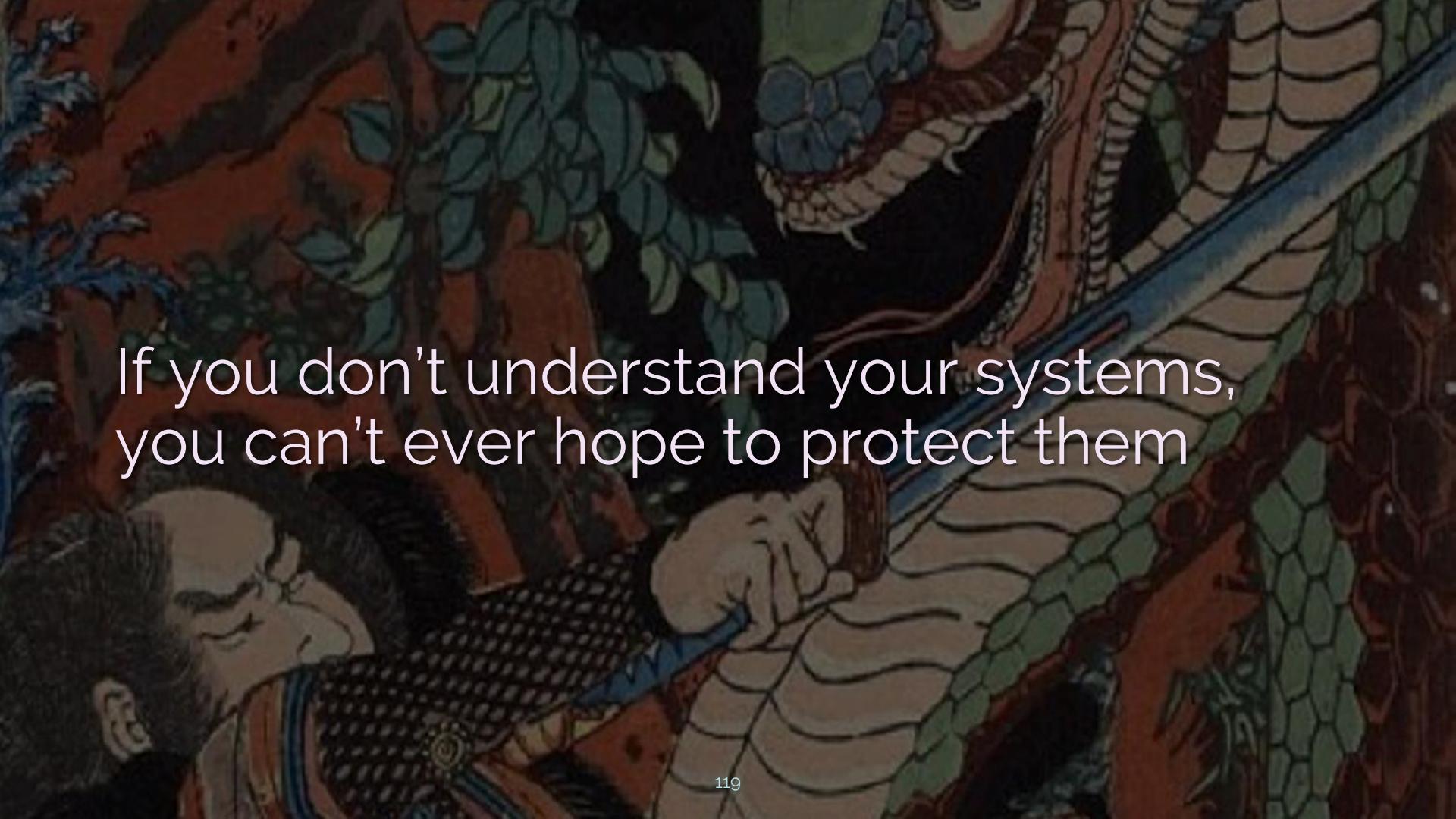
Chaos eng: continual experimentation to evaluate response to unexpected failure

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



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...

