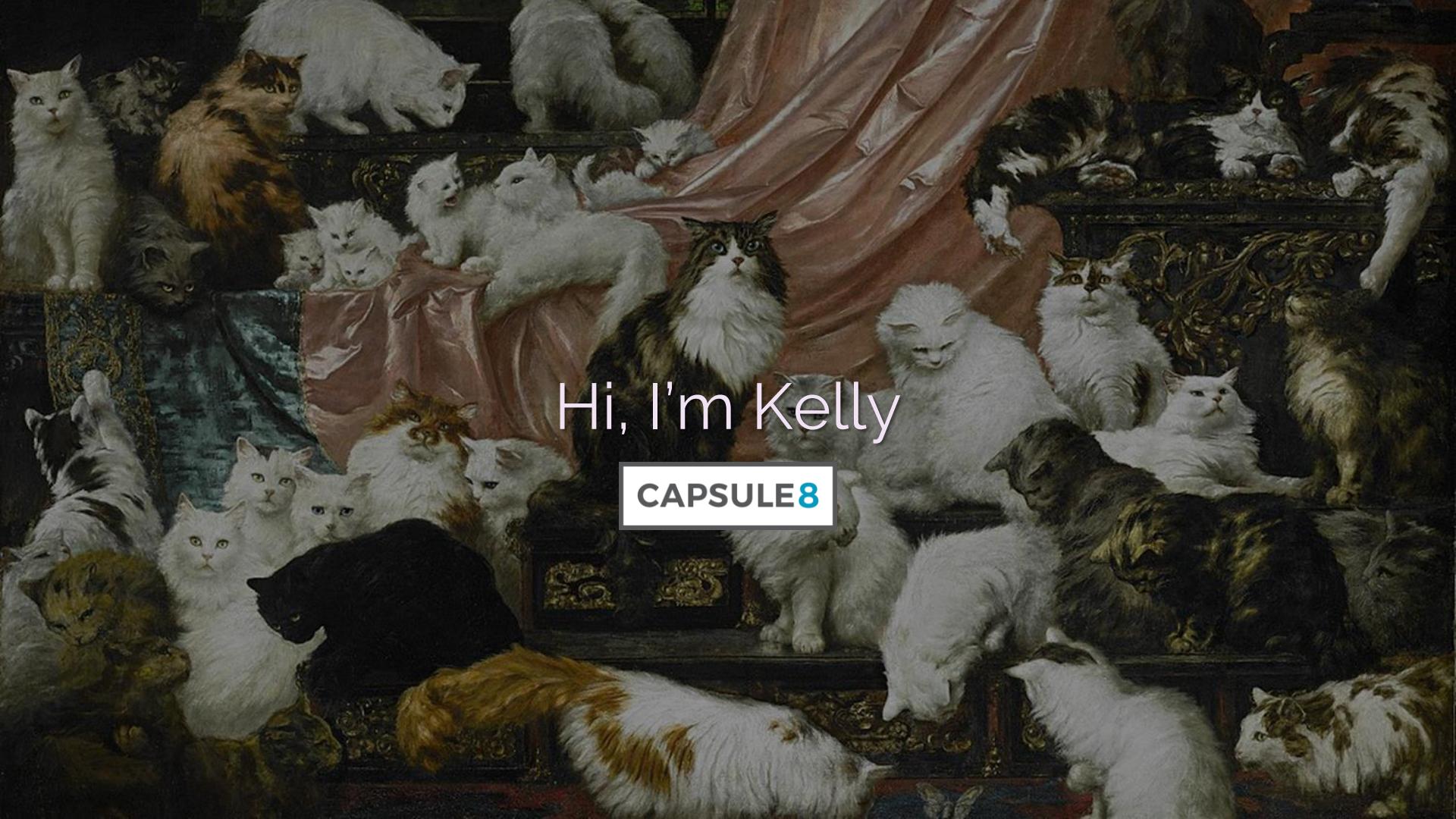


A painting of a man in a dark coat and hat standing on a rocky cliff edge, looking out over a vast, misty landscape.

To ERR IS HUMAN: The Complexity of Security Failures

Kelly Shortridge (@swagitda_)

DC Chaos Eng Meetup, April 2020

A painting depicting a room overflowing with numerous cats of various breeds and colors, including white, black, and calico. They are perched on furniture, curtains, and the floor, creating a dense and chaotic scene of feline activity.

Hi, I'm Kelly

CAPSULE8

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

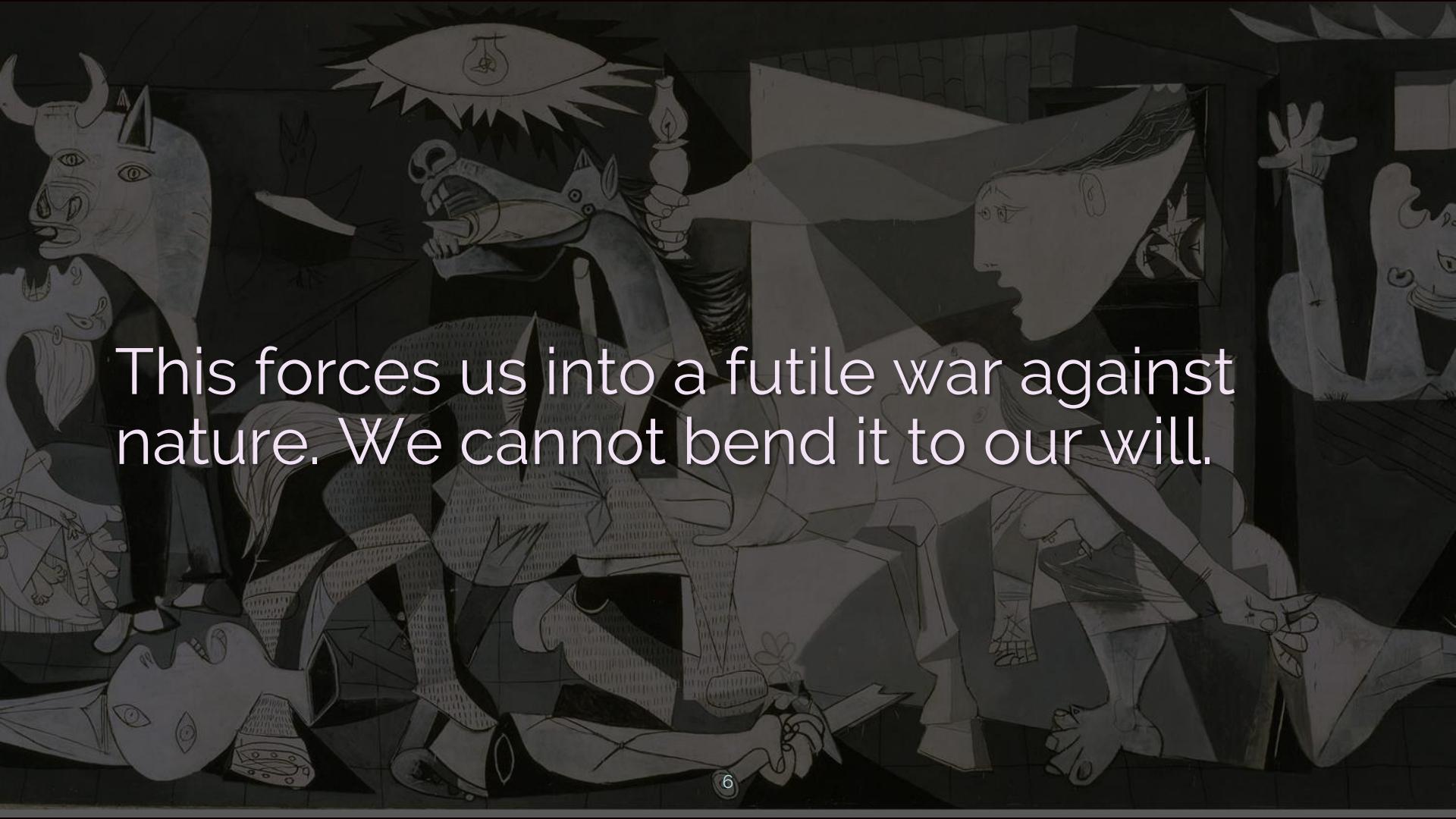


A dark, textured background featuring a close-up of a person's face and shoulders, possibly from a painting. The lighting is dramatic, highlighting the contours of the face and the texture of the clothing.

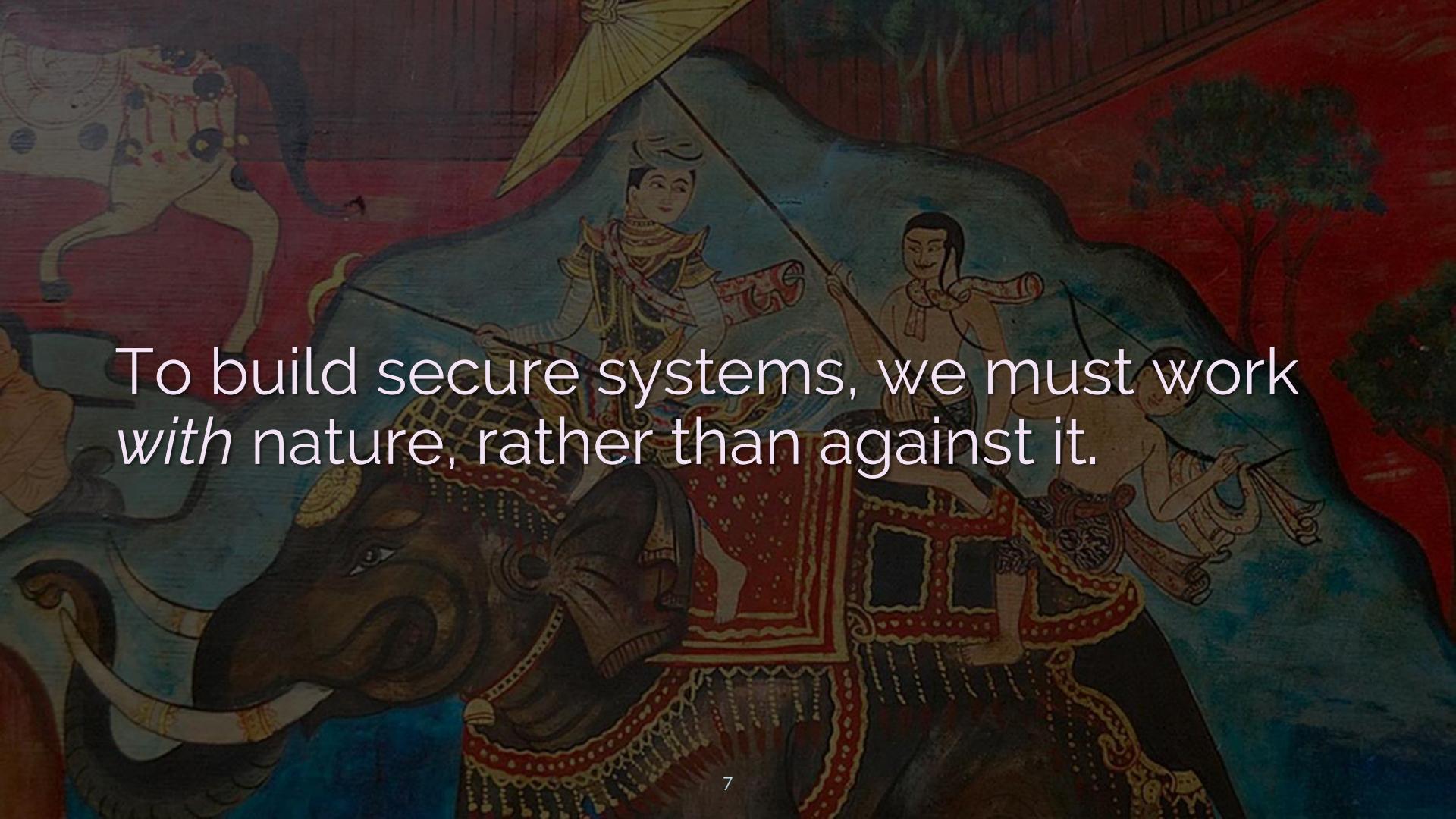
Humans make mistakes. It's part of our nature (it's mostly a feature, not a bug)

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 with a yellow sash 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.

