

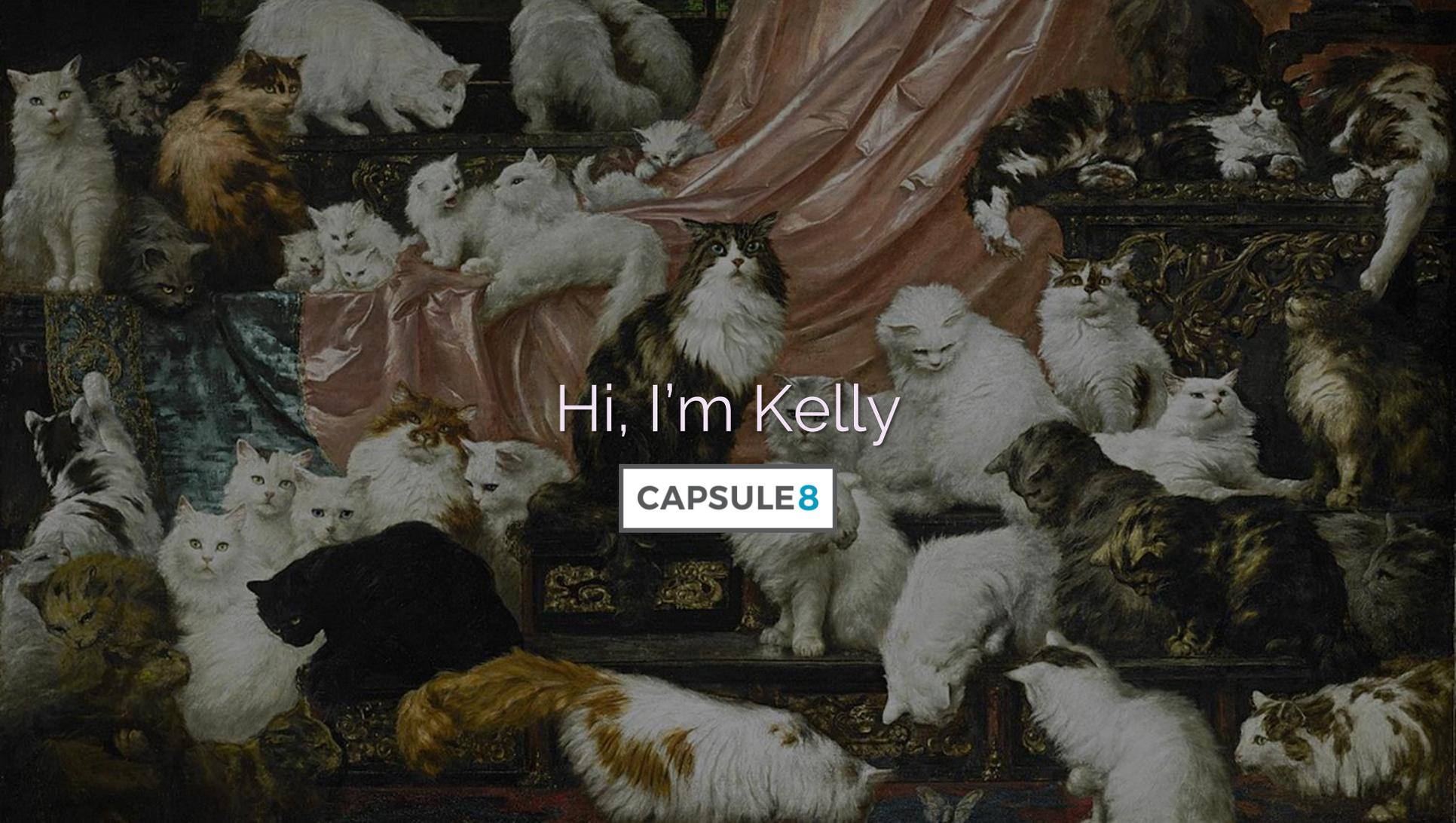
A man with reddish-brown hair, seen from behind, stands on a dark, rocky outcrop. He is wearing a long, dark, textured coat and holding a long, thin staff or walking stick. The background is a vast, misty landscape with rolling hills and mountains under a grey, overcast sky. The overall mood is somber and contemplative.

TO ERR IS HUMAN:

The Complexity of Security Failures

Kelly Shortridge (@swagitda_)

DC Chaos Eng Meetup, April 2020



Hi, I'm Kelly

CAPSULE 8

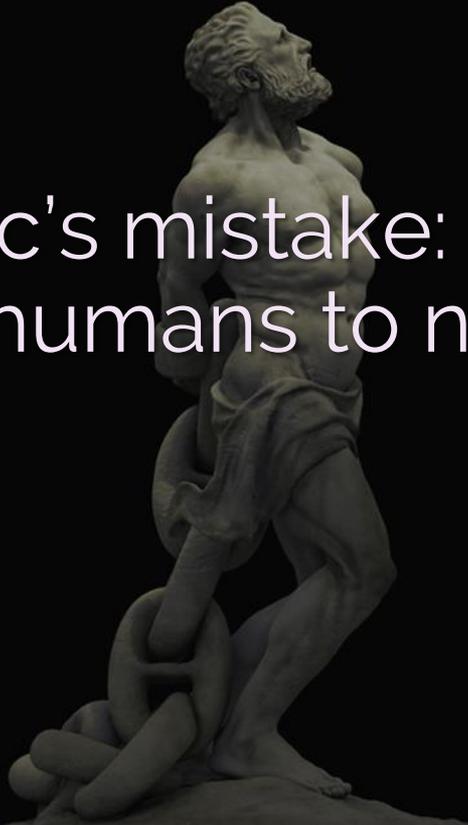
“To err is human; to forgive, divine.”
– Alexander Pope