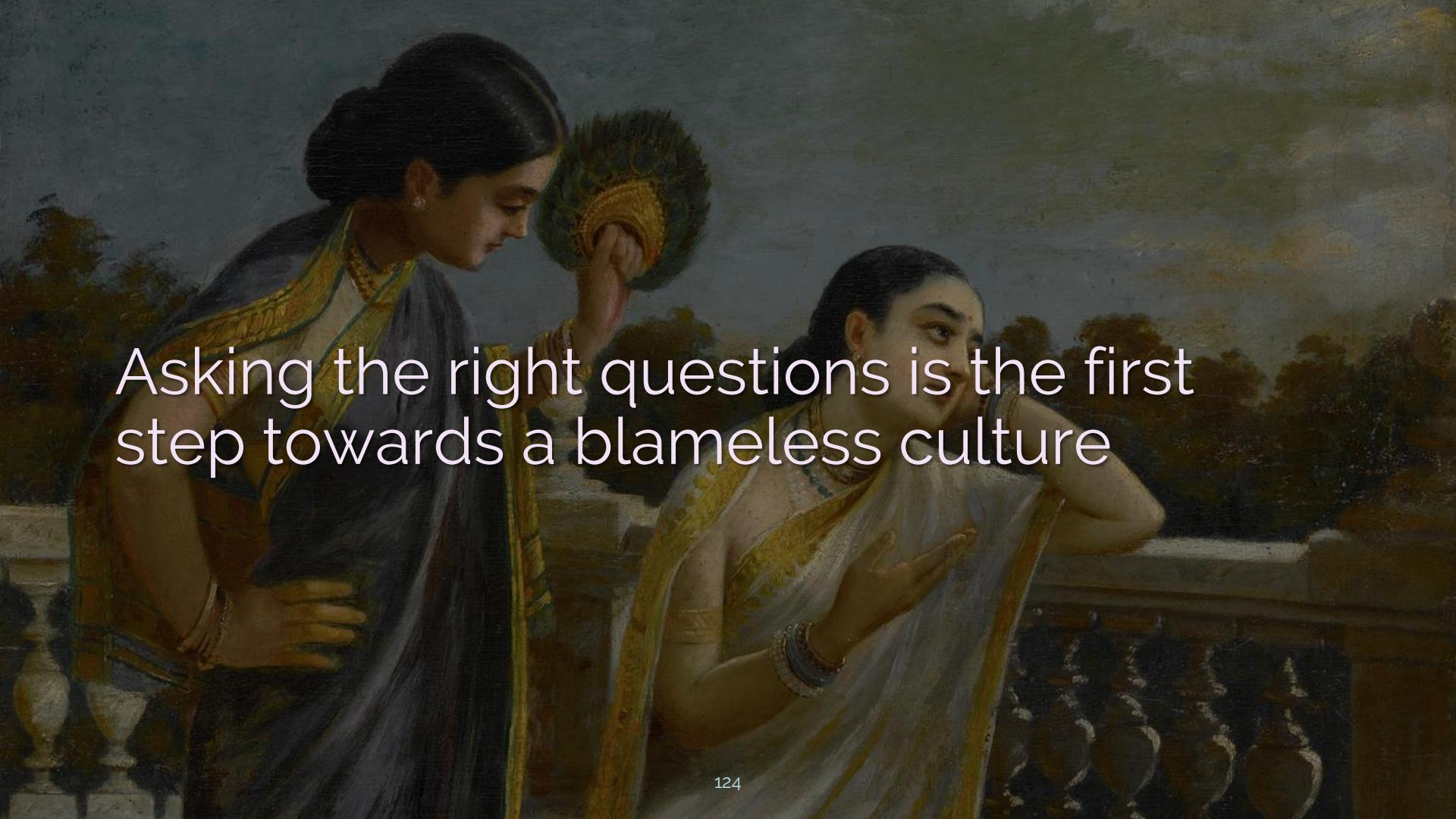
The background of the image is a close-up of a rock wall covered in ancient handprints. These prints are made of red ochre and are arranged in several horizontal rows. The rock has a rough, weathered texture with some darker staining and small white spots. The lighting is low, creating deep shadows and highlighting the texture of the rock and the edges of the handprints.

Blameless Culture



A blameless culture balances safety and accountability – not absolution

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

A traditional Indian painting depicting two women in a garden. One woman, in the foreground, is shown from the side, wearing a dark blue sari with a yellow border and a red blouse. She has her hands joined in a gesture of respect or prayer. The other woman, in the background, is facing towards the viewer, wearing a yellow sari with a green border and a red blouse. She is holding a small golden object, possibly a flower or a piece of jewelry. The background features stylized trees and foliage.

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

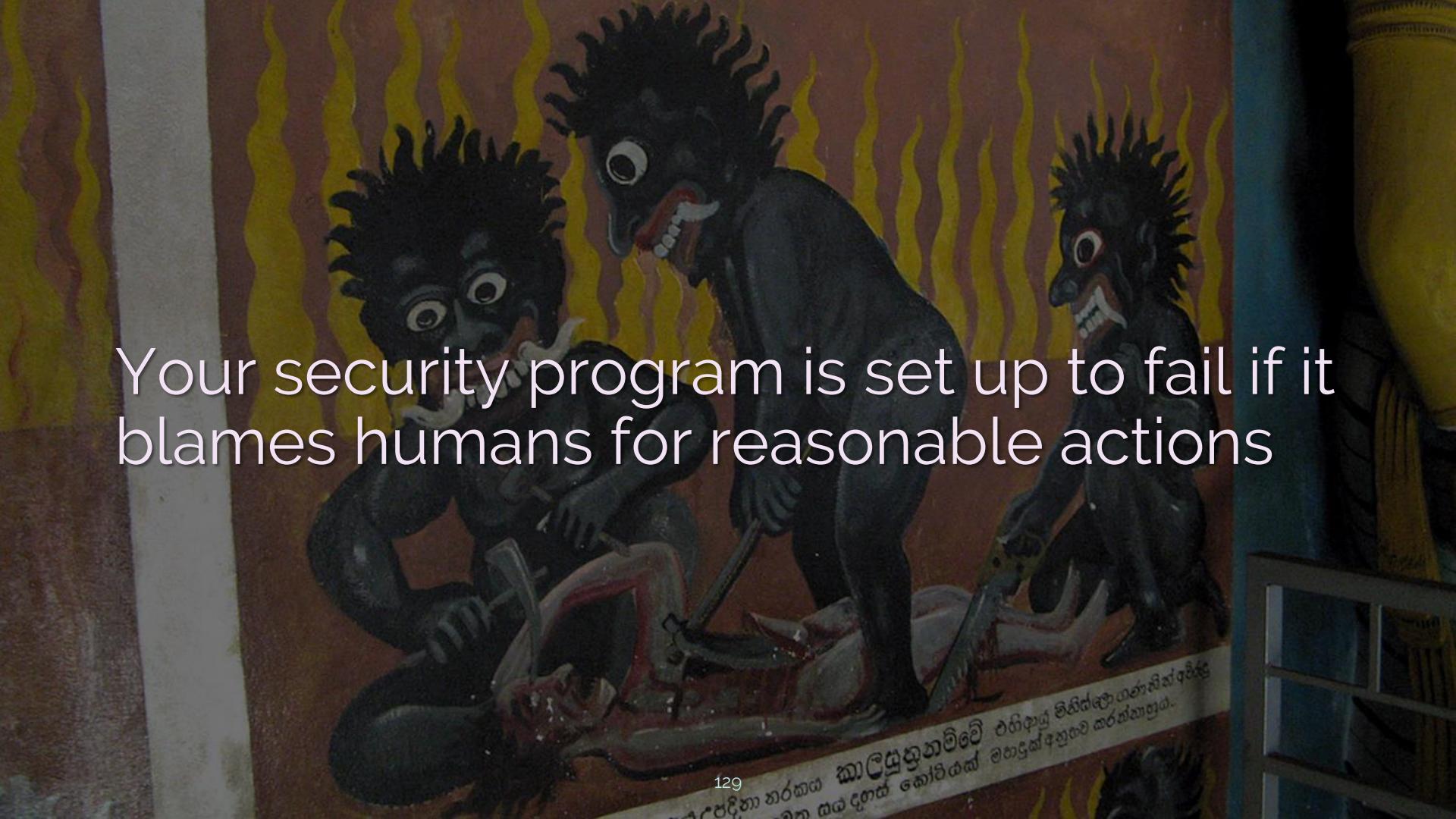
Neutral questions prevent bias from seeping into our incident review