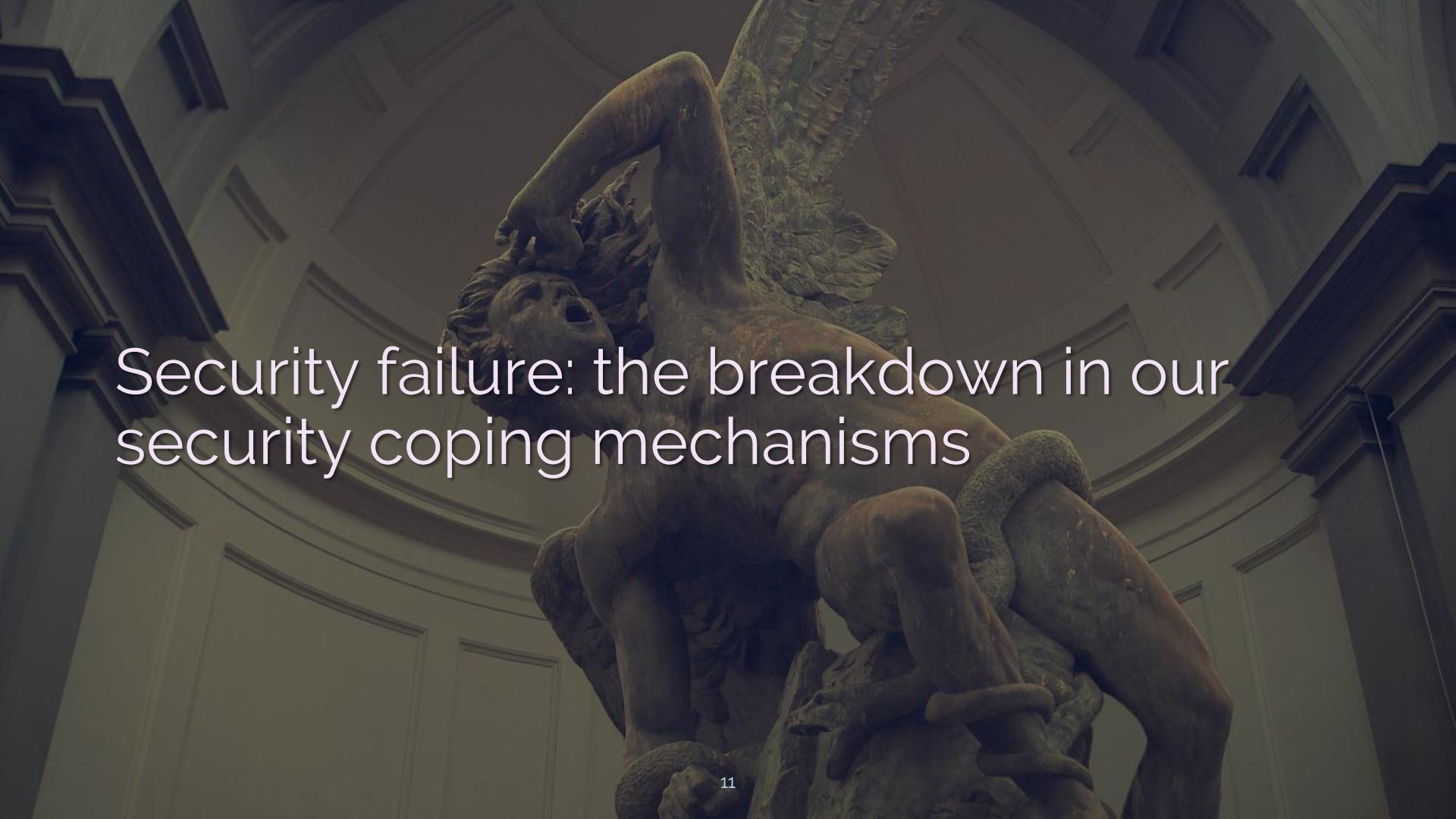
To build secure systems, we must work
with nature, rather than against it.

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.

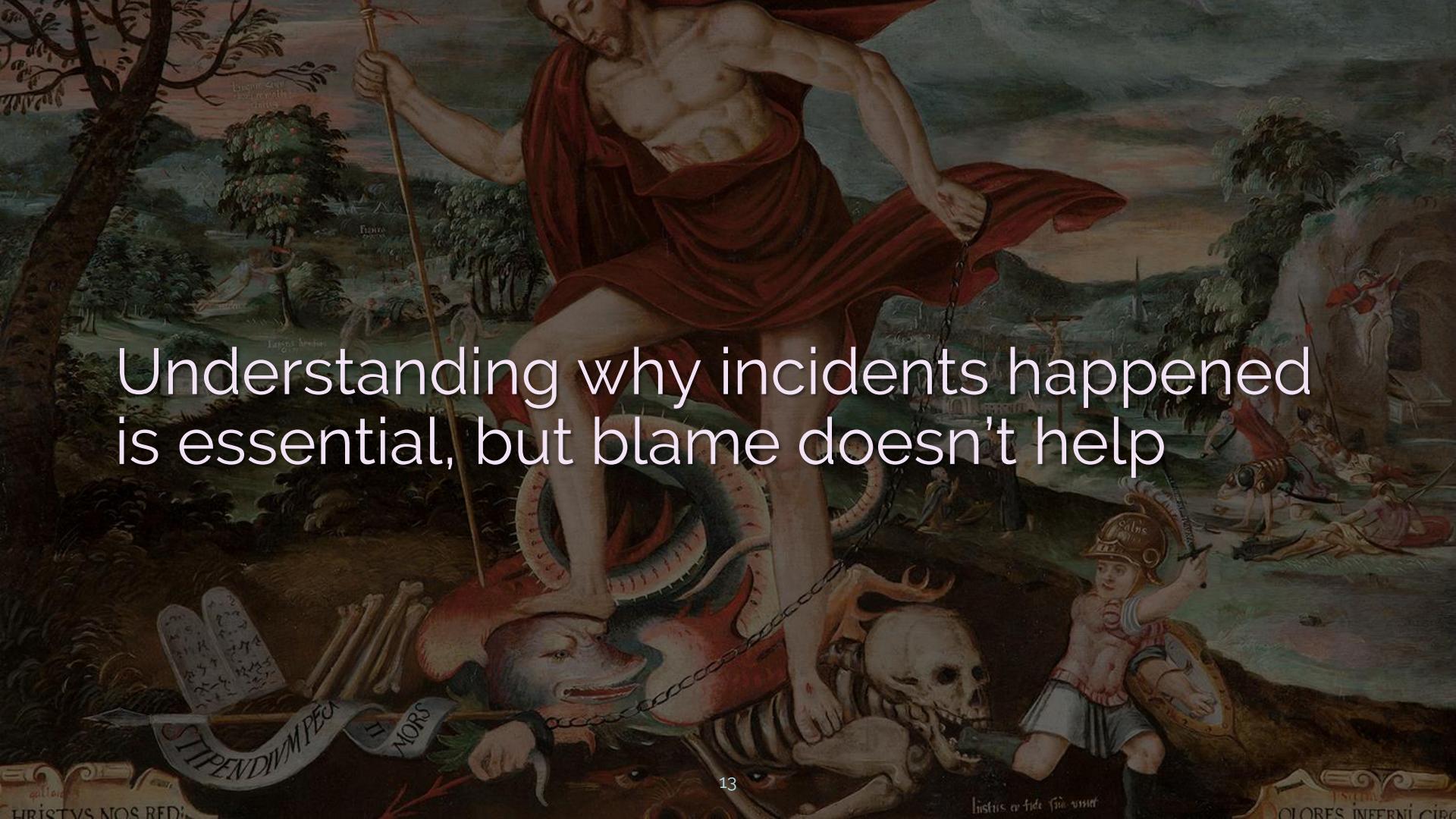
Clearing the Err

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



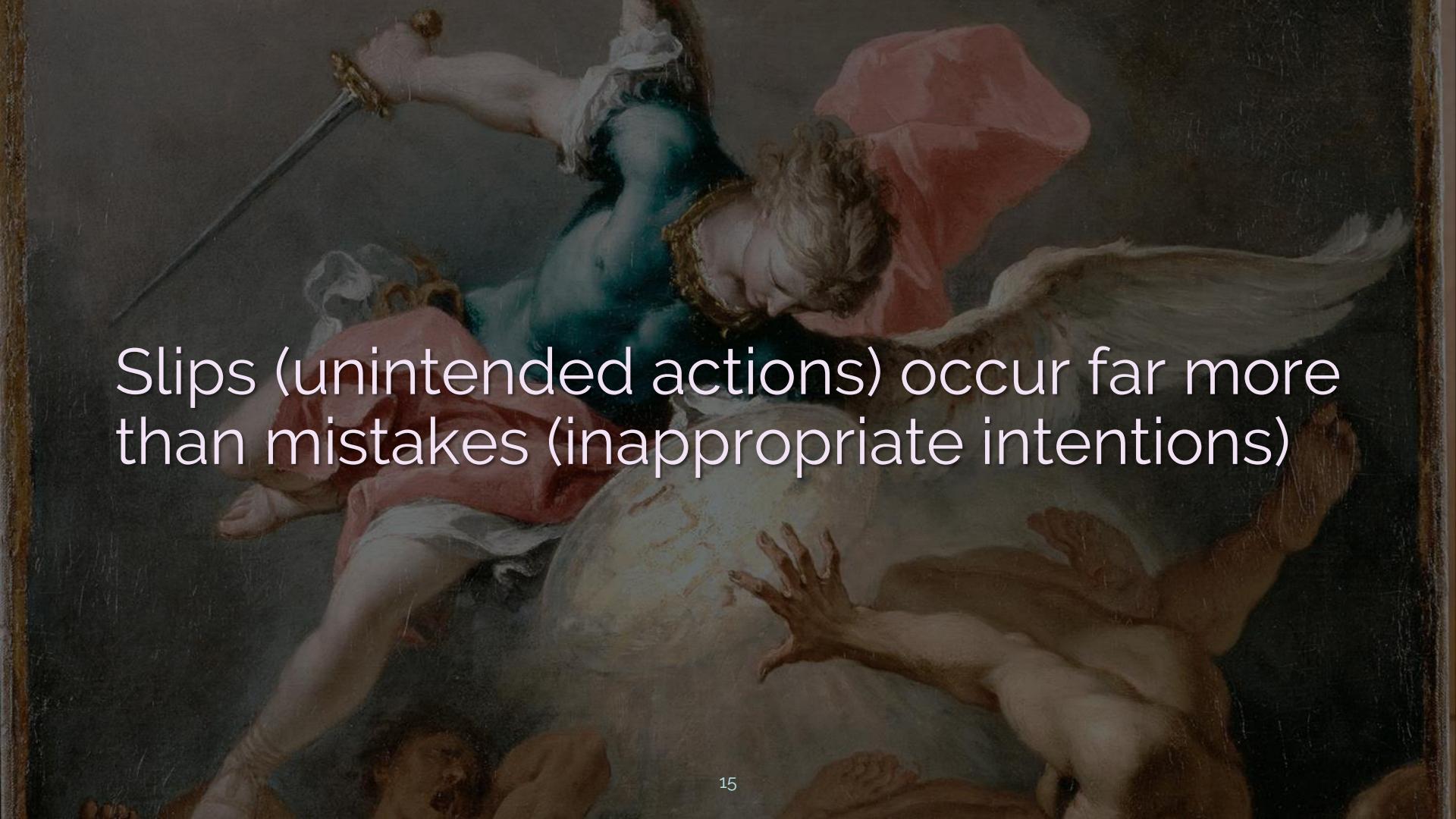
Security failure: the breakdown in our security coping mechanisms

“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)