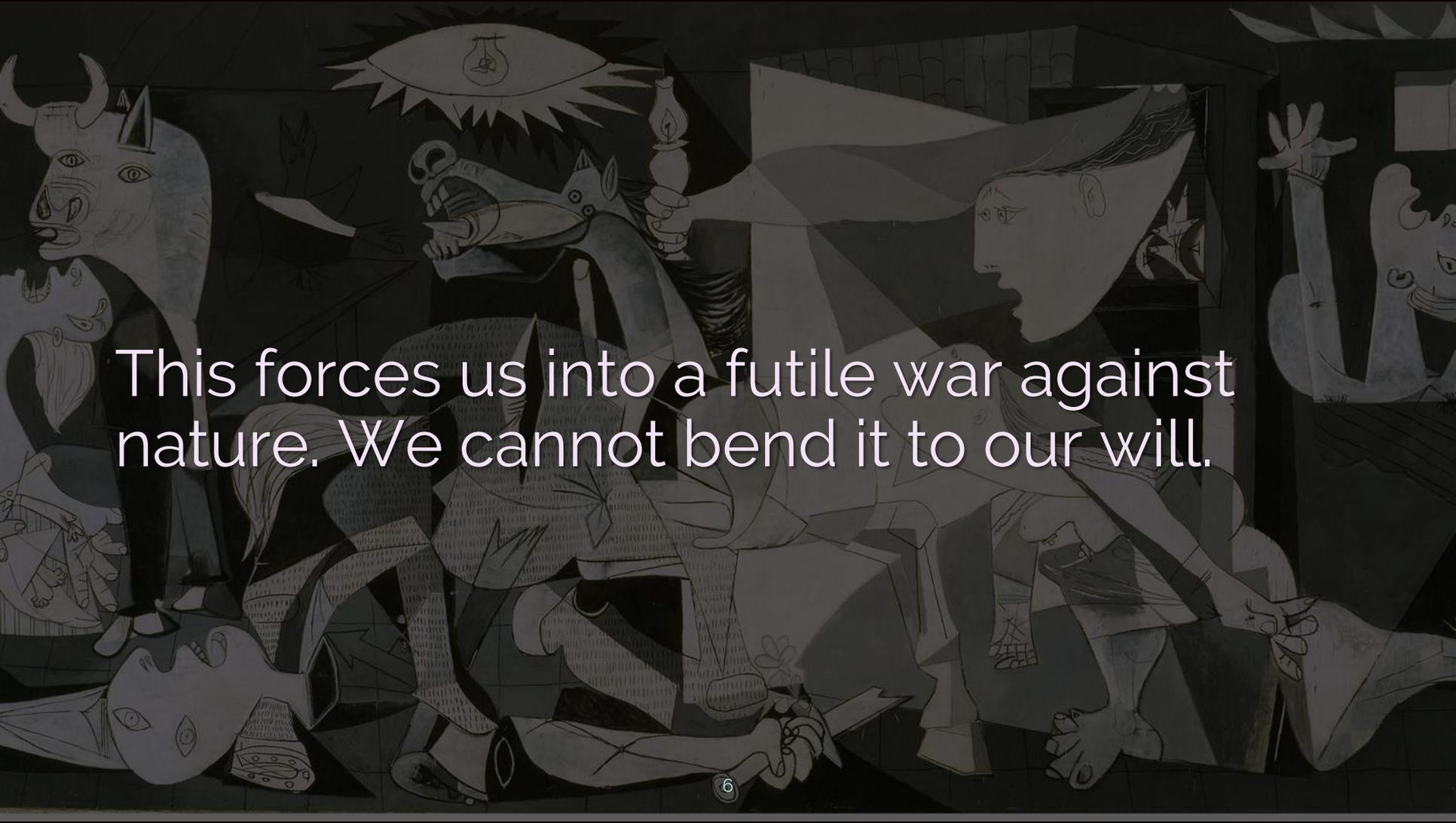




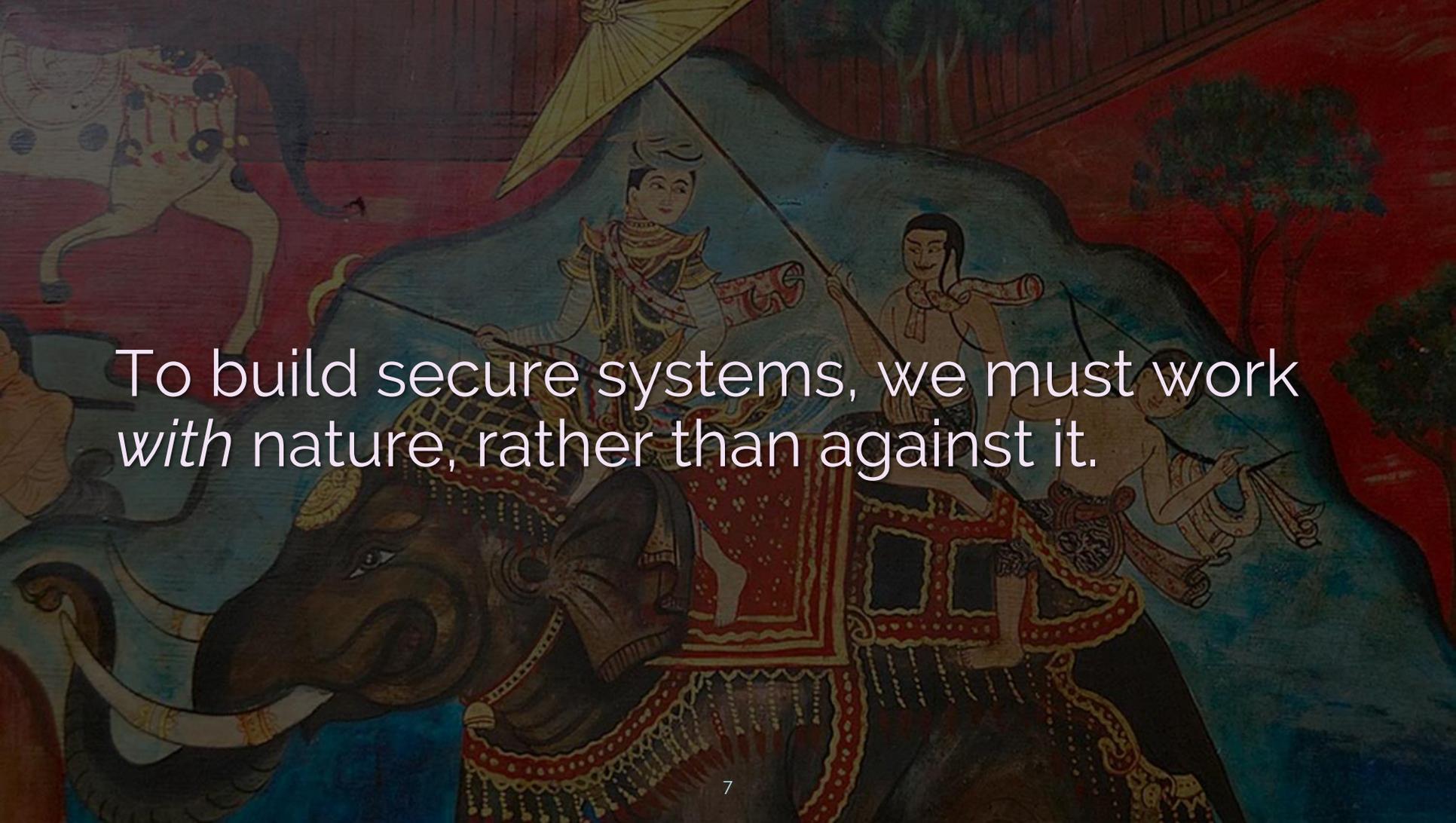
Humans make mistakes. It's part of our nature (it's mostly a feature, not a bug)

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.



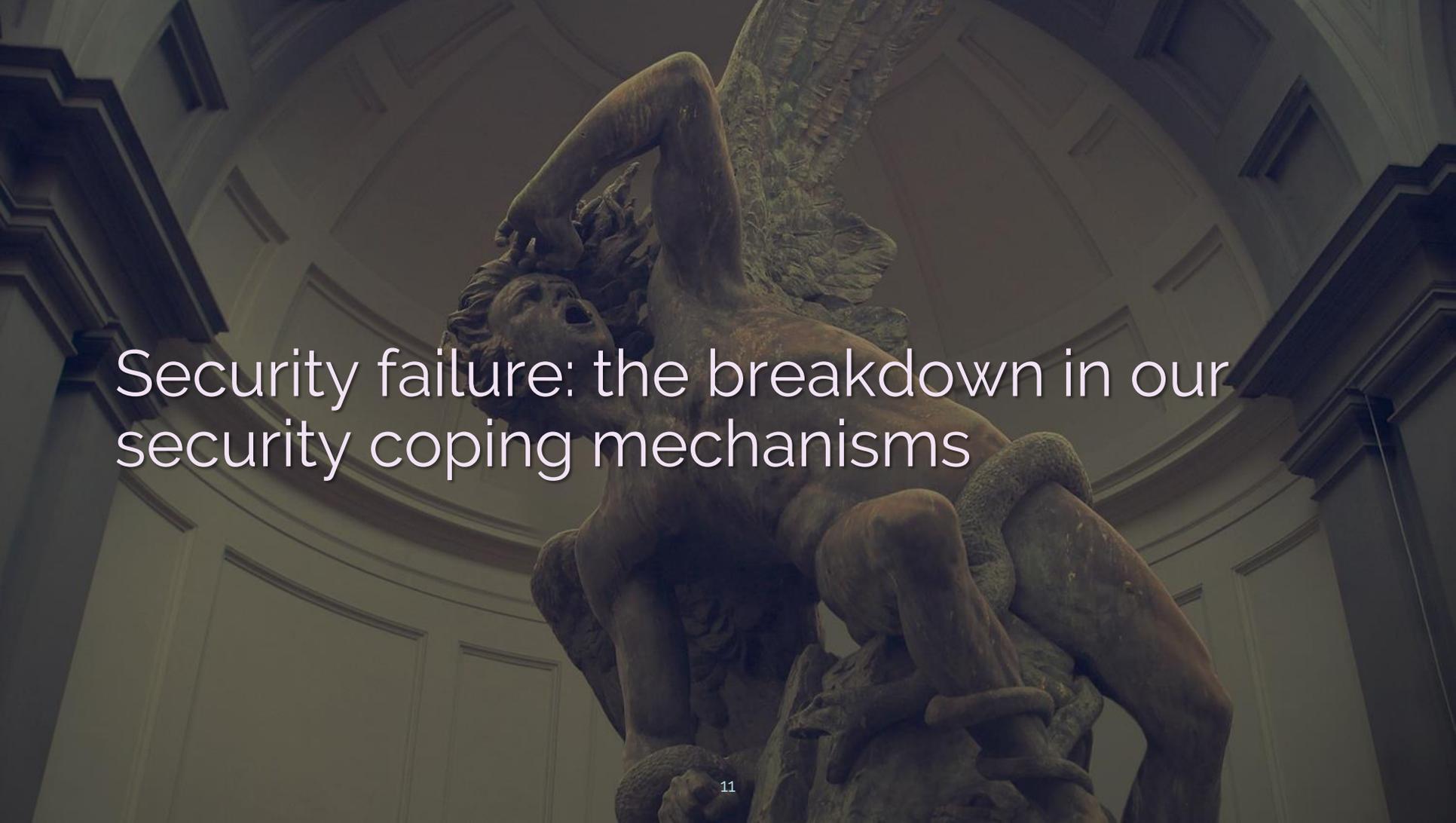
To build secure systems, we must work *with* nature, rather than against it.

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

The background of the slide 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

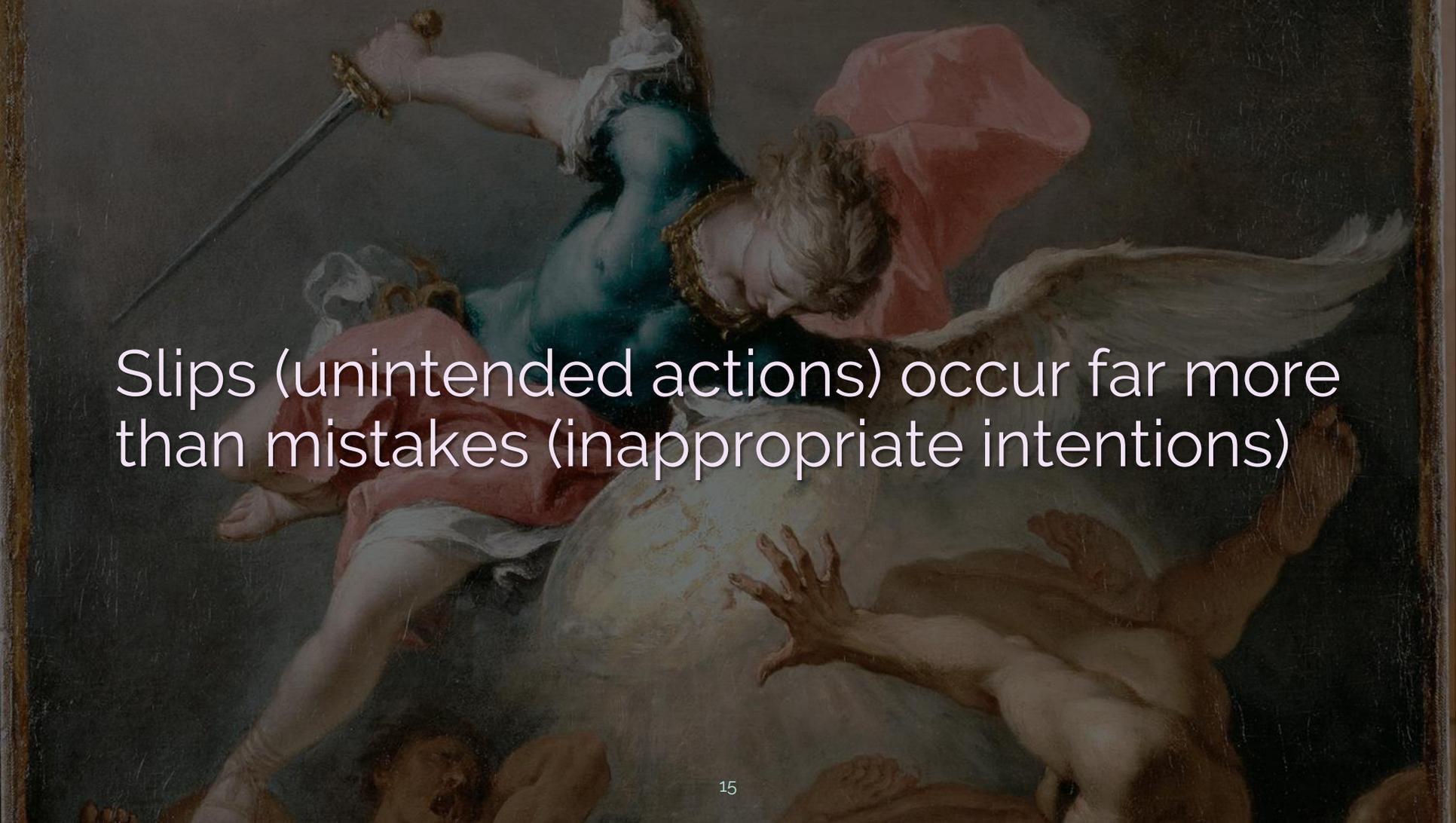
A bronze statue of a winged figure, possibly a personification of Liberty or Justice, is the central focus. The figure is depicted in a dramatic, almost contorted pose, with one arm raised and the other bent. The wings are spread, and the figure's expression is one of intense emotion or struggle. The statue is set against a dark, ornate architectural background, likely the interior of a grand building with a domed ceiling. The lighting is dramatic, highlighting the musculature and texture of the bronze.