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

Case study: the stressed accountant

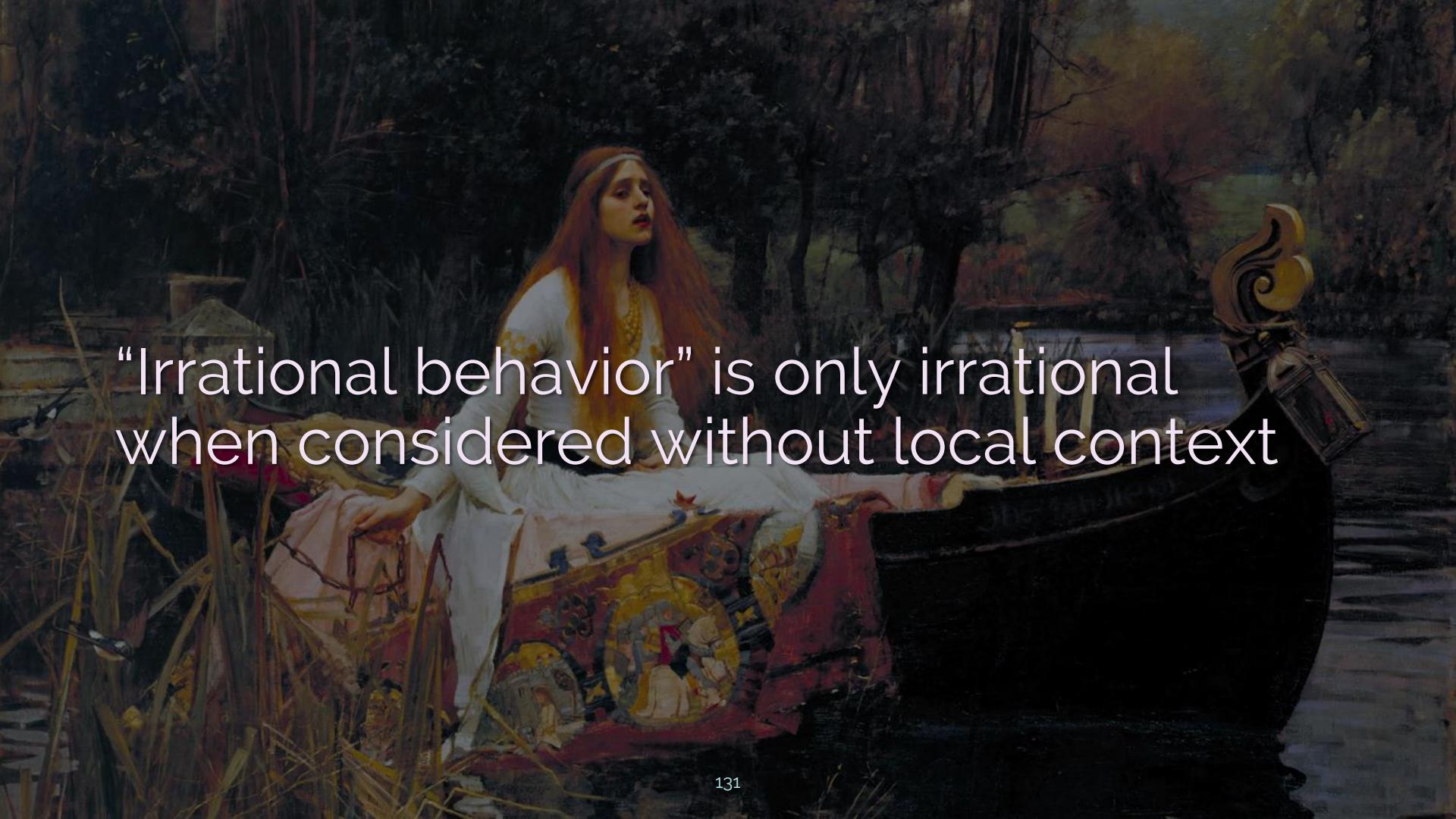
..41.
Courbet.

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



Your security program is set up to fail if it blames humans for reasonable actions

Neutral practitioner questions help sketch a portrait of local rationality

A painting of a woman with long red hair standing next to a horse-drawn carriage. She is wearing a white dress and a yellow necklace. The carriage is decorated with a golden crest. The background is a dark, wooded area.