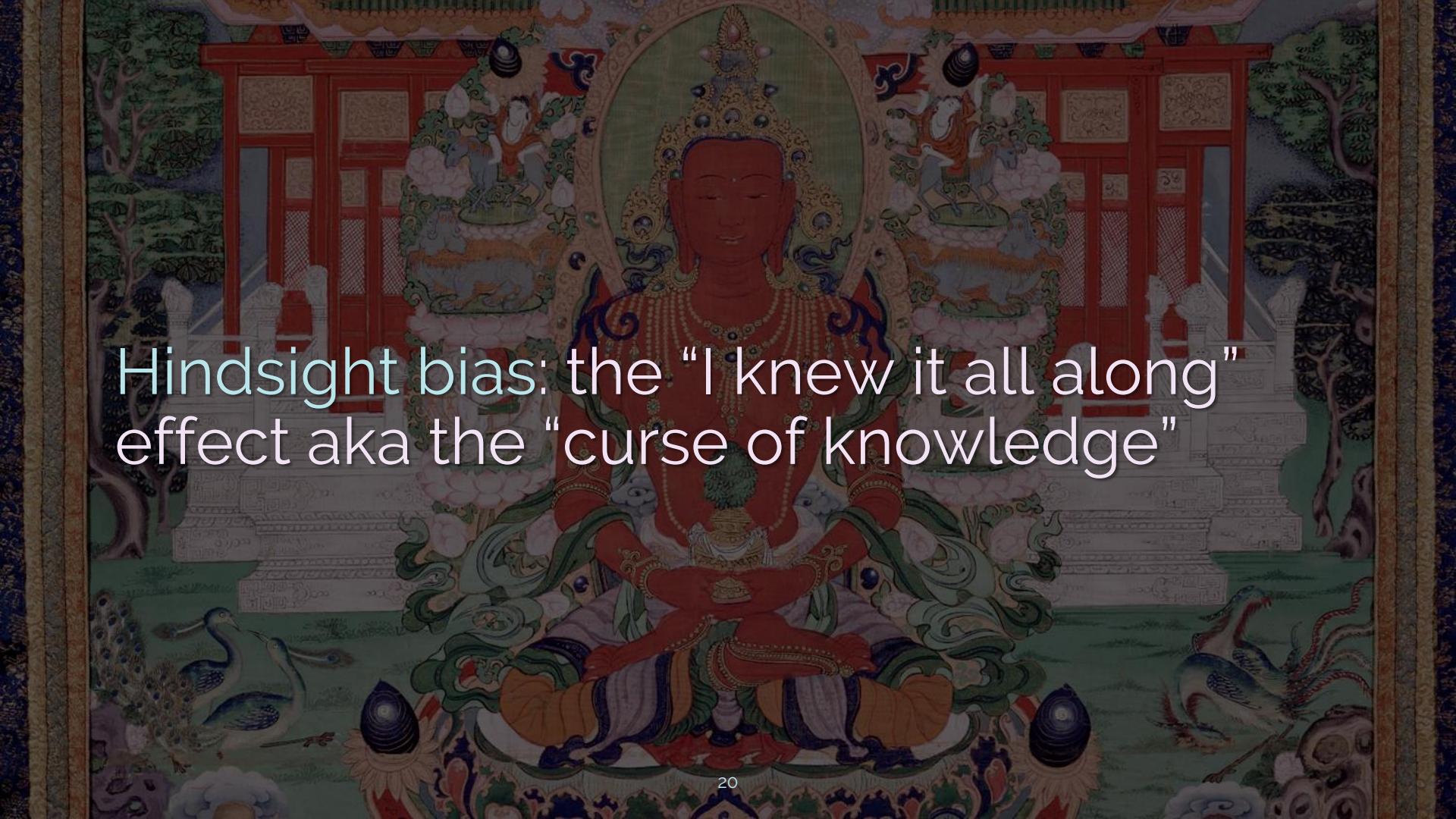
The term “human error” is less grounded to reality than we believe...

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.

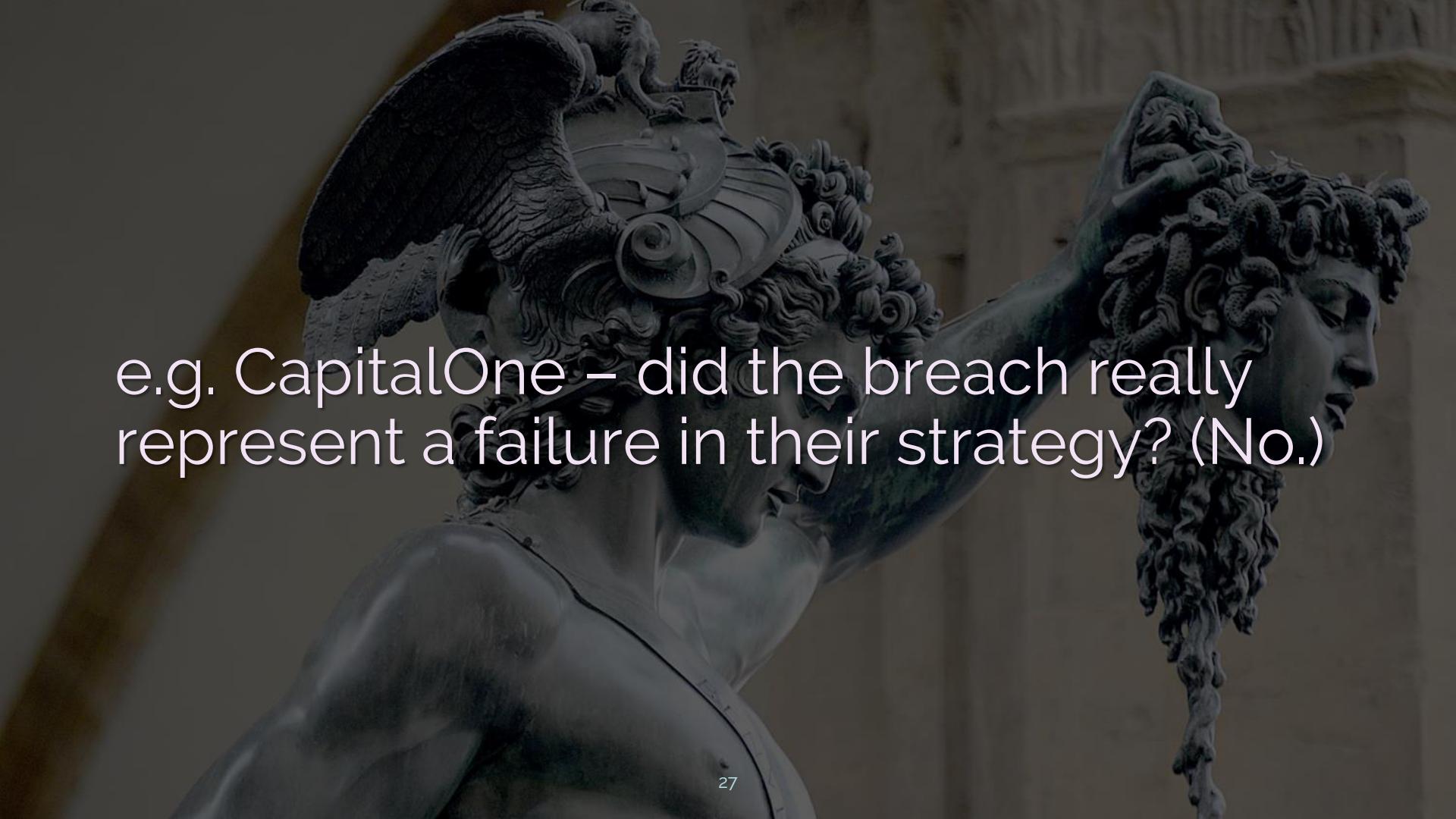
Outcome bias: judging a decision based
on its eventual outcome

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 is sitting on the keys of the harpsichord. The background shows a room with a tiled floor and some foliage.

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...

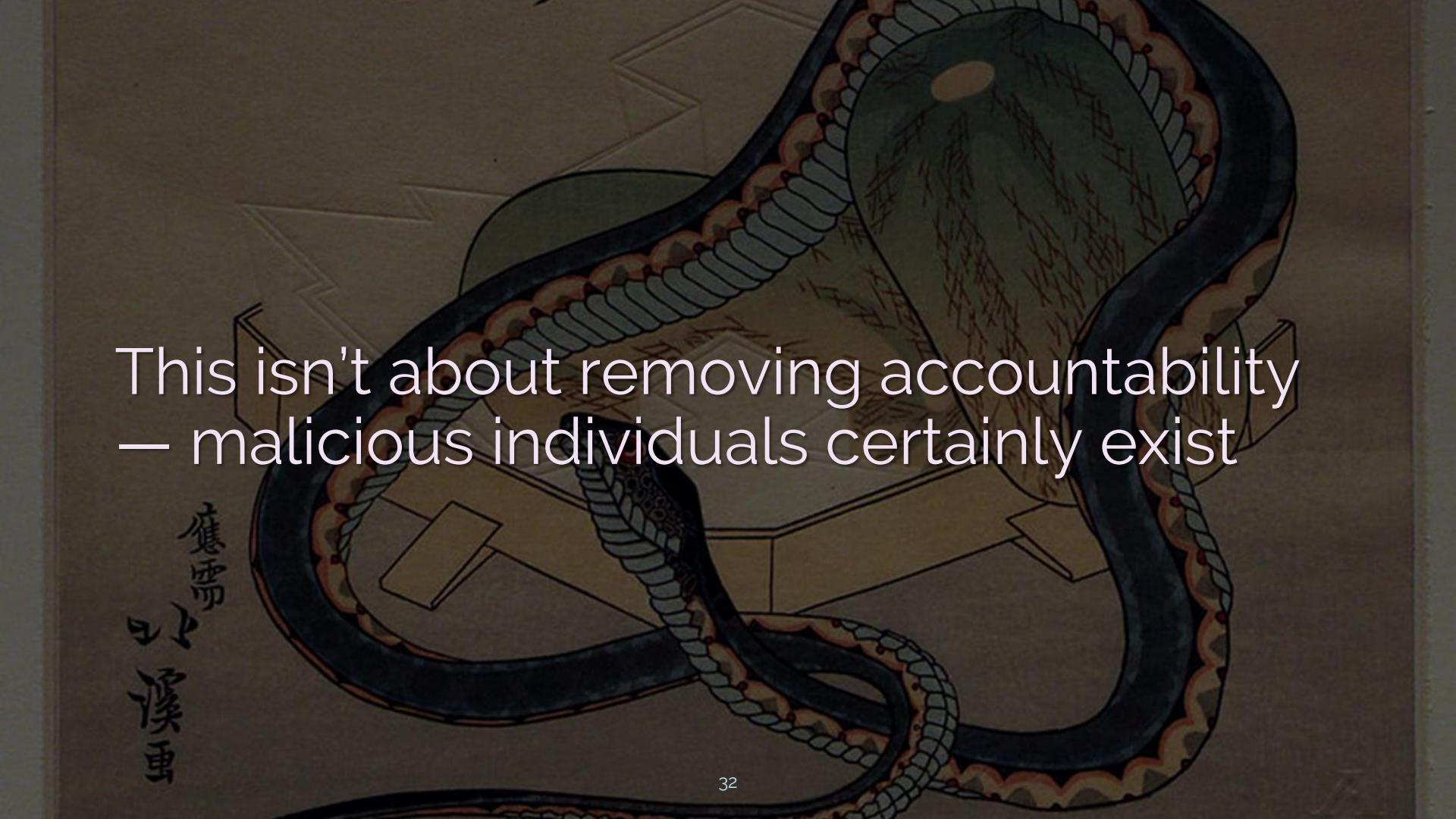
A dark, somber painting depicting a man in a suit holding a bloody hand, appearing distressed or in pain. Another figure is visible in the foreground, seemingly unconscious or deceased. The scene conveys a sense of trauma and despair.

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

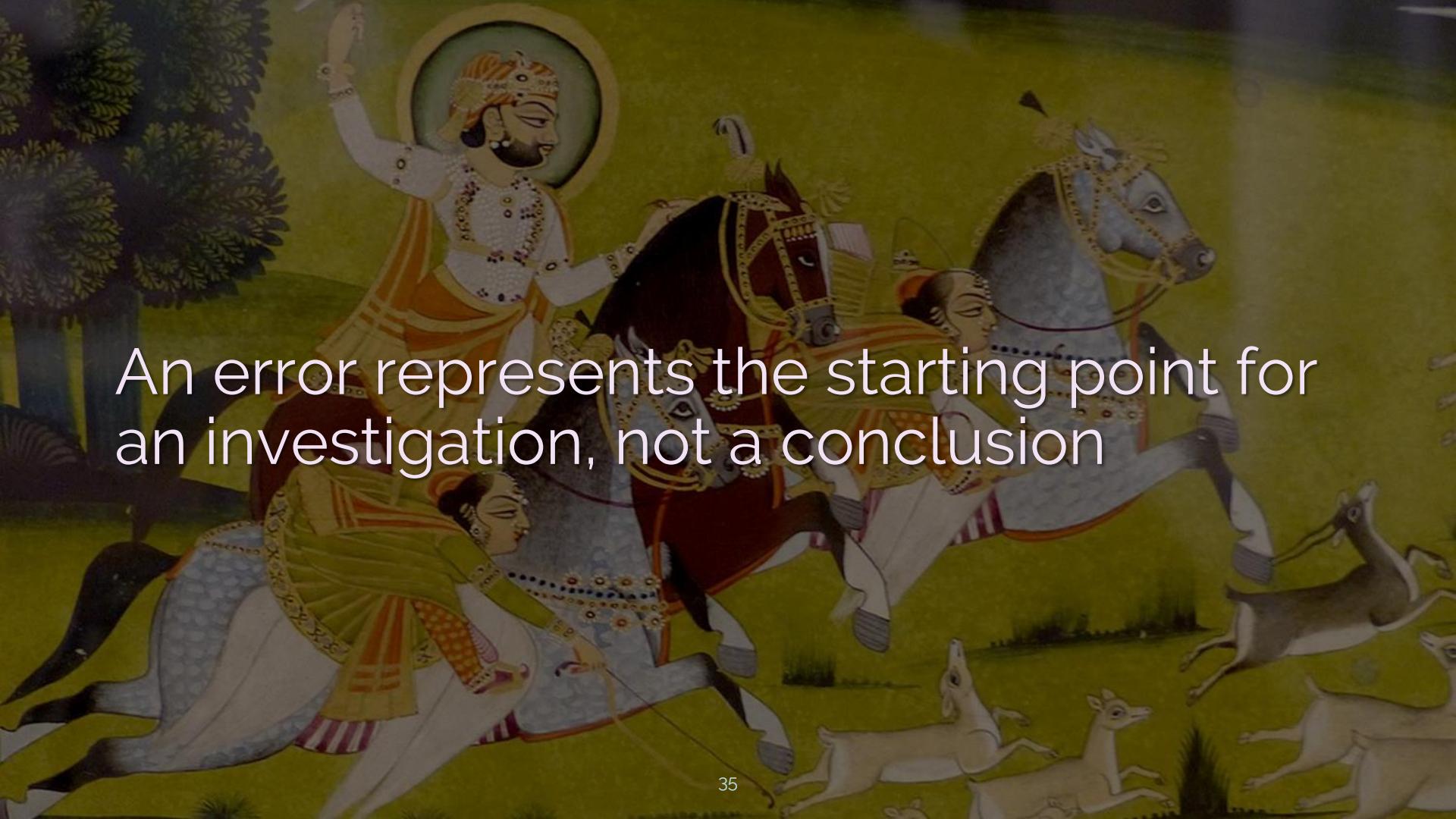


This isn't about removing accountability
– malicious individuals certainly exist

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?”