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

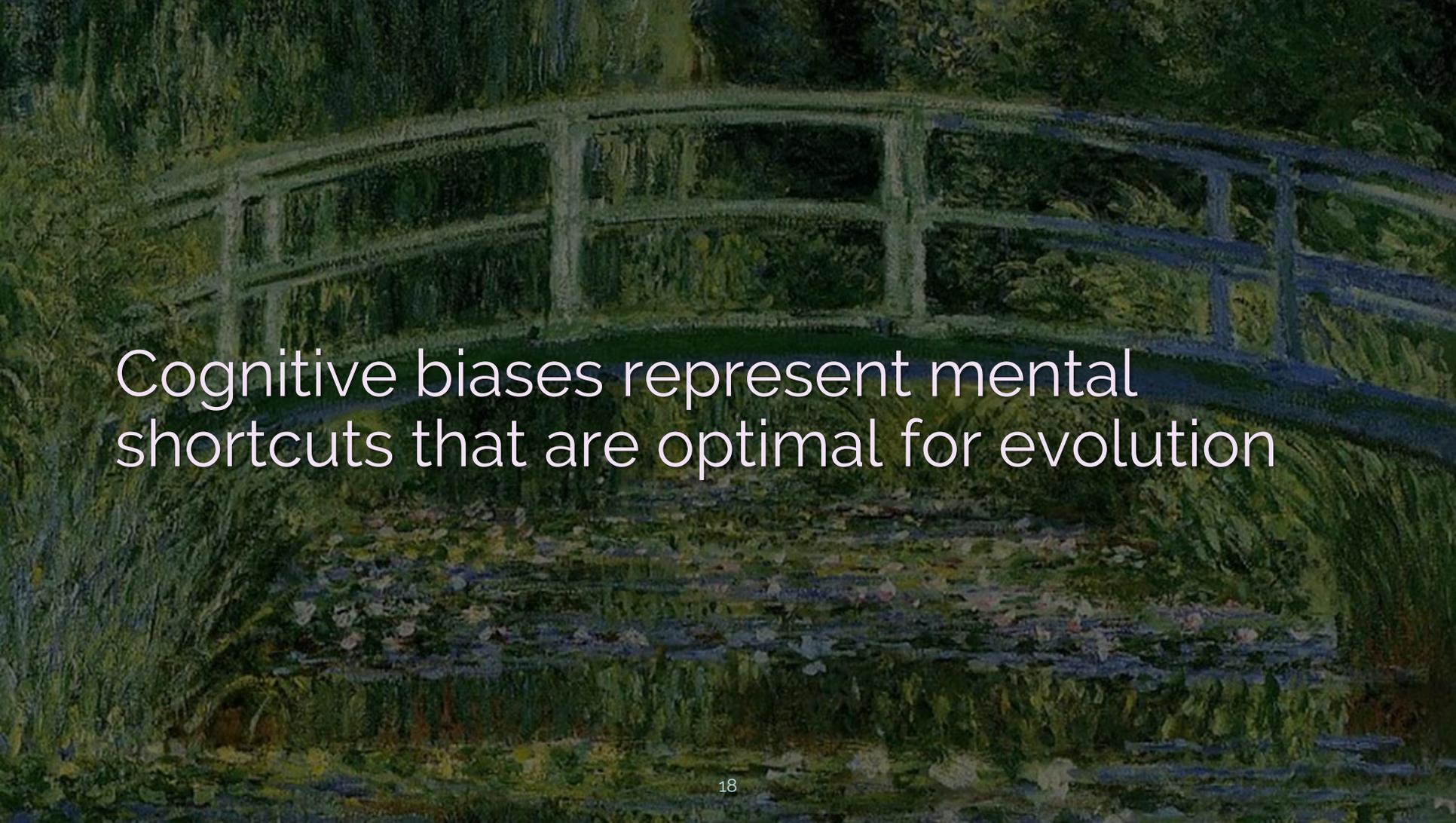


Slips (unintended actions) occur far more than mistakes (inappropriate intentions)

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

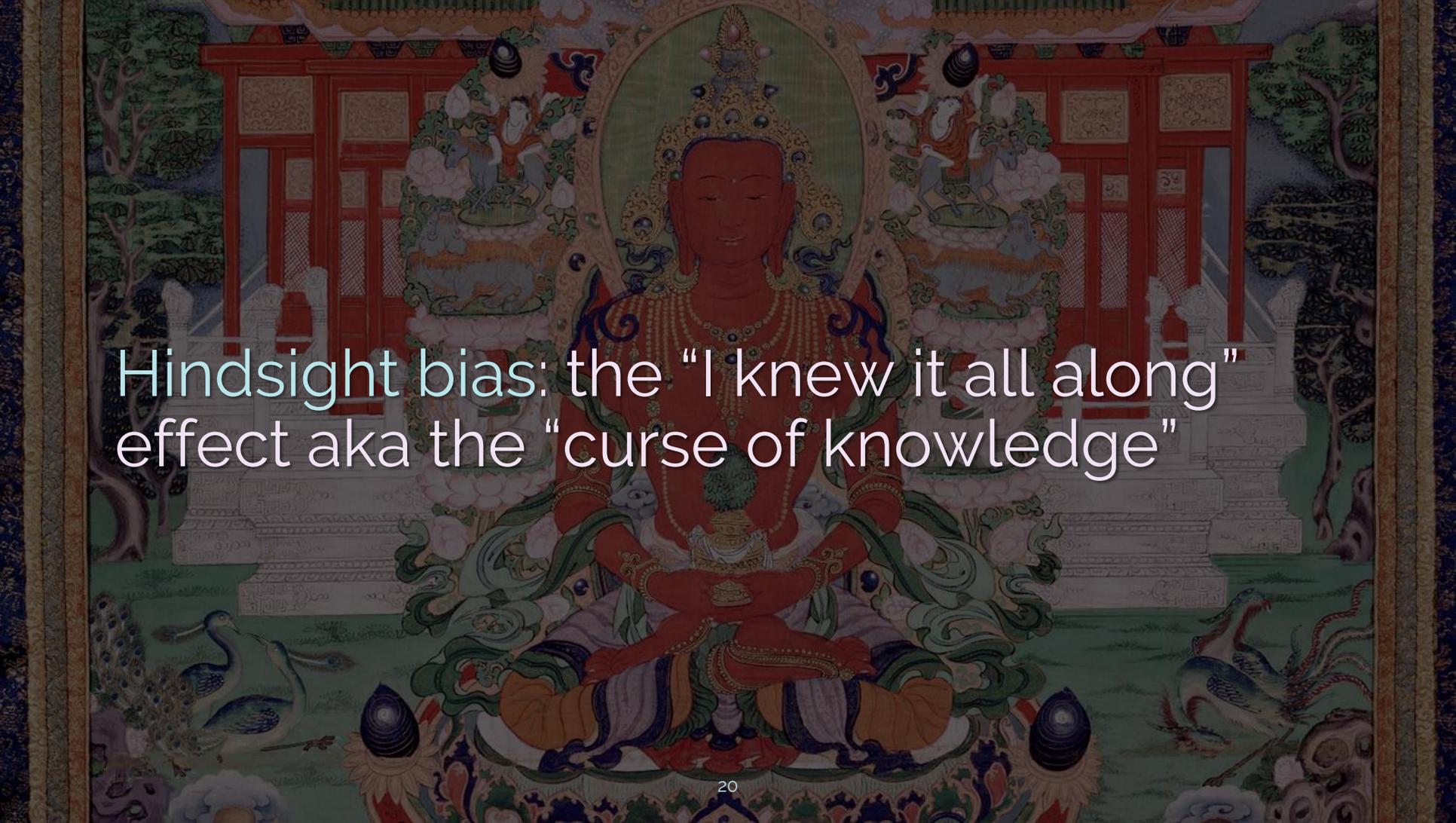


Hindsight & Outcome Bias

The background is a painting of a stone bridge with a wooden railing, crossing a stream. The scene is filled with dense, dark green foliage and trees, creating a sense of a secluded, natural setting. The brushwork is visible, giving the painting a textured, impressionistic feel.

Cognitive biases represent mental shortcuts that are optimal for evolution

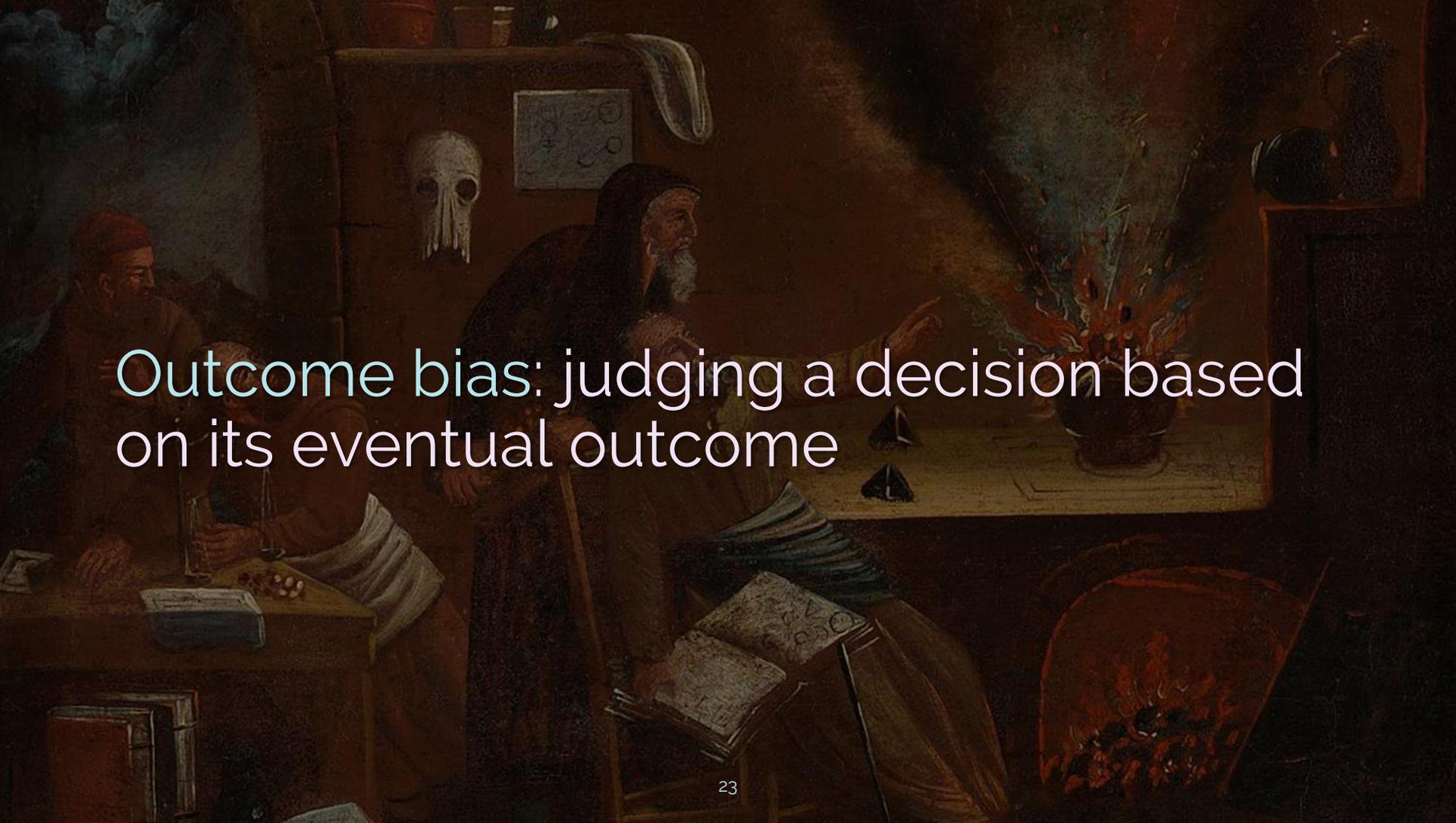
We learn from the past to progress, but our “lizard brain” can take things too far