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

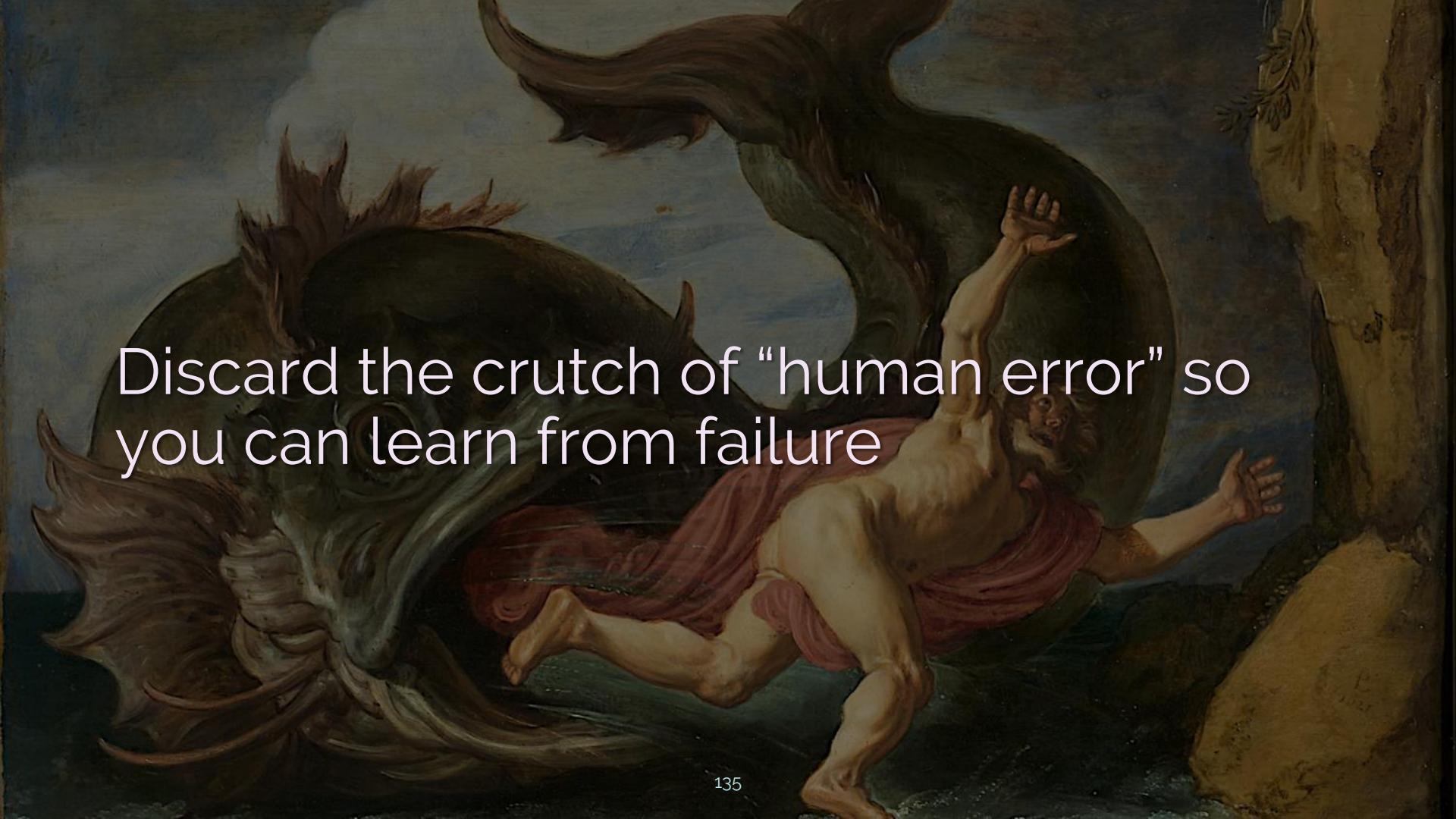
Our goal is to change the *context* of decision-making to promote security