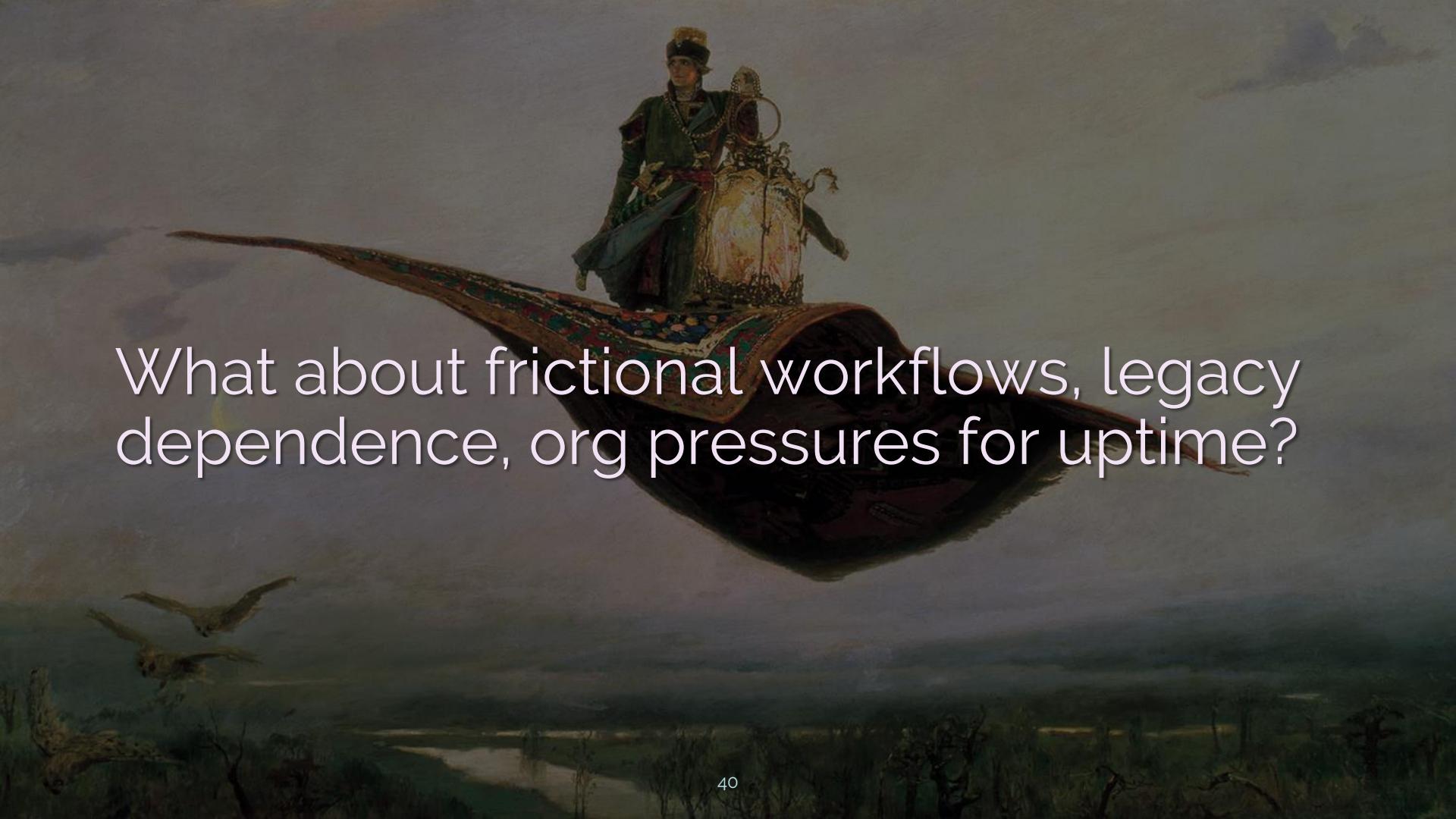
“Why did clicking a link lead to pwnage?”

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.

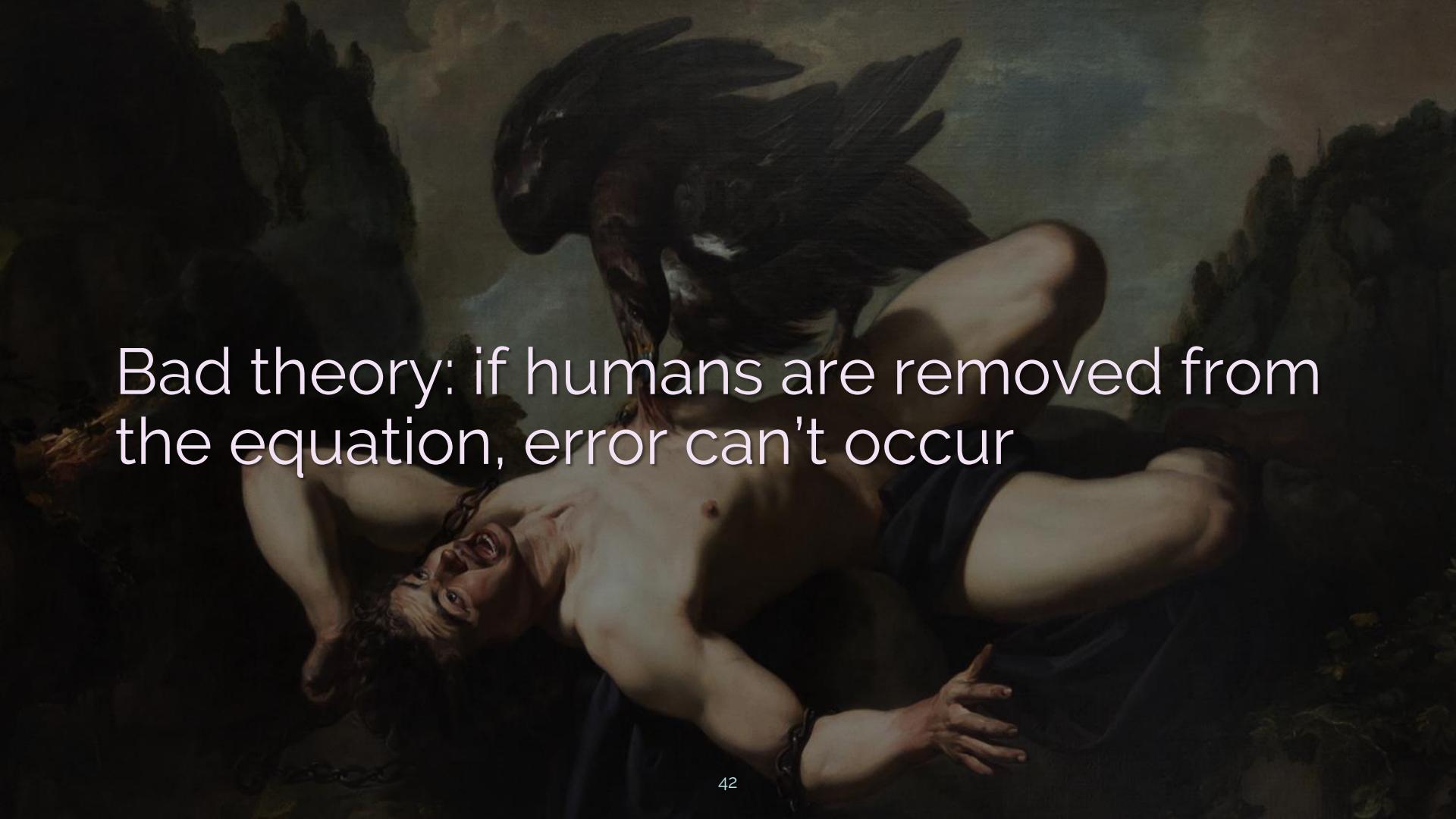
e.g. training devs to “care about security”
completely misses the underlying issue

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, sitting on a large, ornate, flying carpet. The carpet is decorated with intricate patterns and has long, flowing ends. The man is looking towards the right. Below him is a landscape with rolling hills and a few birds in flight. The overall atmosphere is mysterious and fantastical.

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 field with mountains in the background.

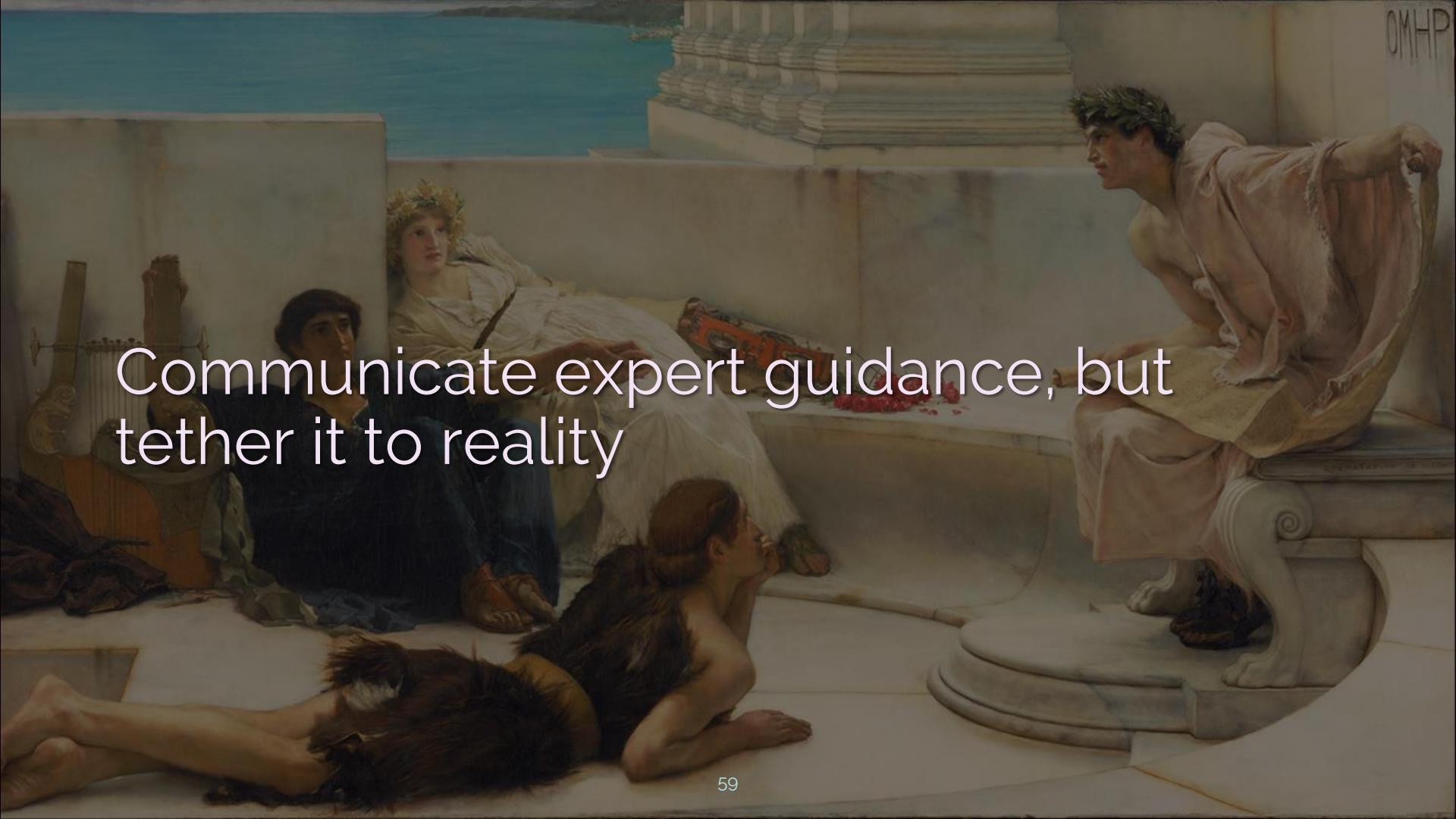
Discipline doesn't actually fix the "policy violation" cause (but it does scapegoat)

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, emphasizing the intensity of the moment.