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”



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 three individuals seated around a low, ornate table, engaged in a board game. The man on the left wears a blue and gold headdress and a patterned kilt. The woman in the center is dressed in white with gold jewelry and a headband. The man on the right wears a yellow headscarf and a patterned kilt. The table is set with a grid and small game pieces. The background shows a room with a patterned wall and a doorway leading to a landscape 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

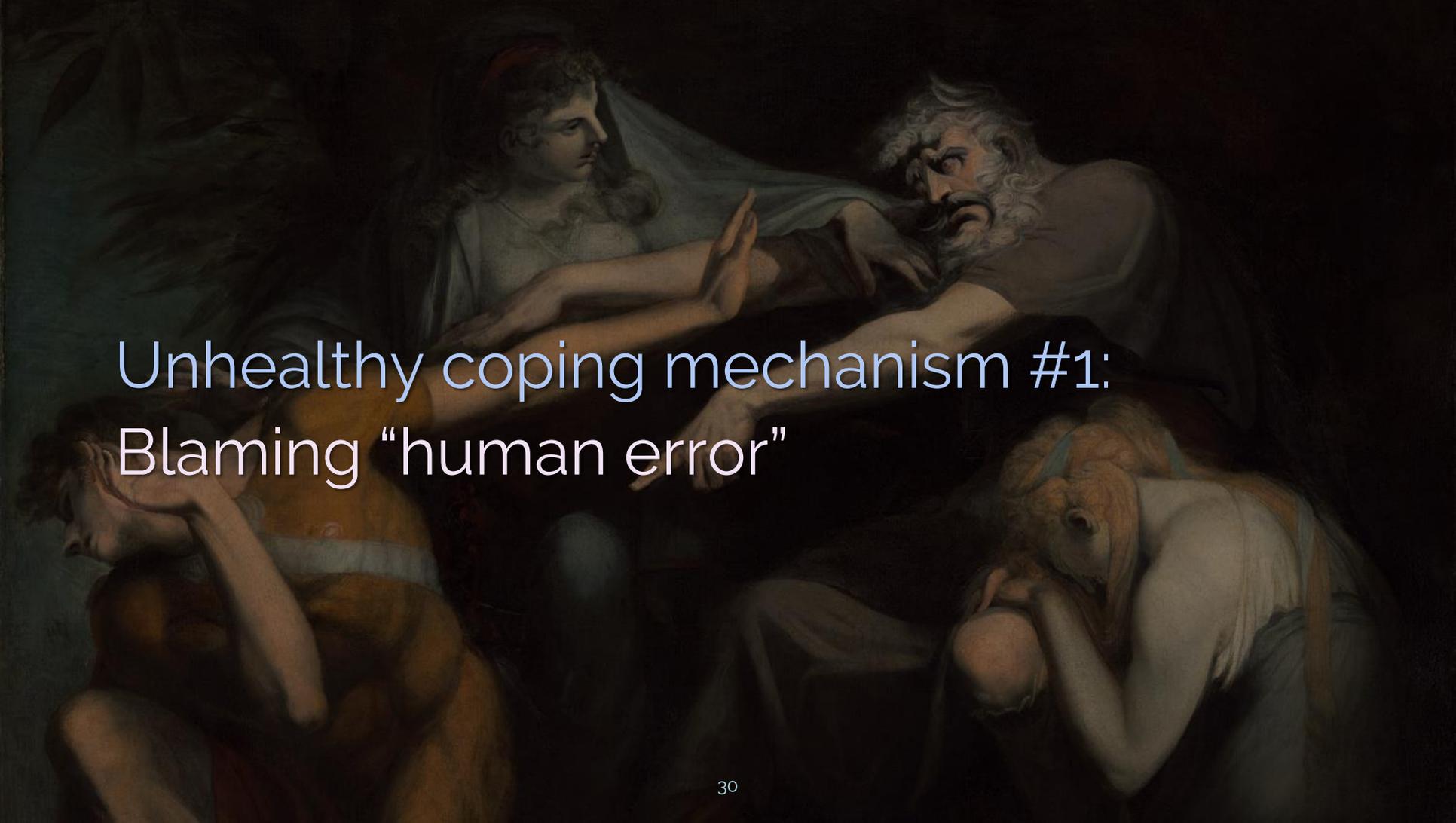
A dark, monochromatic photograph of a classical sculpture, likely the Statue of Liberty, with the text overlaid. The sculpture is shown in profile, facing right, and features a large, ornate crown. The background is a blurred, light-colored architectural structure.

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”

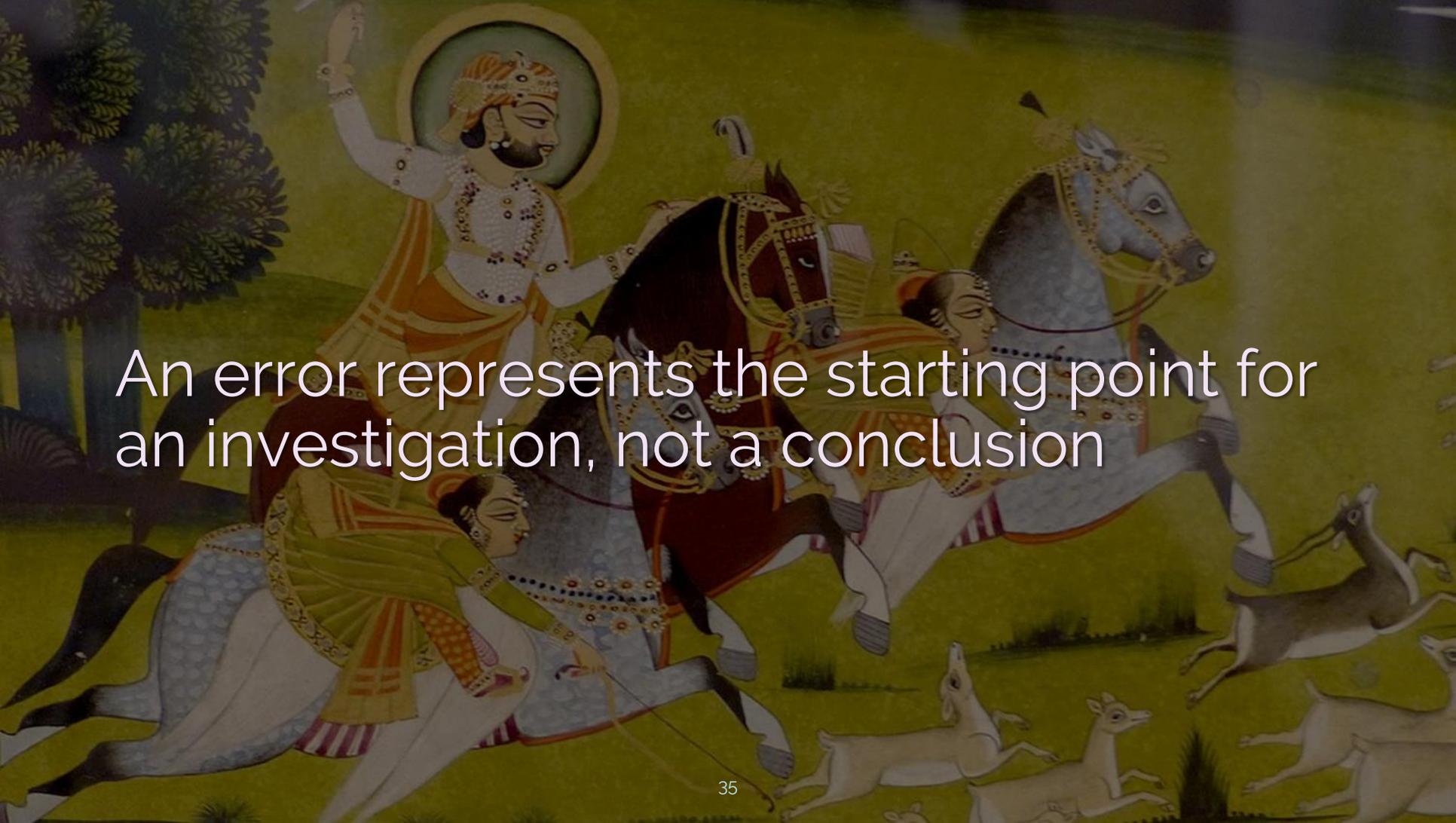
Infosec's fav hobbies: PICNIC & PEBKAC

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?”