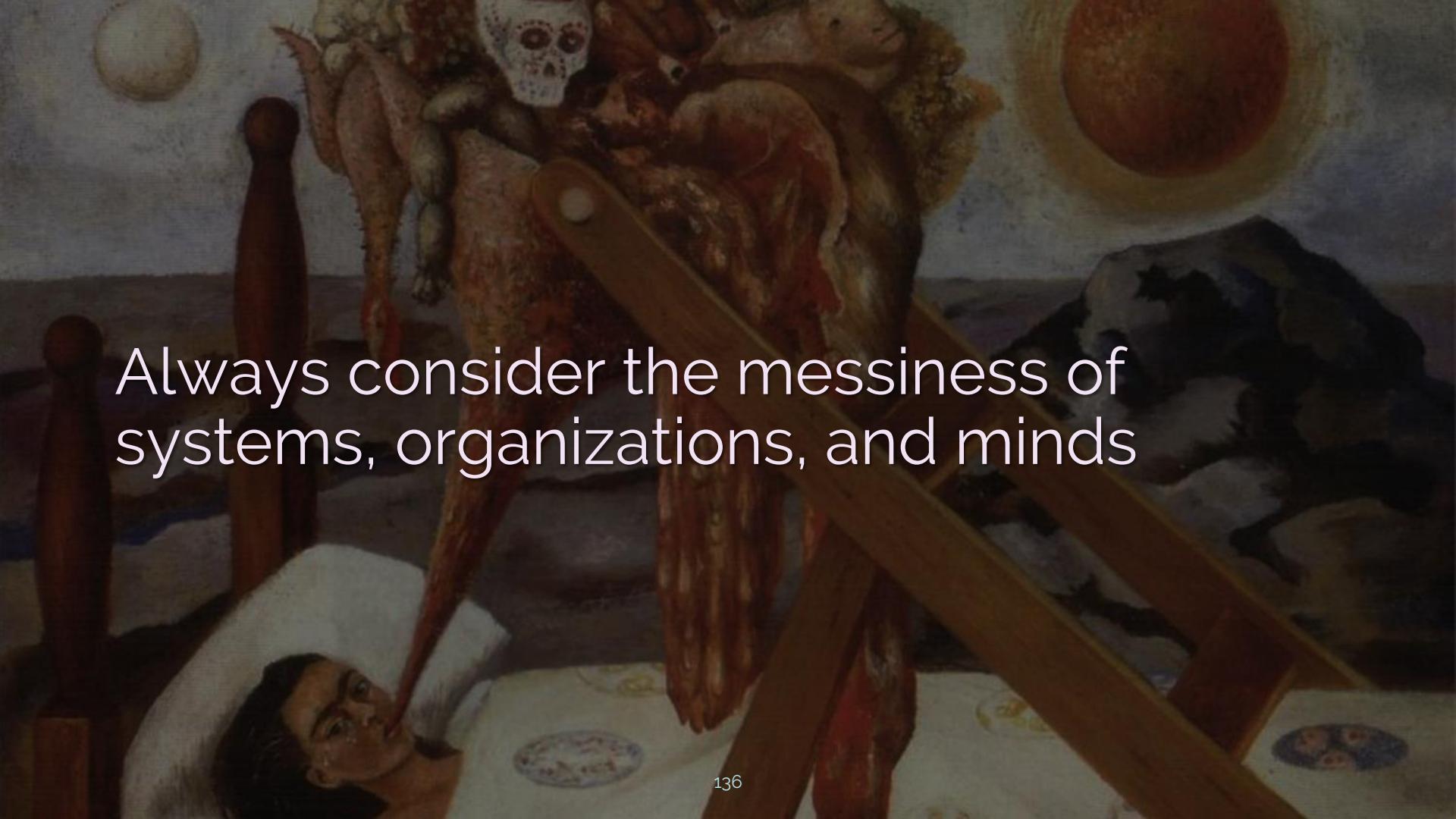
If you're using an ad-hominem attack in incident review, you've veered astray

In Conclusion

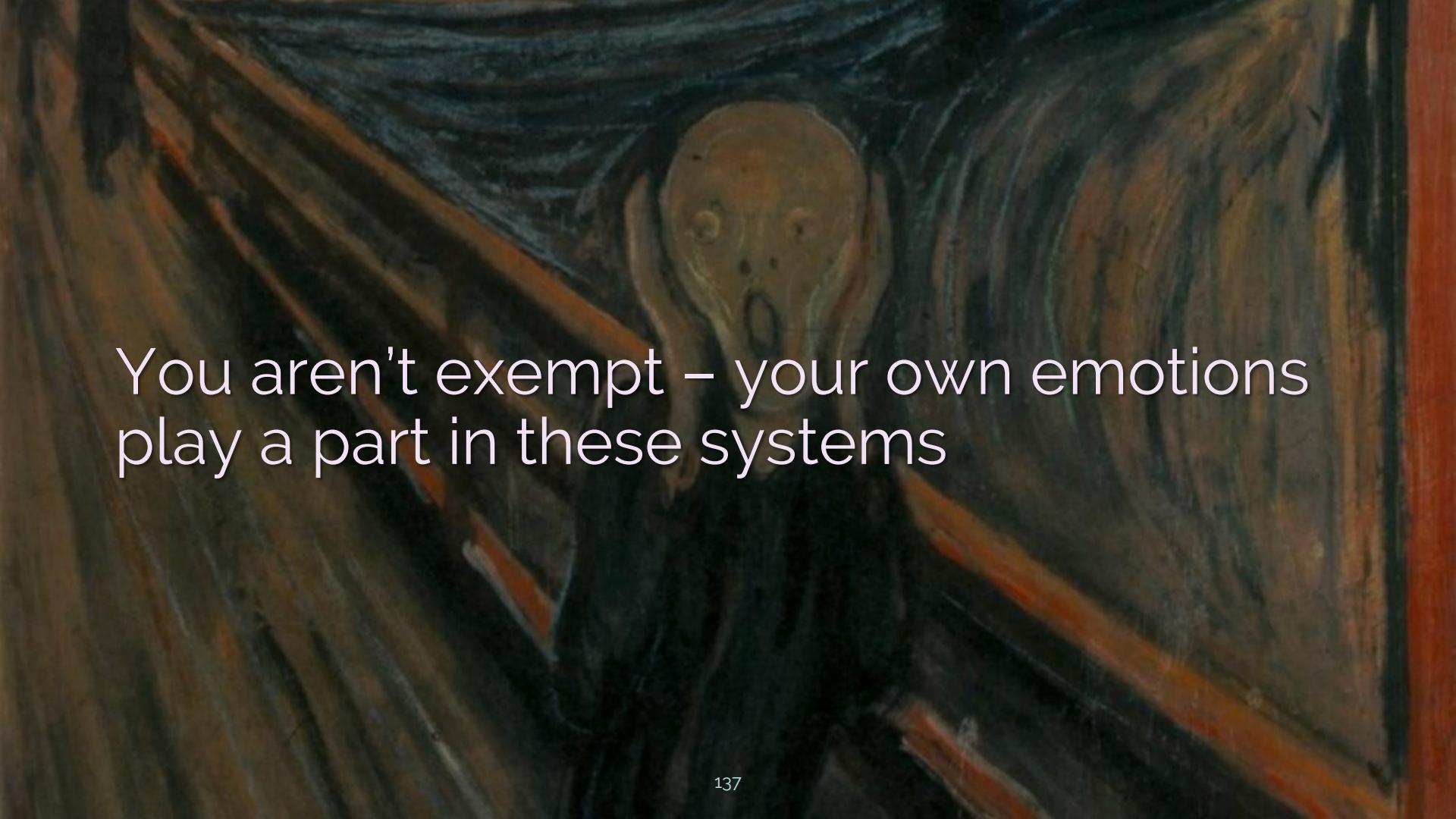


A dramatic painting of a figure falling from a cliff edge, symbolizing failure or a fall from grace. The figure is depicted in mid-fall, suspended by their arms, with a look of despair on their face. Their body is angled downwards, and their long, flowing hair and red cloak billow out behind them against a dark, turbulent background.