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 lies on the floor, looking up at a man who is kneeling on a large, ornate column. The kneeling man is holding a scroll and appears to be reading or explaining something to the other figure. In the background, a woman in a white robe with a laurel wreath on her head is reclining on a bed, looking towards the scene. Another figure is visible in the shadows behind the reclining woman. The setting is a grand, light-colored room with a balcony overlooking a body of water. The overall mood is one of mentorship and the transmission of knowledge.

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



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



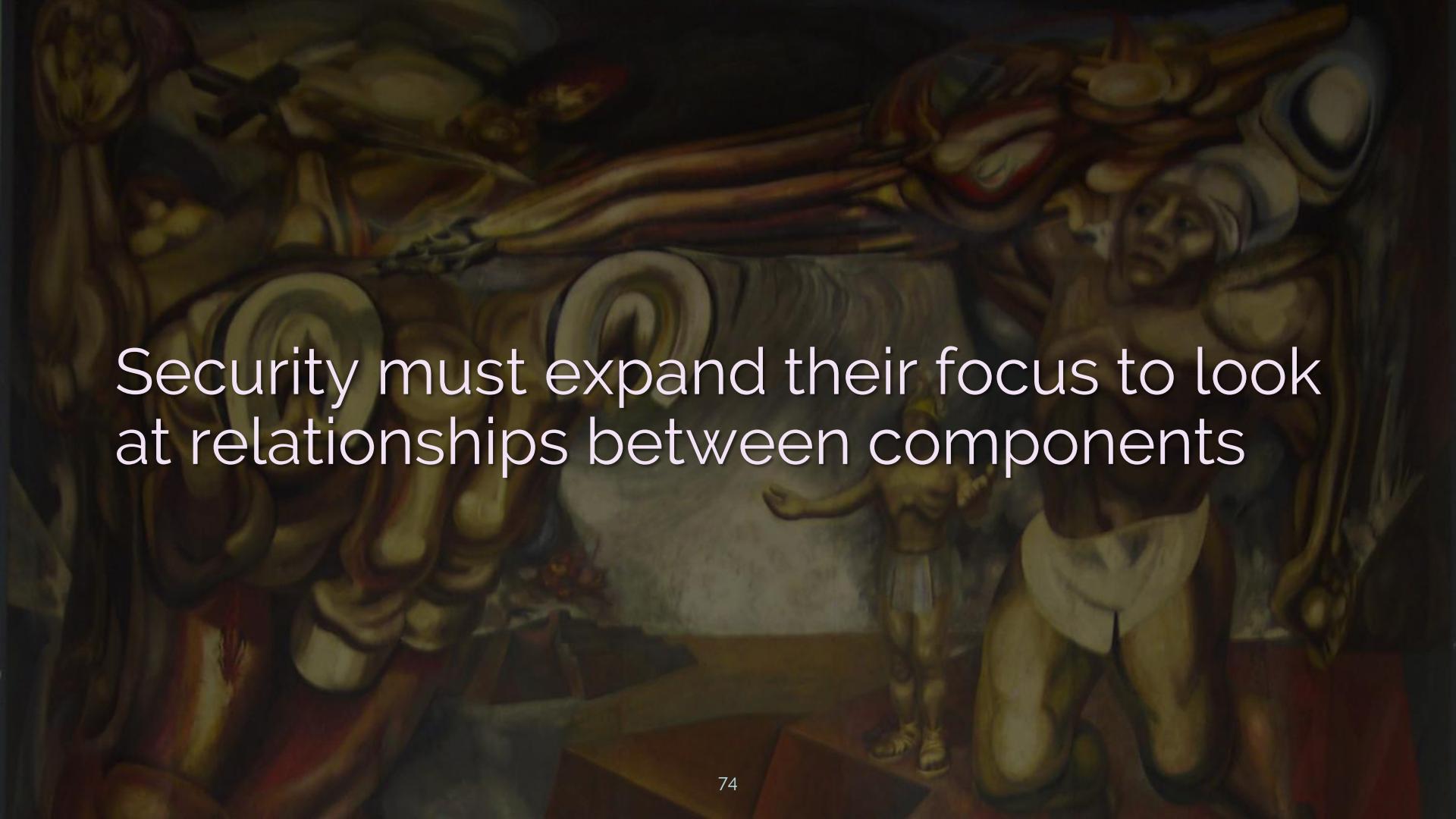
Infosec will progress when we ensure
the easy way is the secure way

1. System perspective
2. A spoiler alert...

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

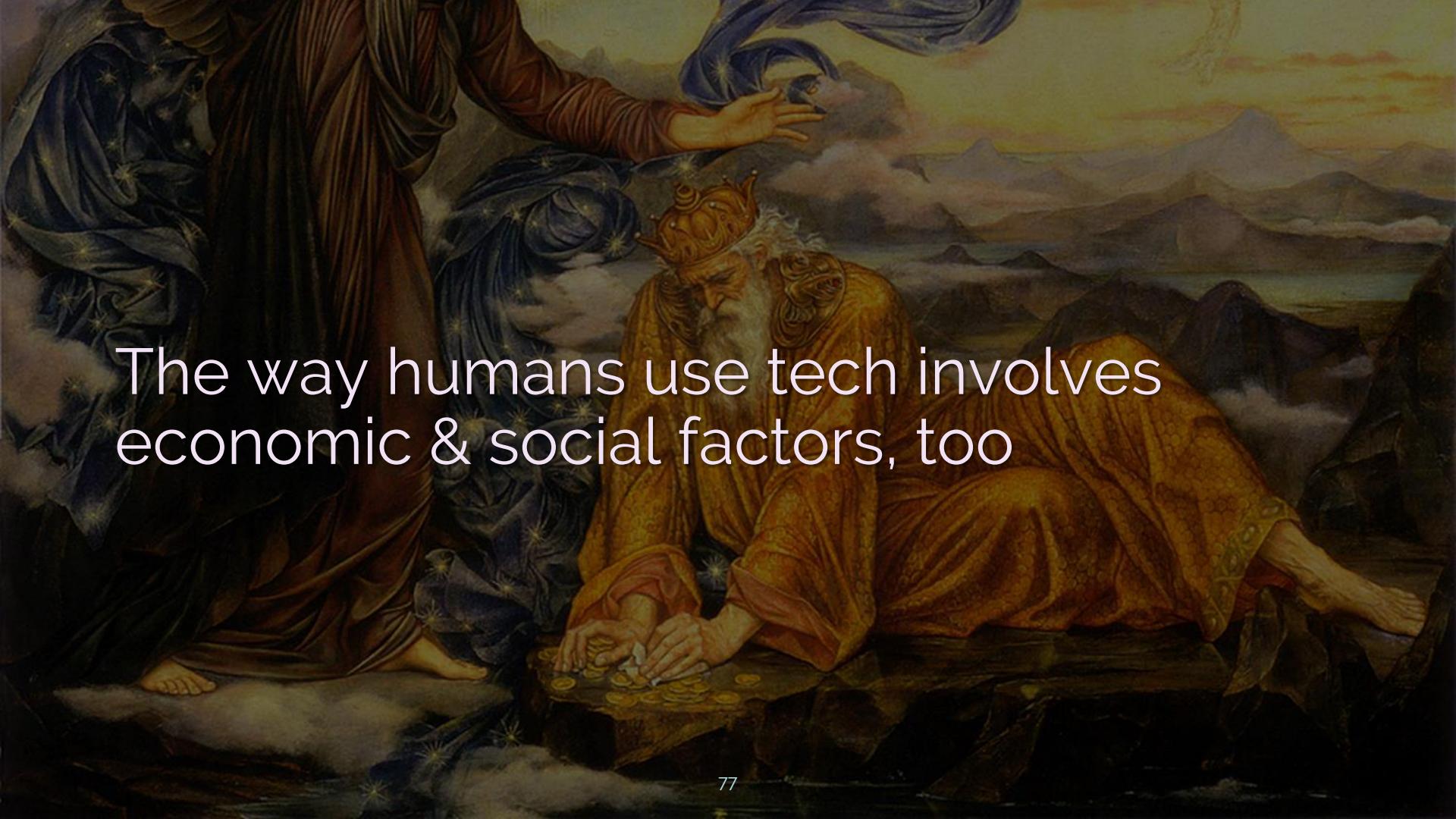
The background of the slide is a dark, abstract painting. It features a central figure with multiple heads and arms, rendered in shades of brown, tan, and grey. The figure appears to be in a dynamic, perhaps dancing or performing pose. Behind the figure, there are swirling, organic shapes in various colors, including yellows, reds, and blues, creating a sense of movement and complexity.

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”

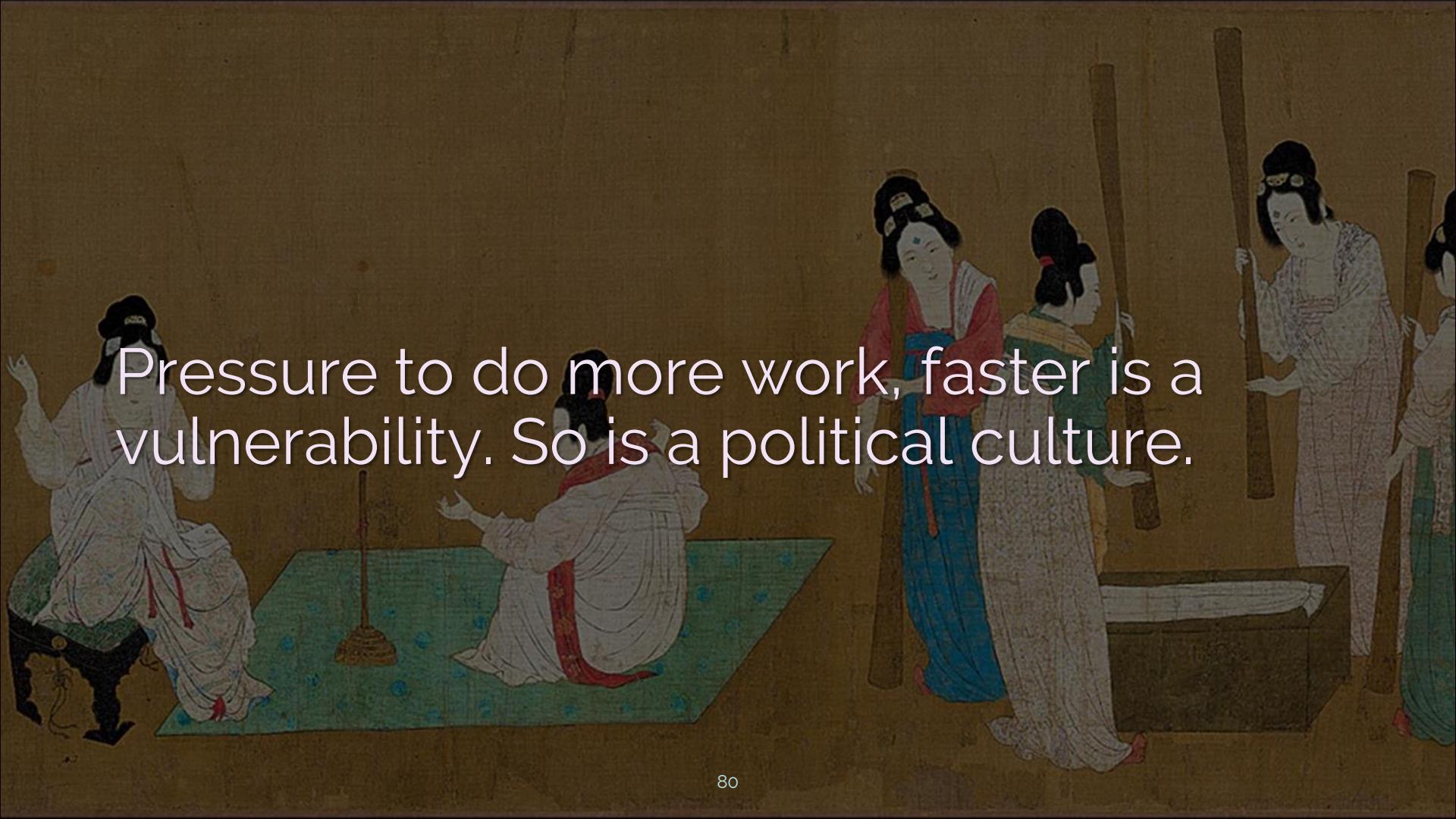
– Nancy Leveson

A painting depicting a king with a crown and a golden robe, 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 towards the hand.