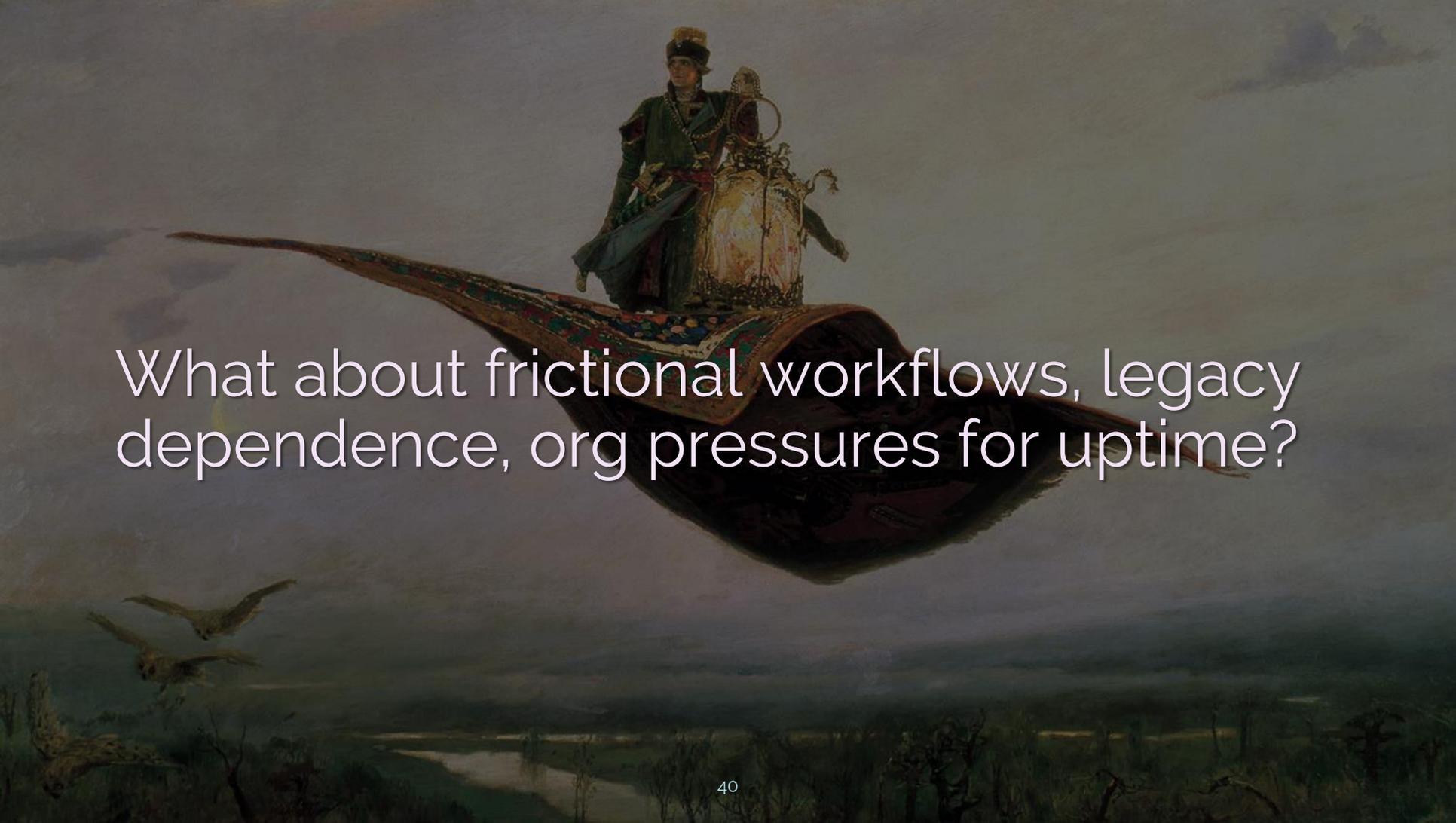
“Why did clicking a link lead to pwnage?”

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



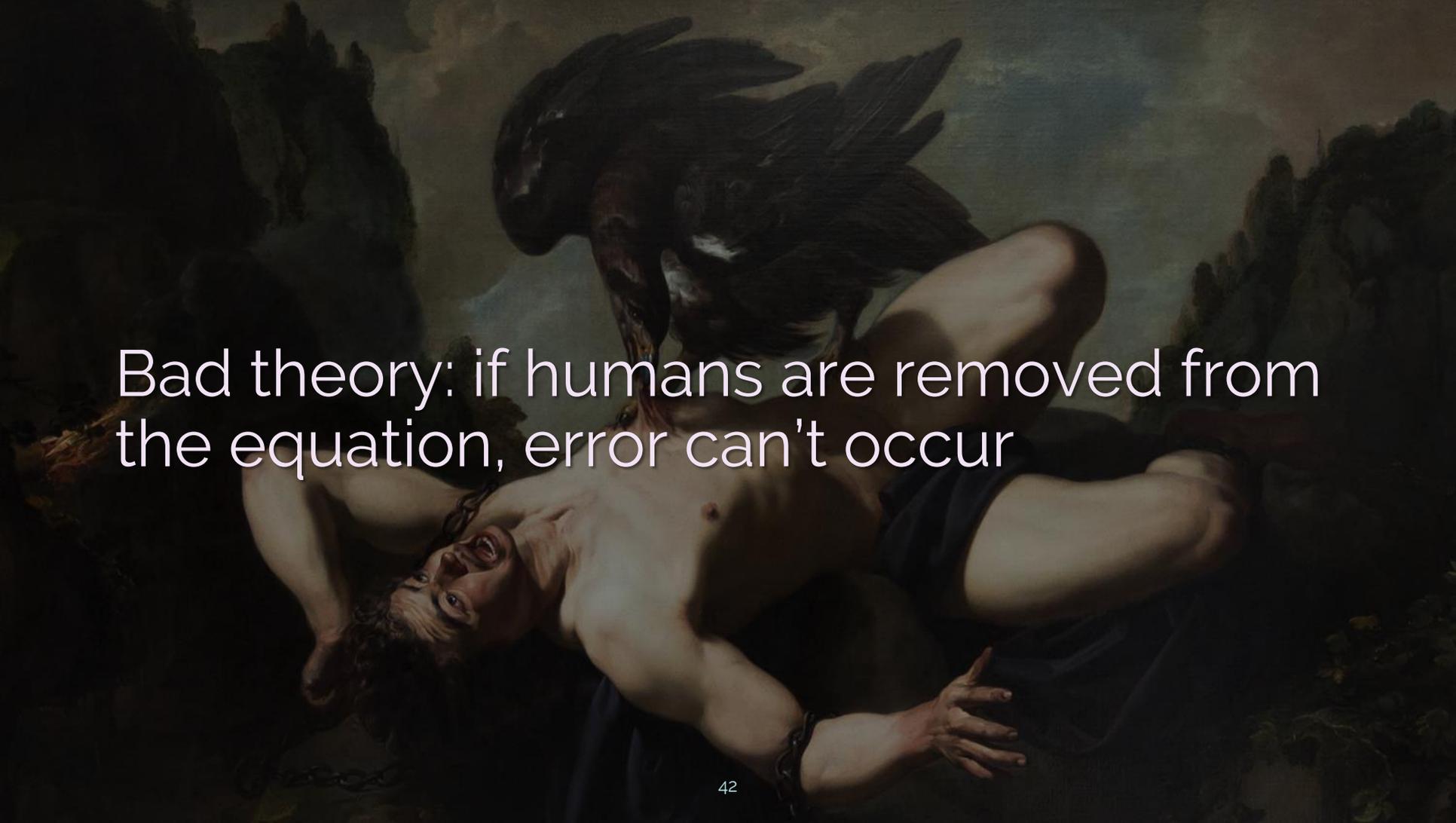
e.g. training devs to “care about security”
completely misses the underlying issue

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

A person in traditional, ornate attire is riding a flying carpet over a landscape. The carpet is dark and has a colorful, patterned border. The person is wearing a green and blue outfit with a gold crown. The background shows a hazy, mountainous landscape with a river and some trees. The overall tone is dramatic and somewhat somber.

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. Her central face is the most prominent, looking forward. The other faces are positioned around her head, some looking to the left and some to the right. She wears a tall, ornate crown (mukuta) and is adorned with multiple necklaces and bangles. Her attire consists of a pink sari with a gold border. In her various hands, she holds several weapons: a trident (trishula), a sword (khadga), a mace (gada), a conch shell (shankha), and a bow (bana). The background is a dense field of peacock feathers, with their characteristic 'eyes' in shades of blue, green, and gold. The overall style is characteristic of traditional Indian miniature painting.

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.

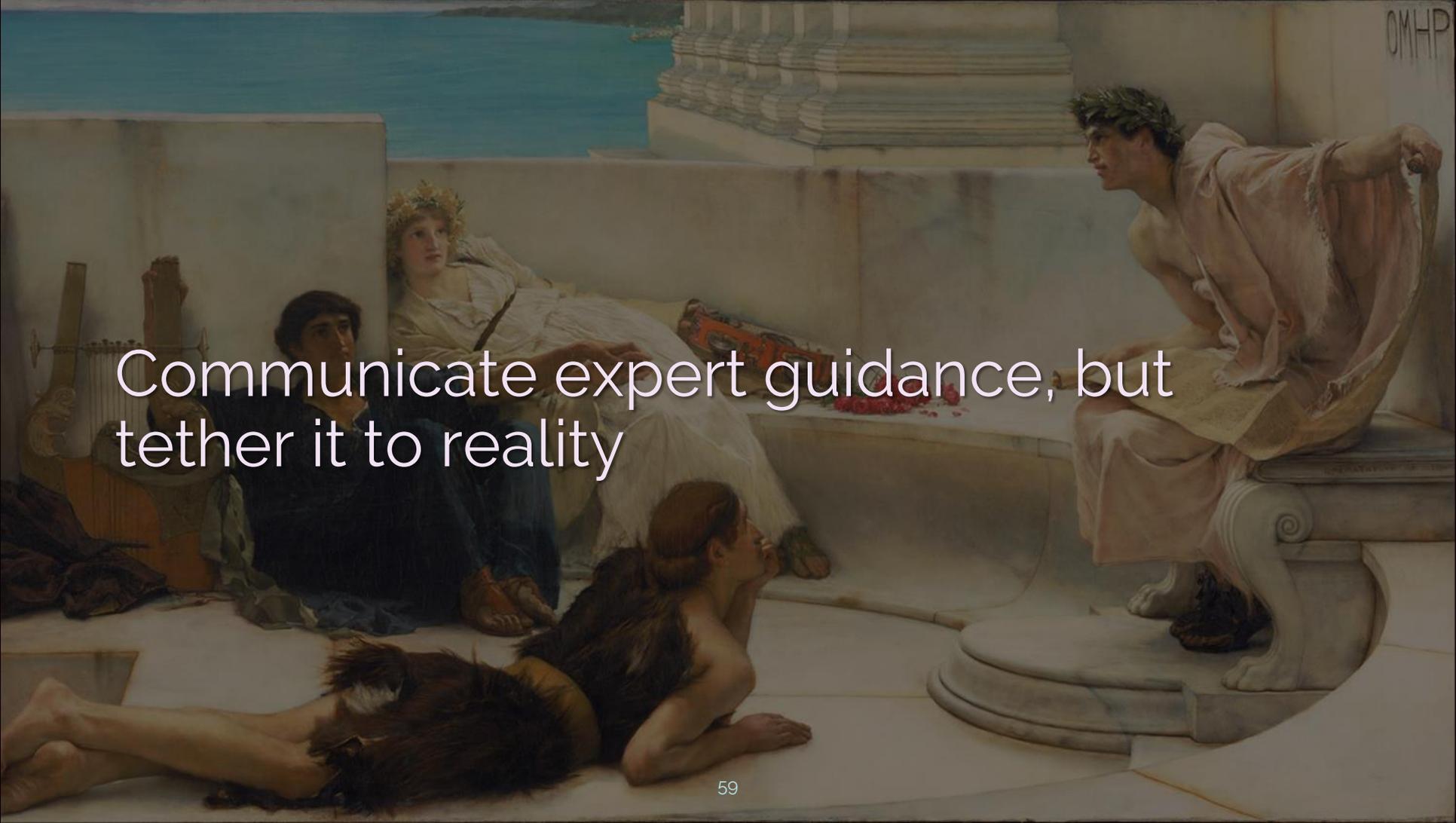
Discipline doesn't actually fix the "policy violation" cause (but it does scapegoat)