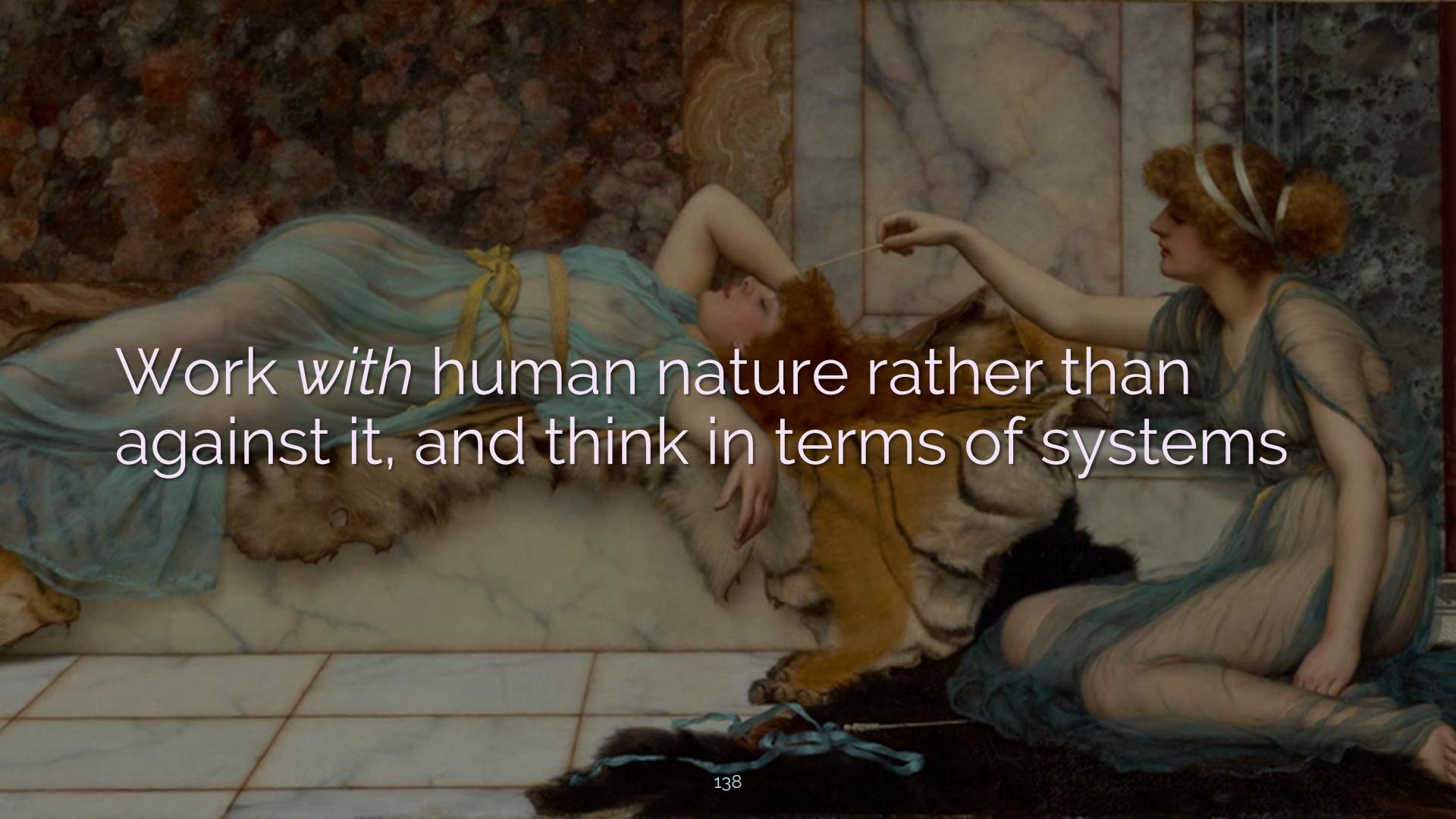
Discard the crutch of “human error” so
you can learn from failure

A dark, surreal painting by Frida Kahlo. In the center, a figure wearing a mask with a skull pattern is suspended from a ladder. Below them, a man lies on his back on a bed. The background features a landscape with mountains and a large sun or moon. The overall mood is somber and dreamlike.