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

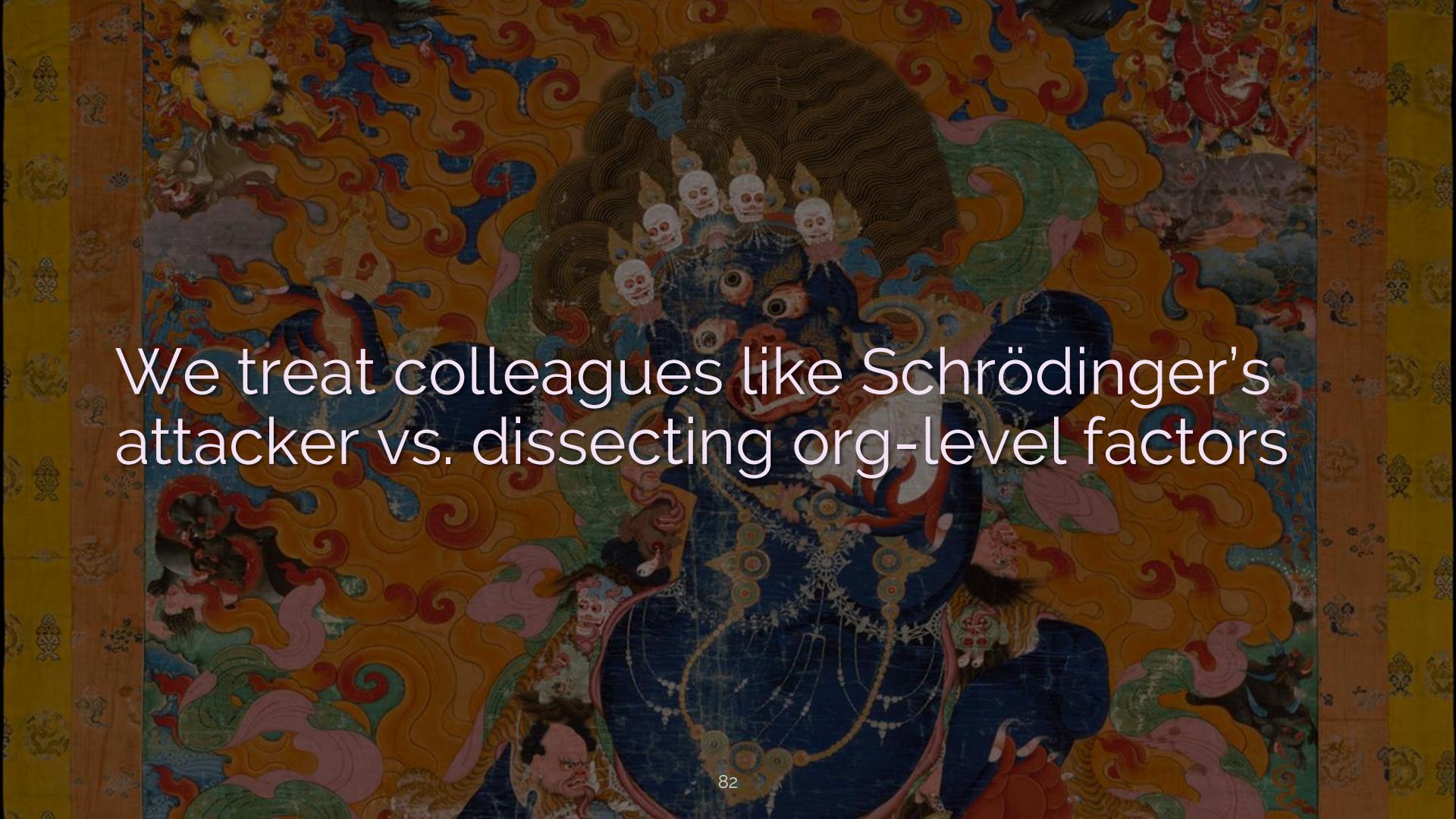
Economic factors: revenue & profit goals,
compensation schemes, budgeting, etc.

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



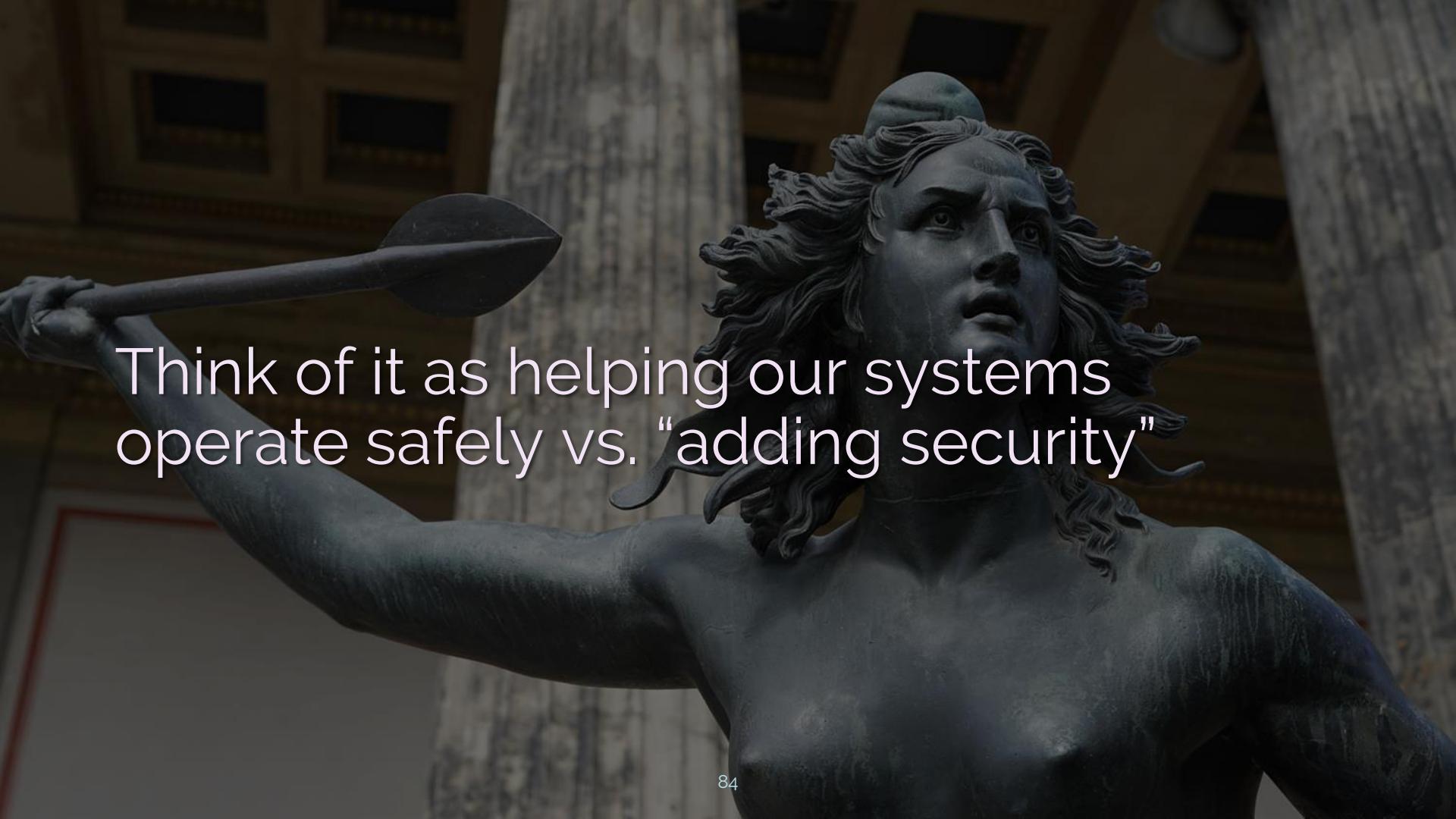
Pressure to do more work, faster is a vulnerability. So is a political culture.

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

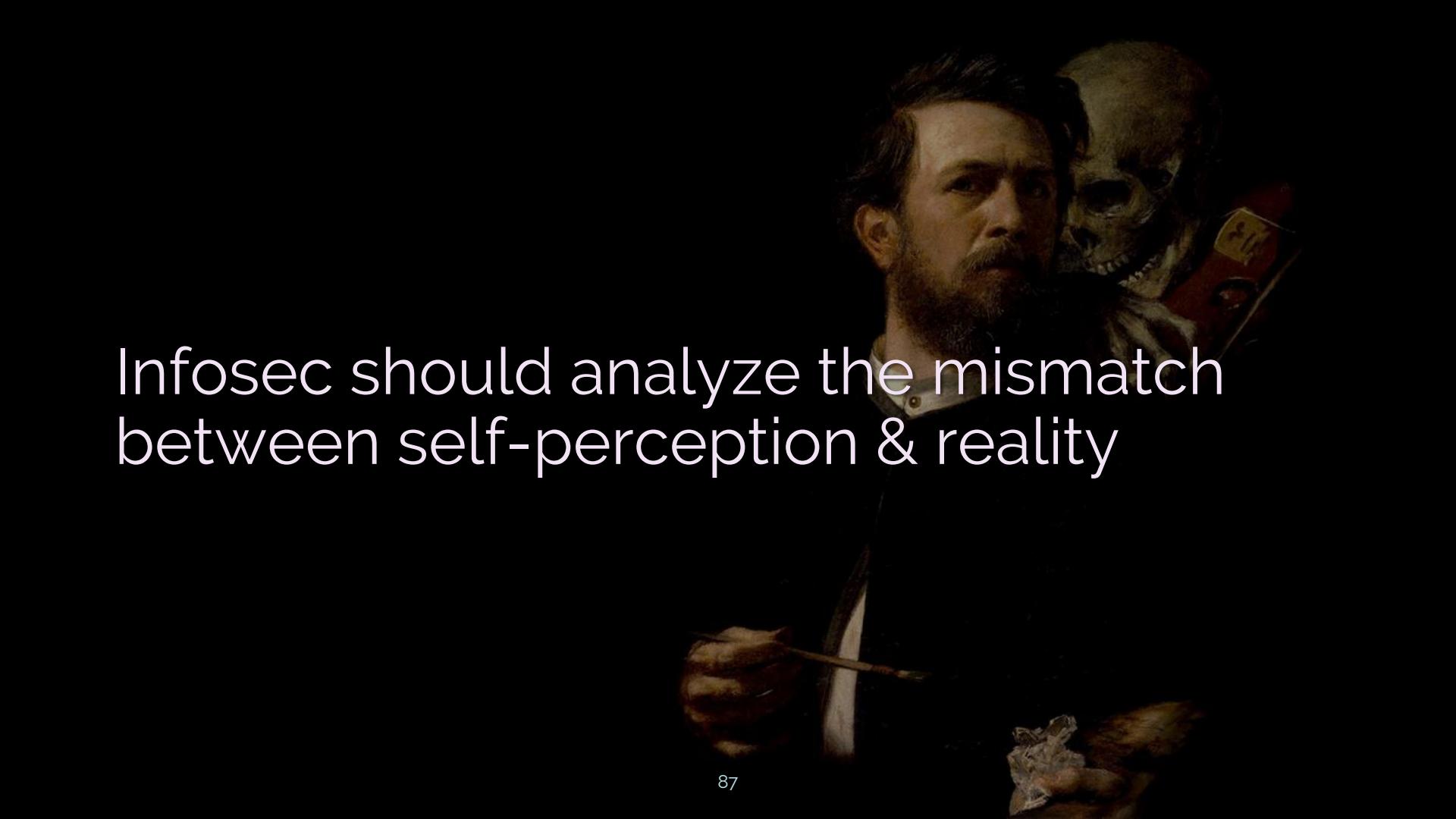
**Security is something a system does,
not something a system has.**



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, moody painting of a man with a beard and mustache, looking slightly to the right. He is holding a skull in his left hand and a palette with a brush in his right hand, painting the skull. The lighting is dramatic, highlighting his face and the skull against a dark background.