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

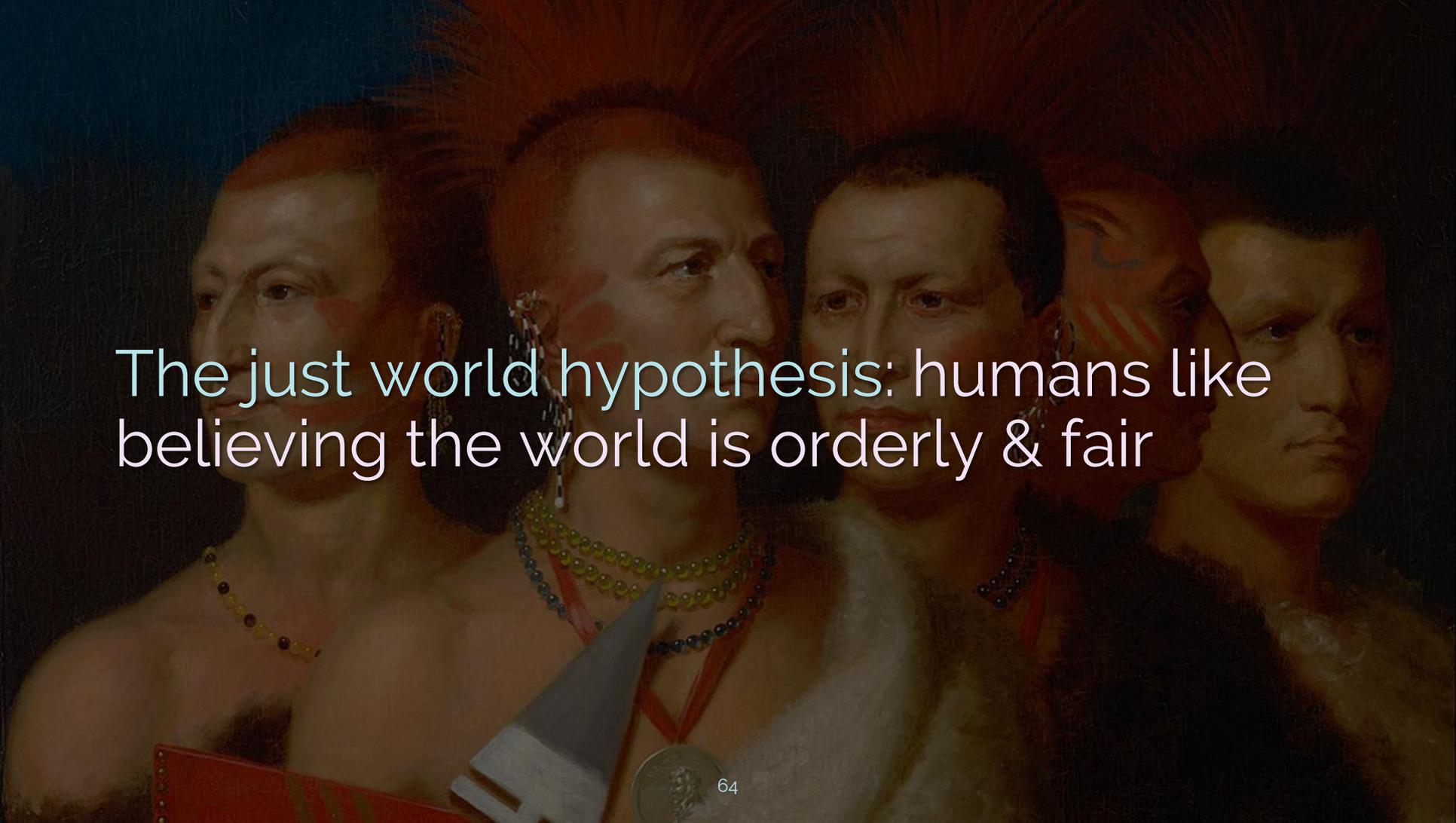
Checklists can be valuable aids *if* they're based on knowledge of real workflows

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 traditional beaded necklaces and large feathered headdresses. The figures are arranged in a row, looking towards the right. The background is dark and textured.

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



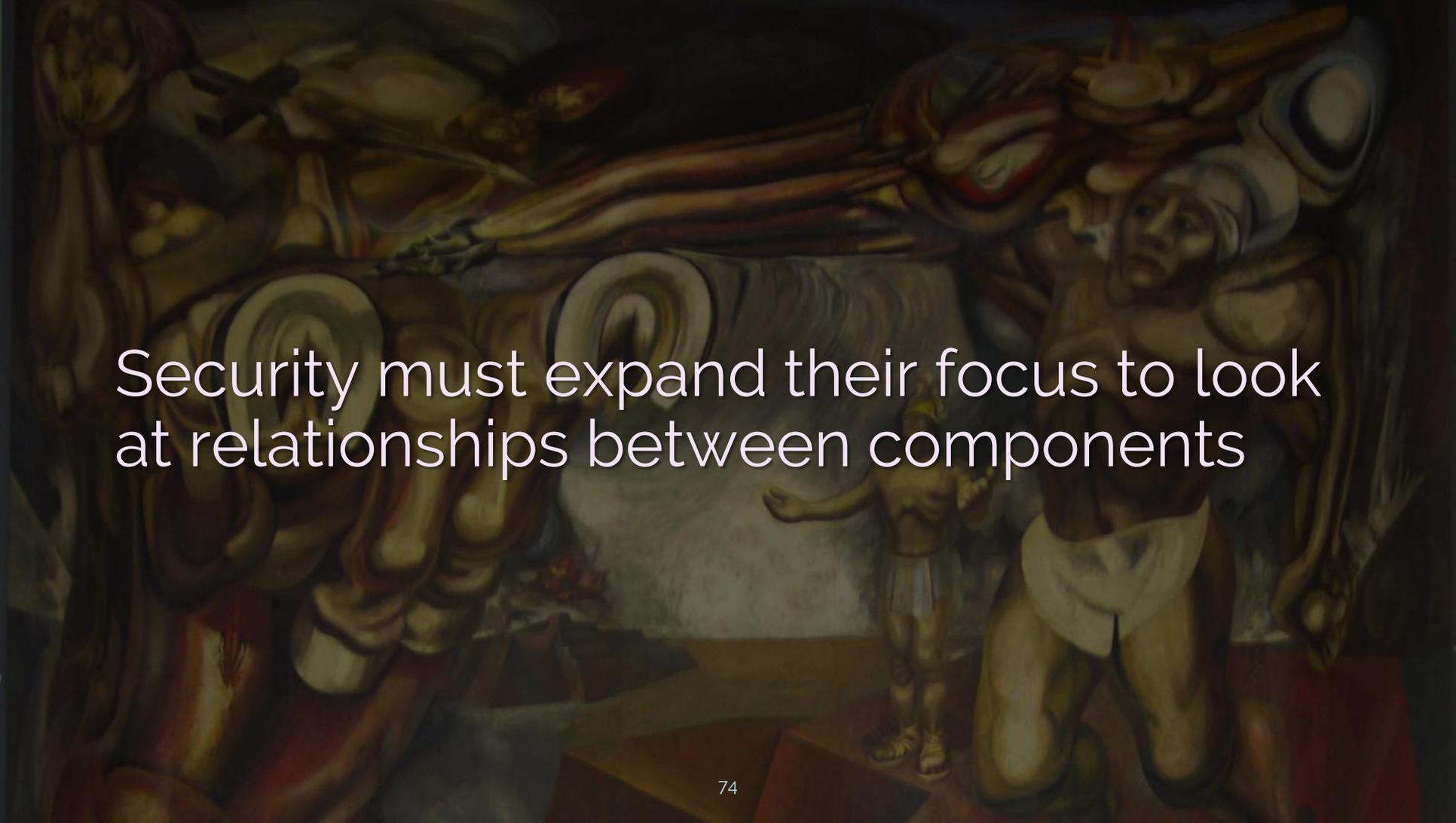
Infosec will progress when we ensure
the easy way is the secure way

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

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 thin black lines, some straight and some curved, creating a sense of movement and structure. The overall color palette is rich and varied, with a mix of warm and cool tones.

System perspective

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

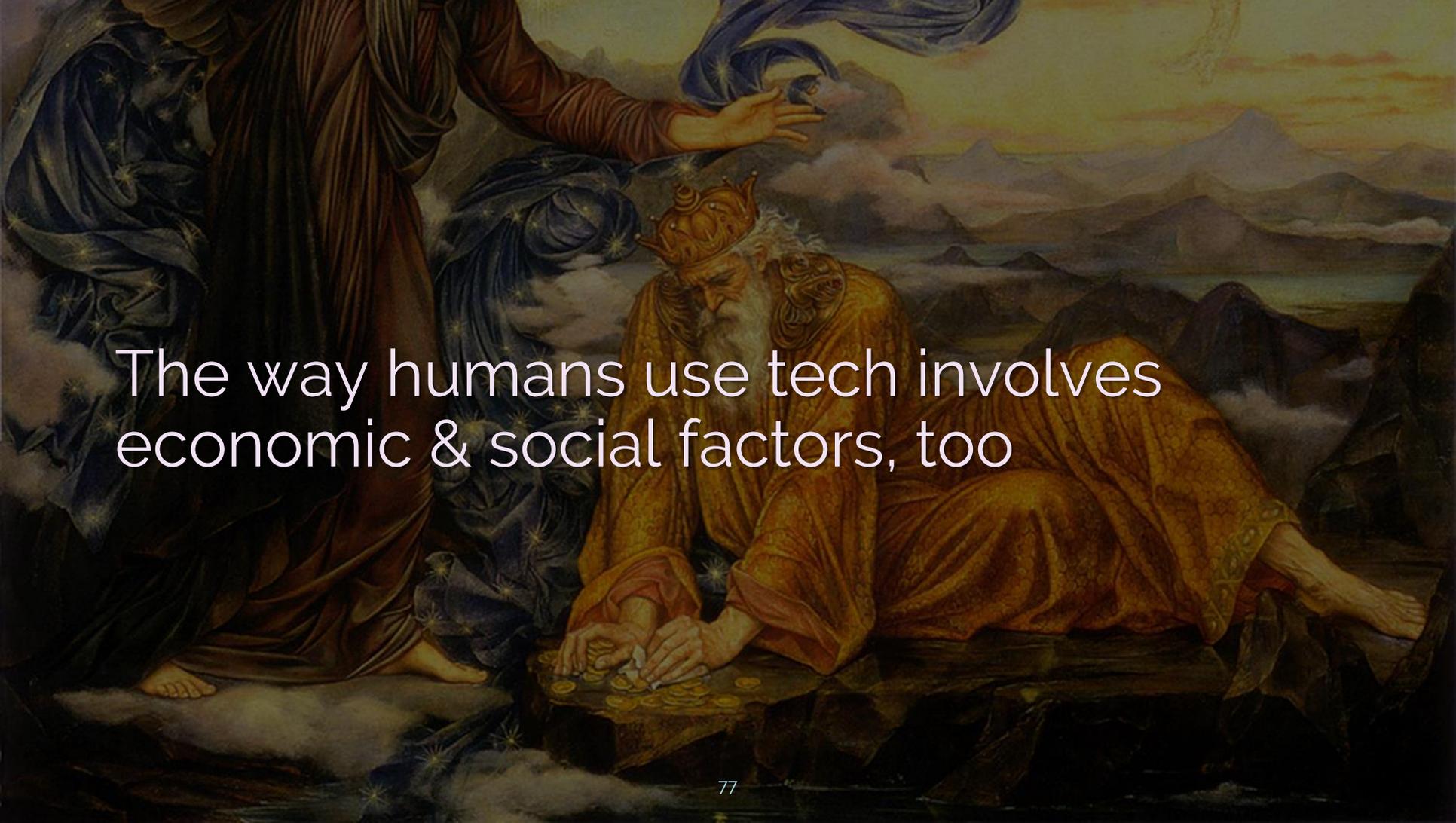
The background is a dark, textured image of a complex, abstract painting. It features several figures, including a prominent one on the right wearing a white headwrap and a white loincloth. There are also smaller figures and swirling, organic shapes in shades of brown, yellow, and white. The overall style is reminiscent of traditional African art or a similar cultural aesthetic.