Always consider the messiness of
systems, organizations, and minds



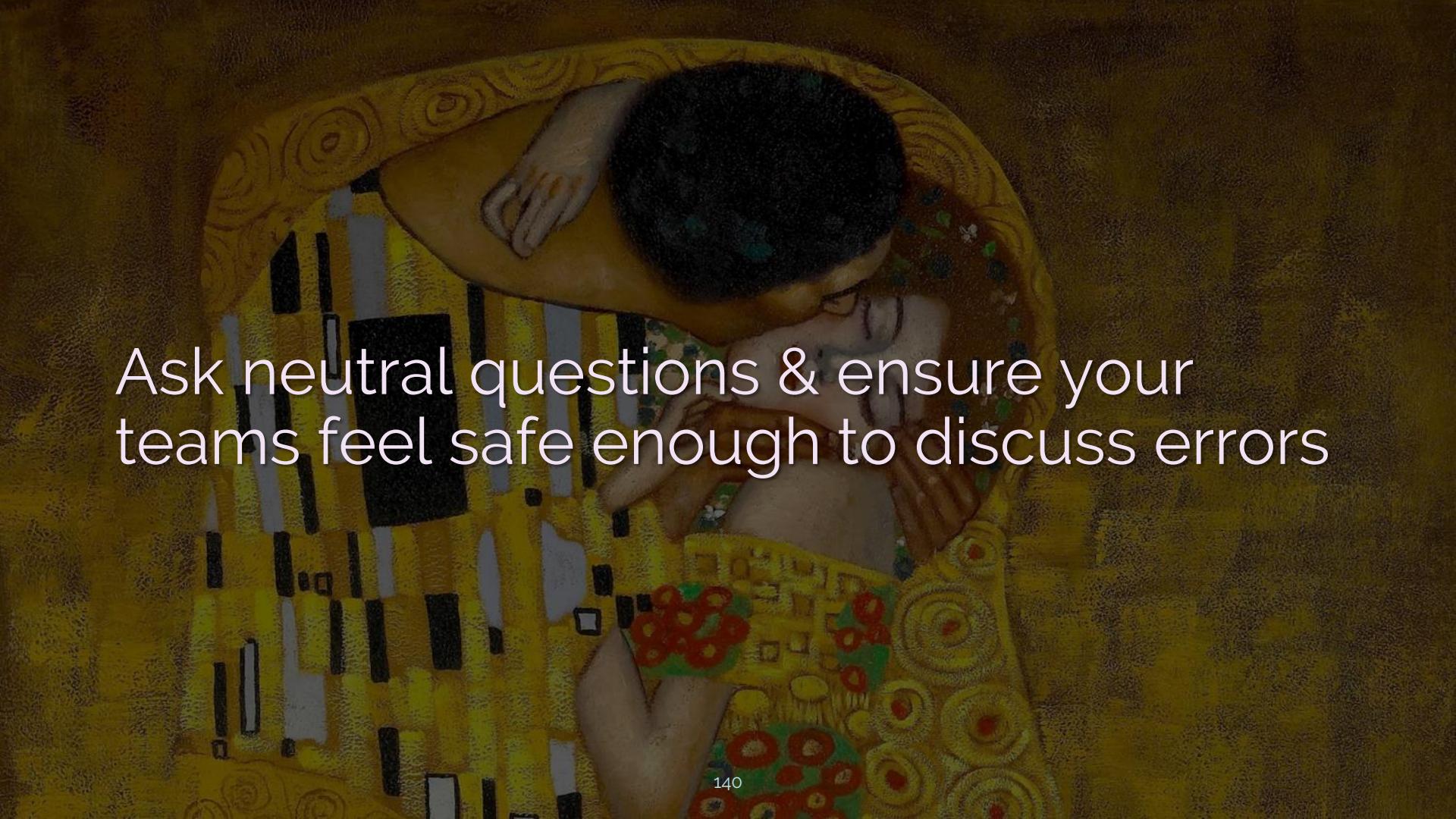
You aren't exempt – your own emotions
play a part in these systems

A painting depicting a scene from a classical or mythological narrative. Two women in flowing, light-colored robes are shown; one reclines on a bed, looking up, while the other sits beside her, holding a small object. A large, shaggy dog lies on the floor between them. The background features a wall with a floral pattern and a marble fireplace.

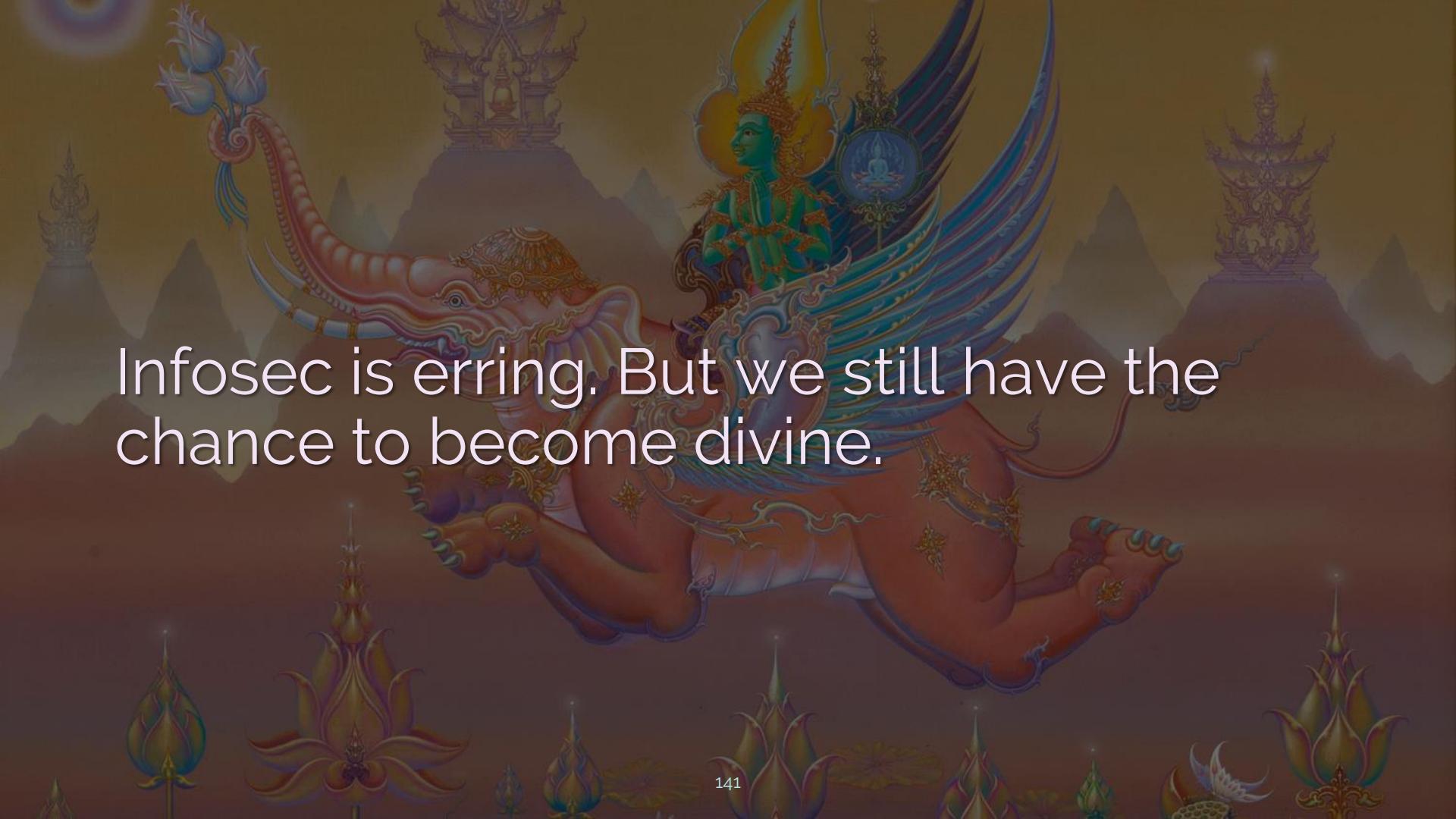
Work *with* human nature rather than
against it, and think in terms of systems