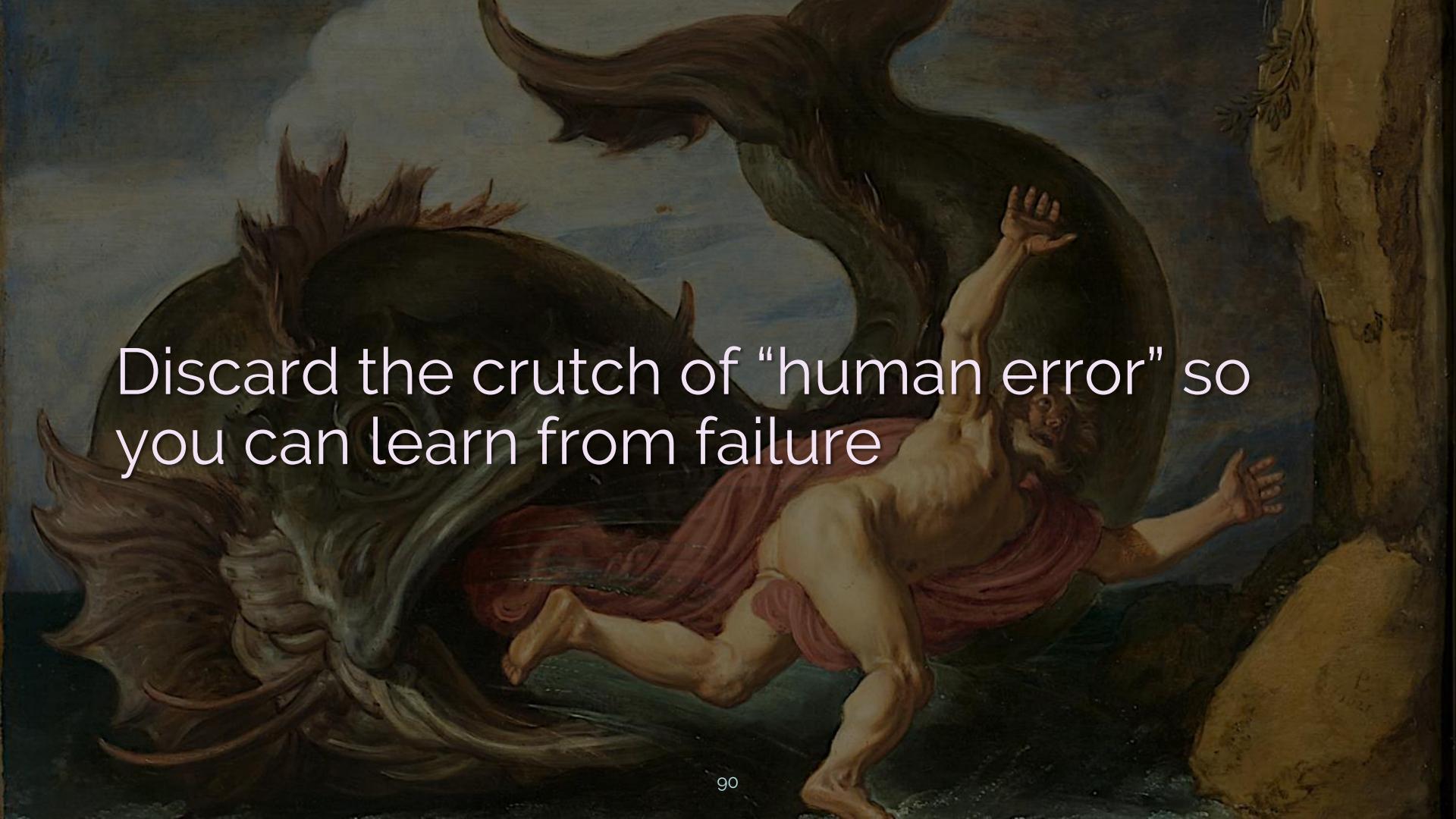
Infosec should analyze the mismatch
between self-perception & reality

The background of this slide is a reproduction of Hieronymus Bosch's famous triptych, "The Garden of Earthly Delights". The central panel depicts a chaotic scene of human folly and vice. In the foreground, figures are shown in various states of debauchery, including a man being impaled on a spike and others engaged in sexual activity. A large, stylized eye dominates the center, symbolizing divine observation. The upper panels show more scenes of human depravity, including a city where people are working on a massive saw and another where figures are being tortured. The overall atmosphere is one of moral judgment and the consequences of earthly sins.

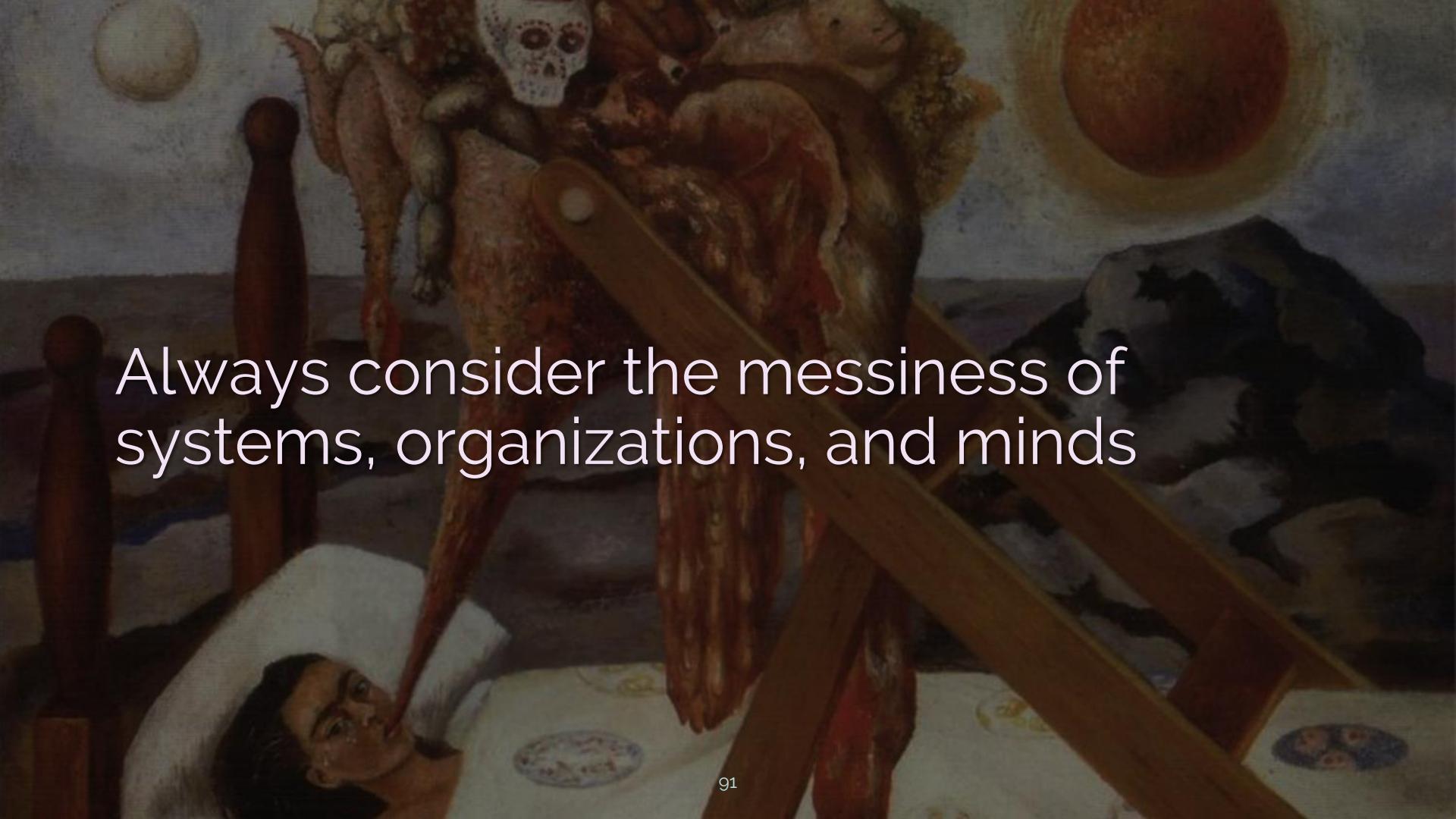
Spoiler alert: security chaos
engineering

In Conclusion

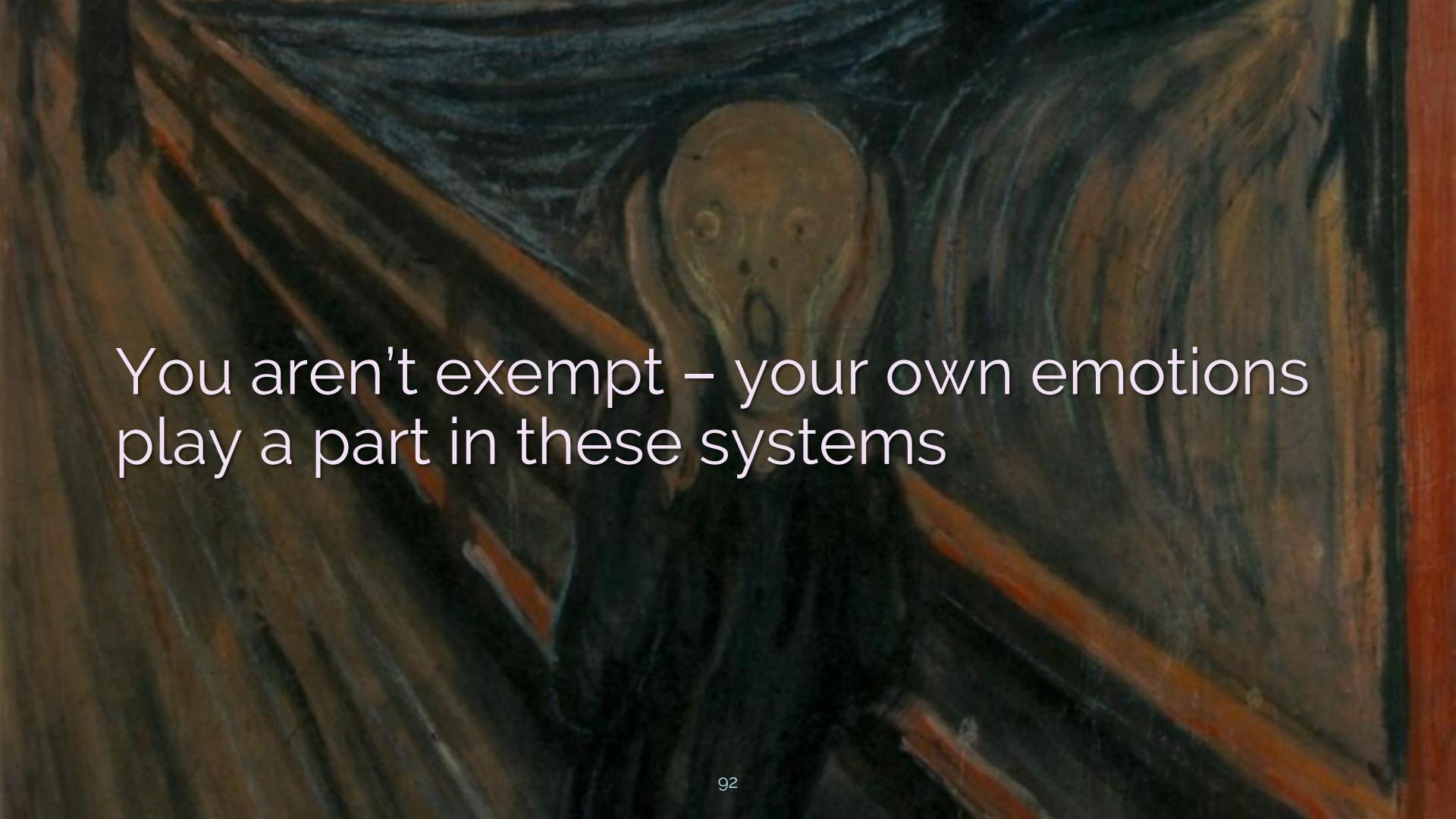


A dramatic painting of a figure falling from a cliff edge, symbolizing failure or a fall from grace. The figure is depicted in mid-fall, suspended by their arms, with long dark hair and a red cloth. The background shows a rocky cliff and a cloudy sky.