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”

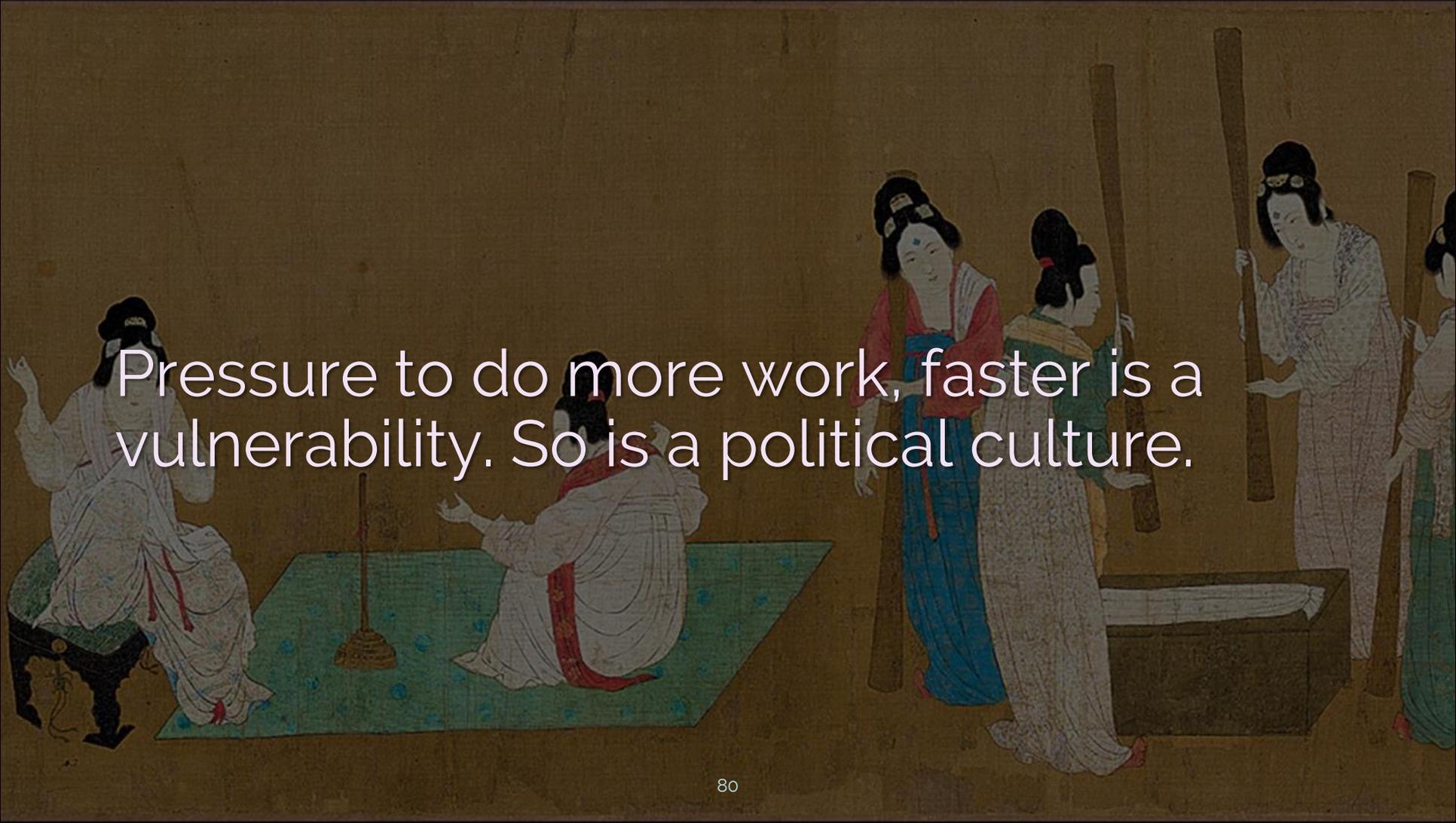
– Nancy Leveson



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

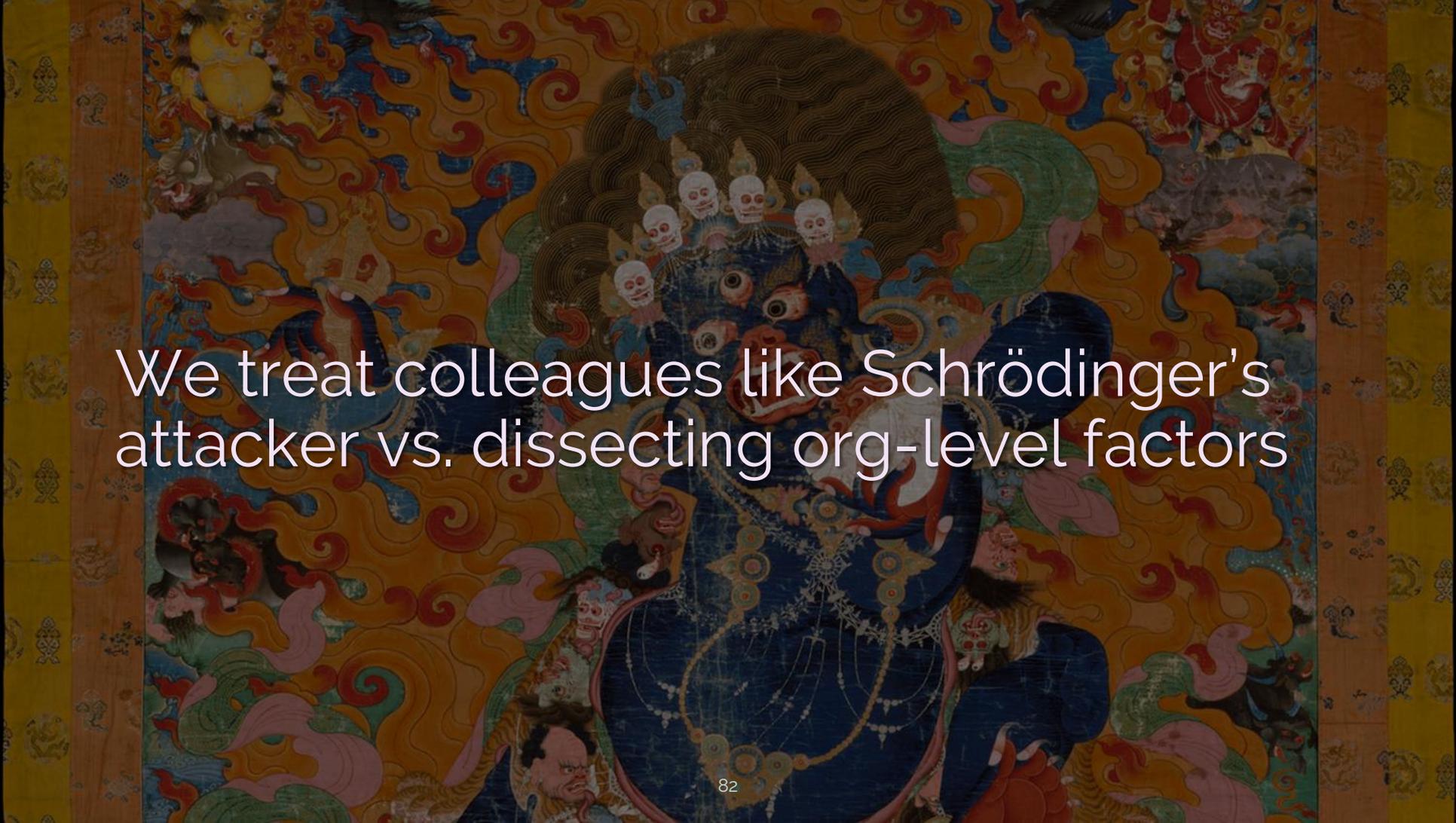
Economic factors: revenue & profit goals, compensation schemes, budgeting, etc.