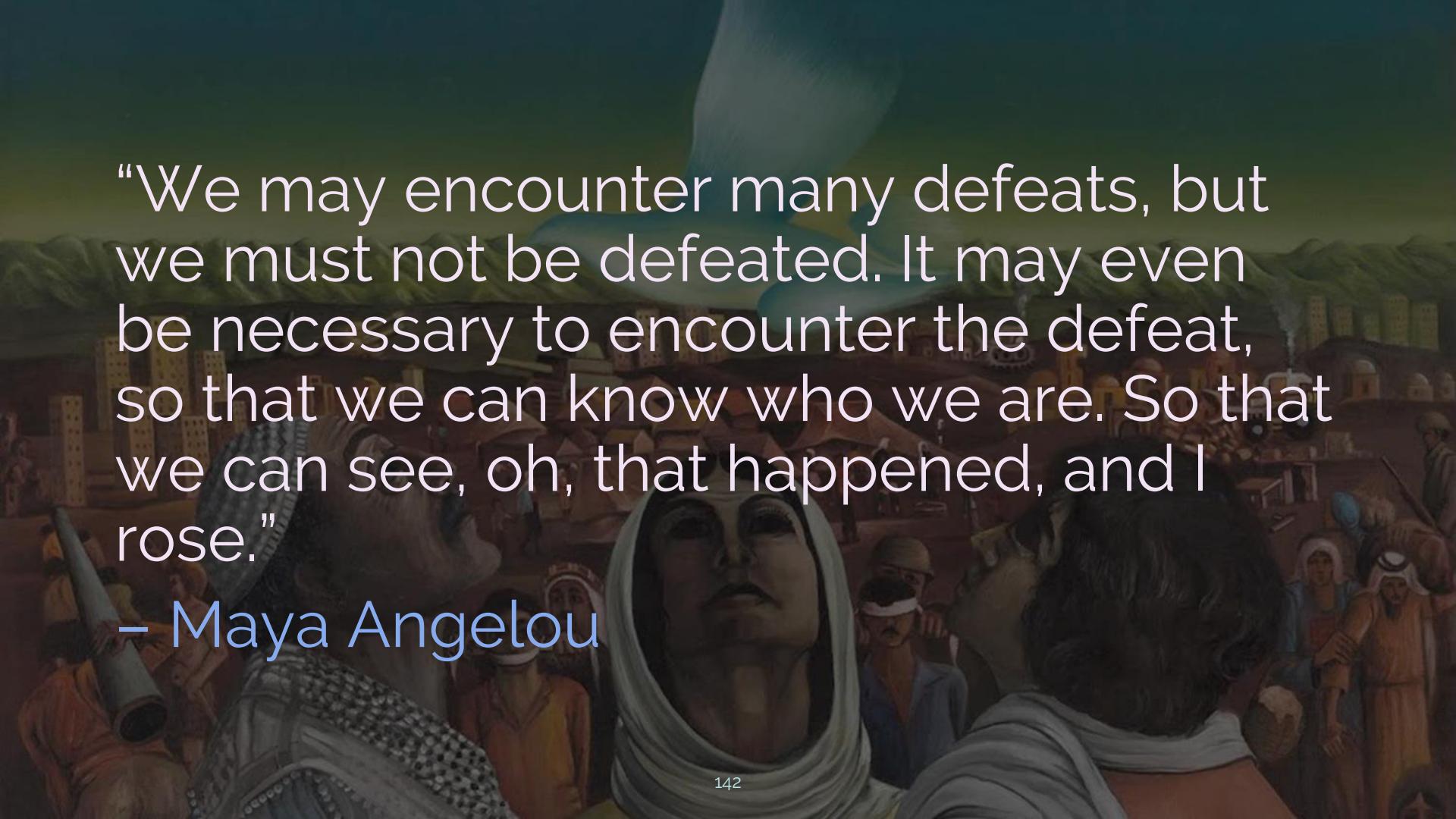
Leverage UX & chaos eng to improve
the context your systems engender



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



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



“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.