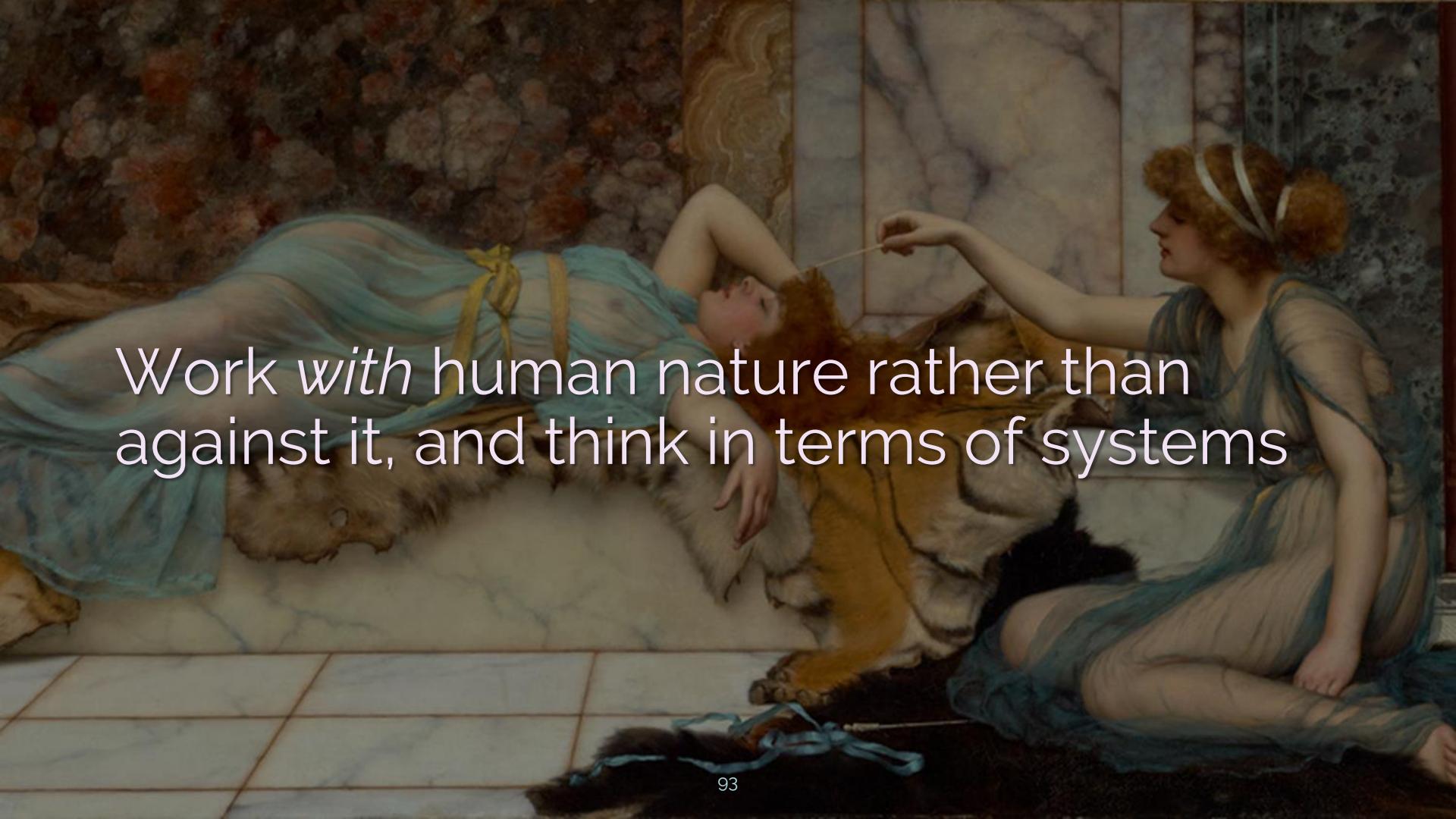
Discard the crutch of “human error” so
you can learn from failure

A dark, surreal painting by Frida Kahlo. In the center, a skull with a colorful, patterned face is perched on a ladder. The ladder leans against a large, dark, craggy mountain. At the base of the ladder, a figure's head is visible, looking up. The background is filled with soft, glowing light from celestial bodies like the sun and moon, and small, colorful circular motifs resembling flowers or coins are scattered on the ground.

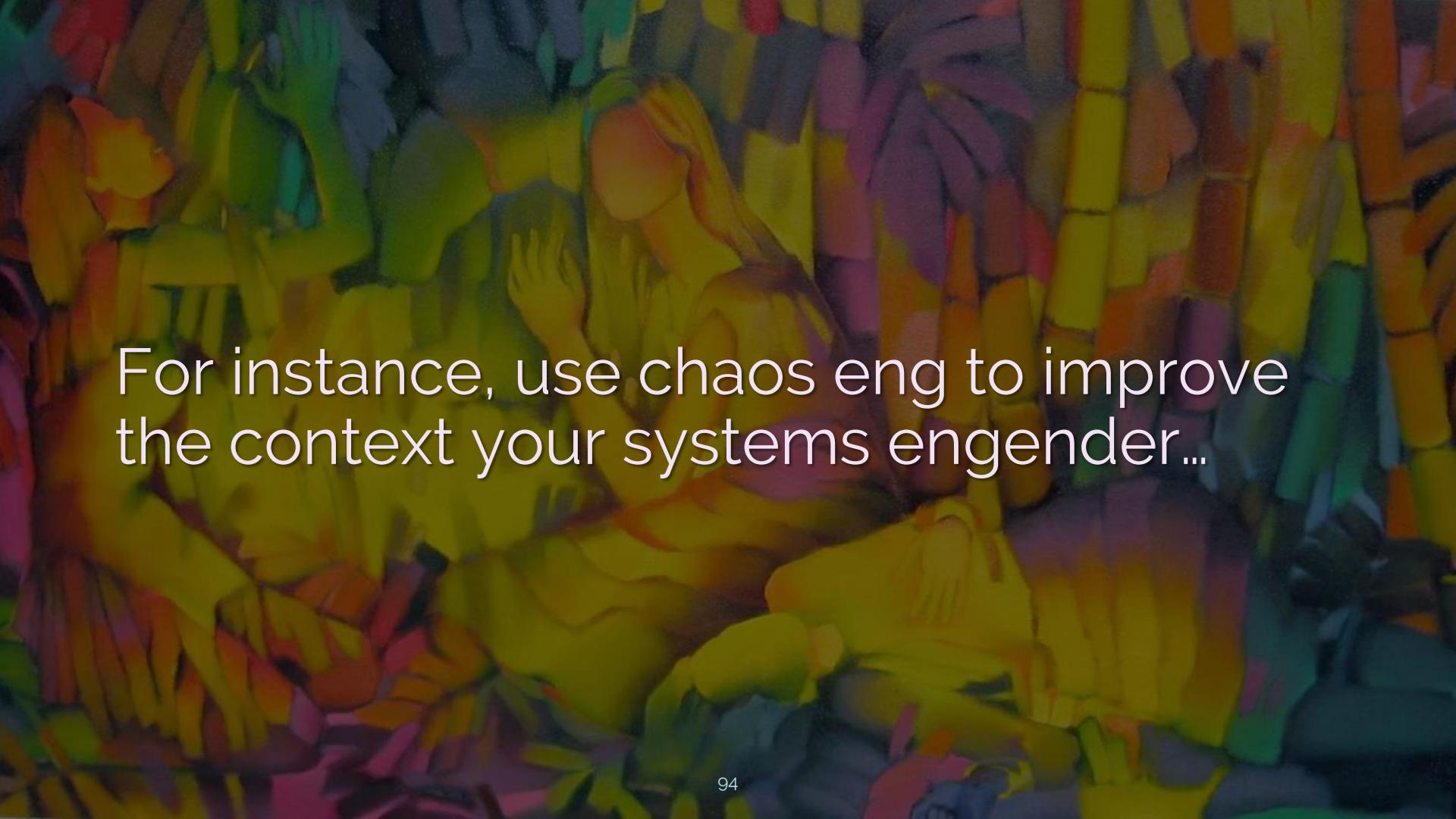
Always consider the messiness of
systems, organizations, and minds



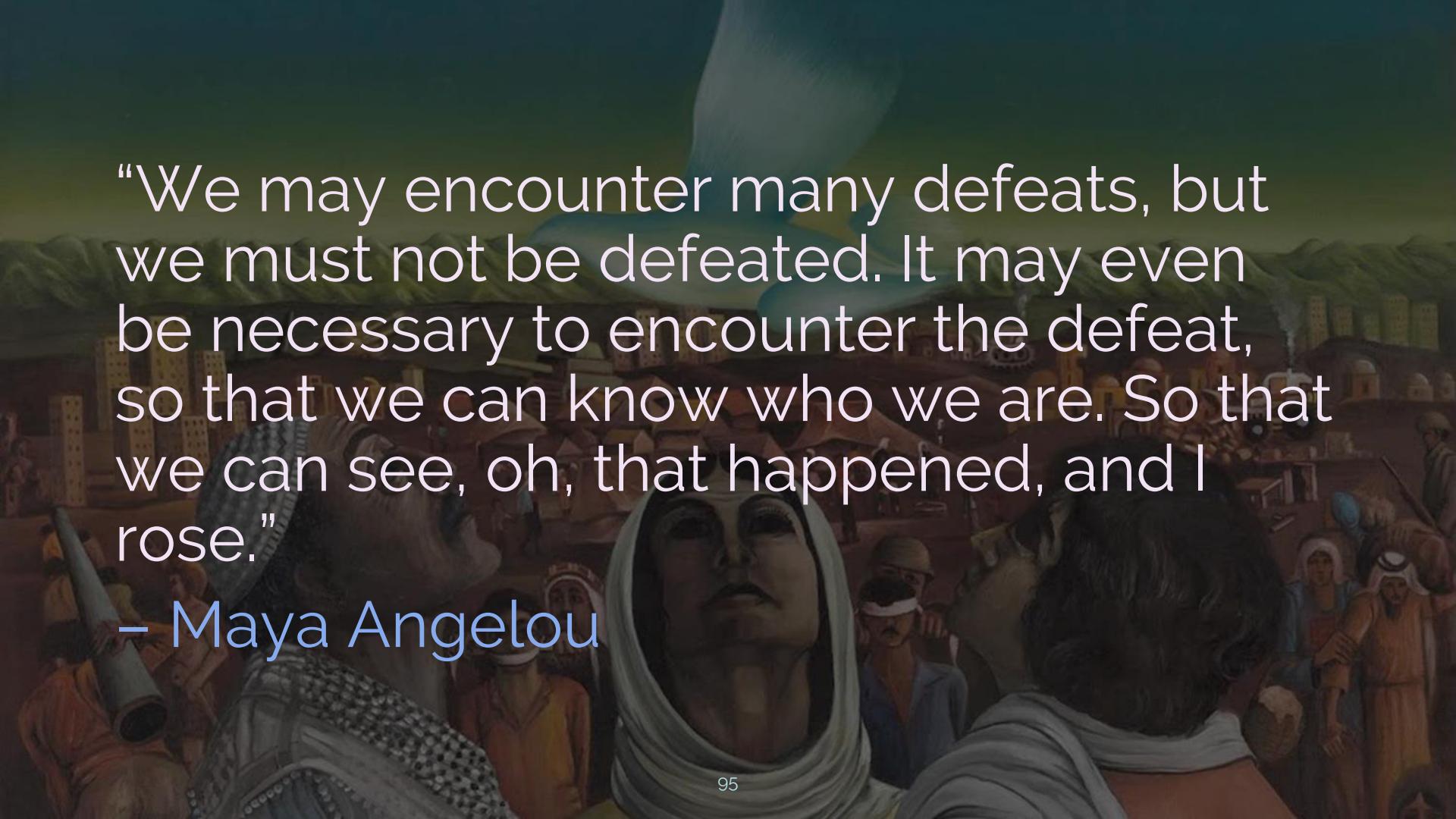
You aren't exempt – your own emotions
play a part in these systems

A painting depicting a scene from a classical or mythological narrative. Two women in flowing, light-colored robes are shown; one reclining on a bed-like surface on the left, and another kneeling on the right, reaching out towards the reclining woman. A large, shaggy dog lies on the floor between them. The background features a wall with a floral patterned wallpaper and a section of light-colored marble or stone. In the bottom foreground, a small object with blue ribbons lies on the floor.

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

The background of the slide features a vibrant, abstract painting style. It consists of numerous overlapping, textured shapes in a variety of colors, including bright yellow, green, blue, and red. These colors are applied in a somewhat muted, painterly manner, creating a soft, layered effect. The overall composition is dynamic and energetic, suggesting movement and complexity.

For instance, use chaos eng to improve
the context your systems engender...

A painting depicting a woman with a white headscarf looking upwards with a contemplative expression. In the background, a sailboat is on the water, and a city skyline is visible under a cloudy sky.

“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@capsule8.com

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.