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



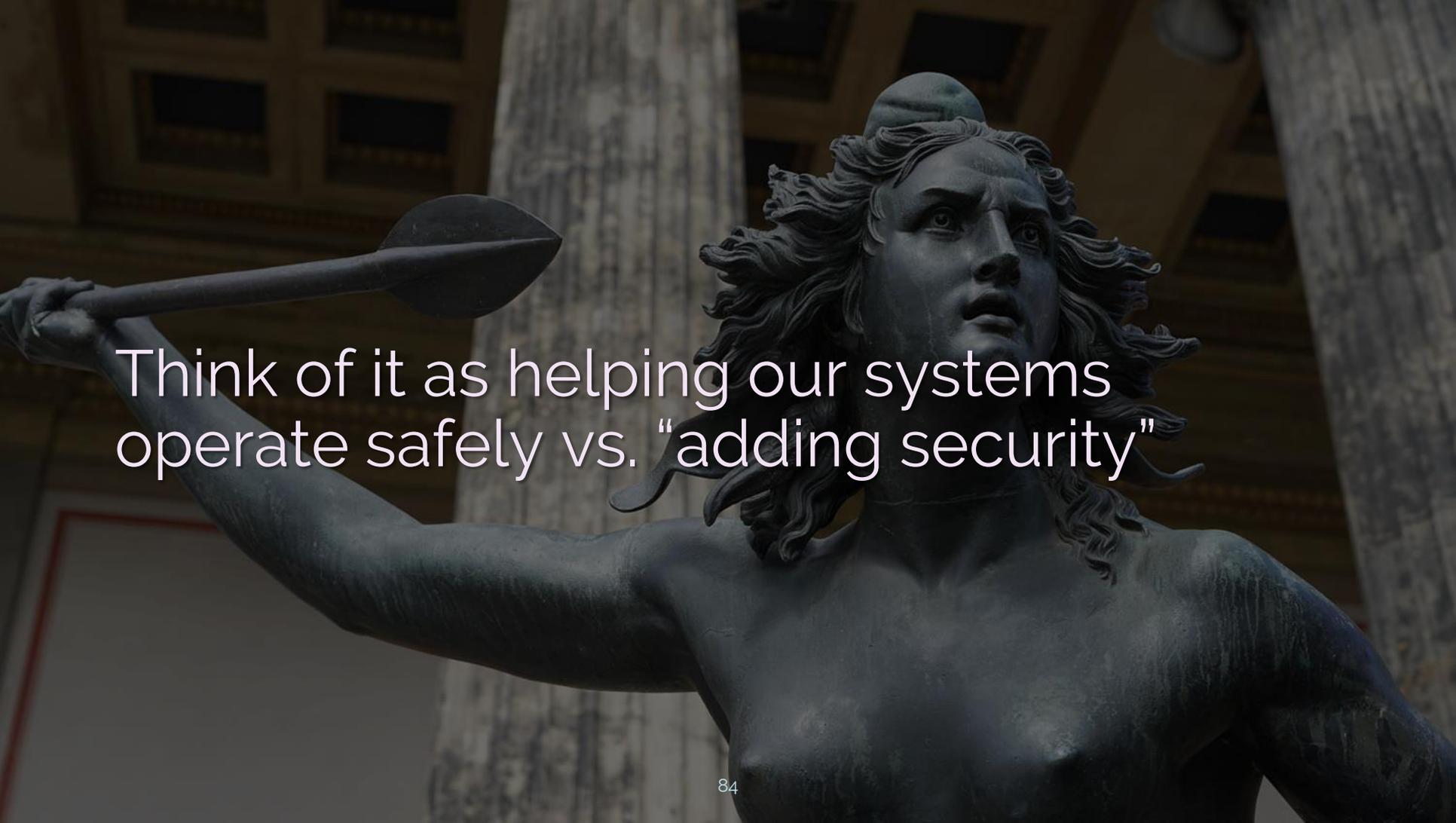
Pressure to do more work, faster is a vulnerability. So is a political culture.

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

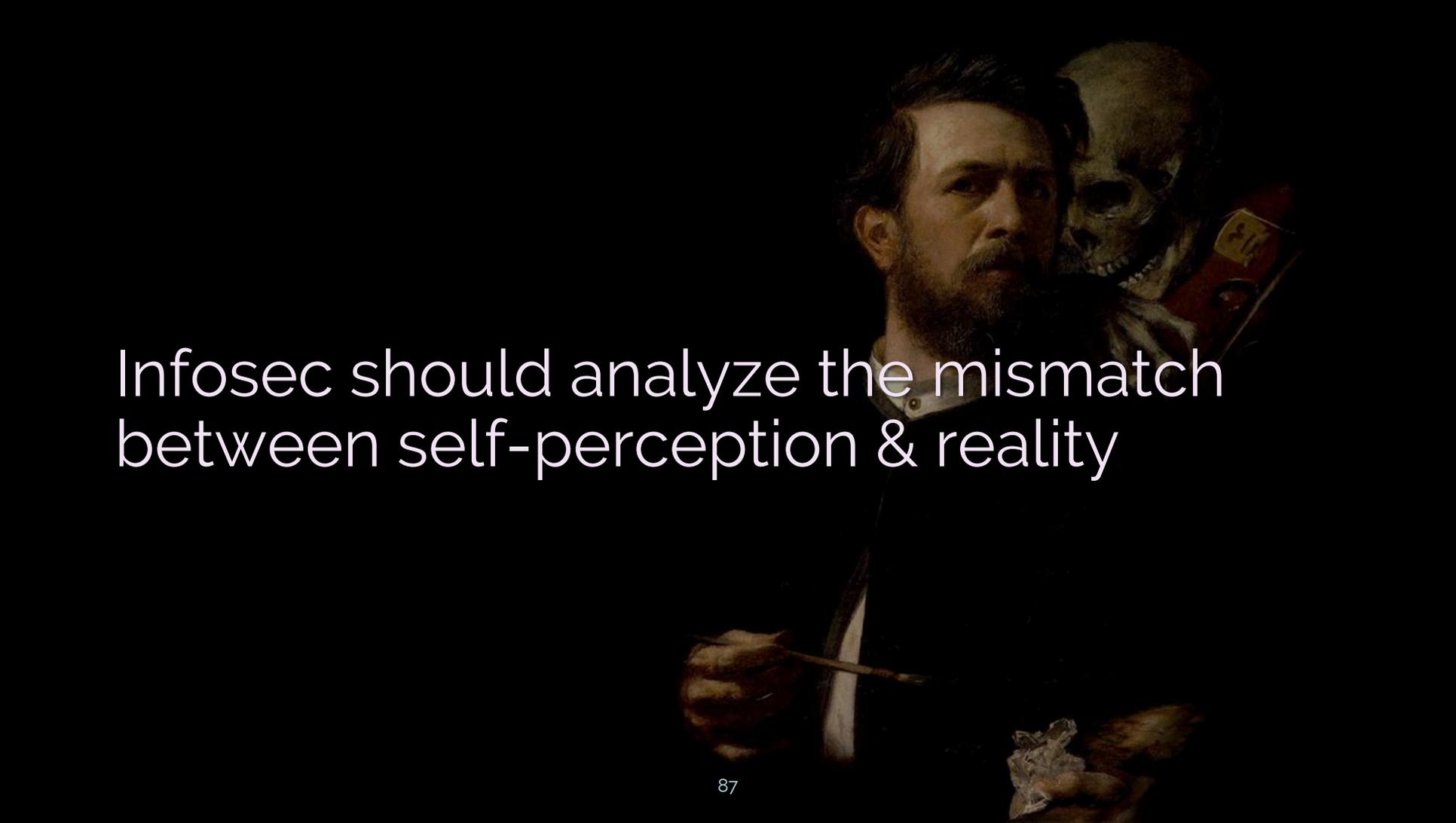
**Security is something a system does,
not something a system has.**



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

A dark, atmospheric painting of a man with a beard and a skull behind him. The man is looking slightly to the right with a serious expression. He is wearing a dark coat over a white shirt. Behind him, a human skull is visible, and to the right, there is a red book or document with a yellow label. The overall scene is dimly lit, with the man's face and the skull being the primary light sources.

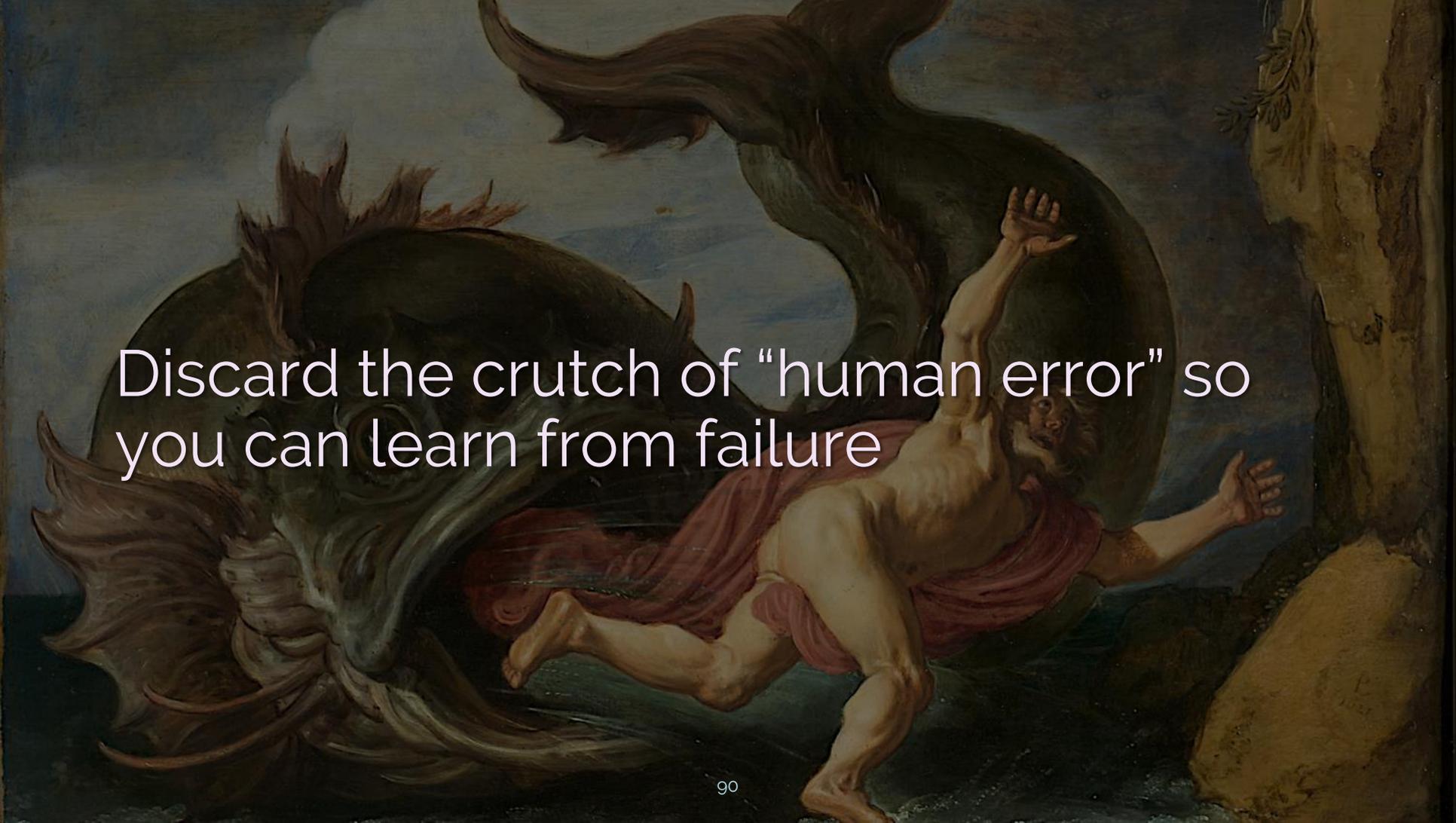
Infosec should analyze the mismatch
between self-perception & reality



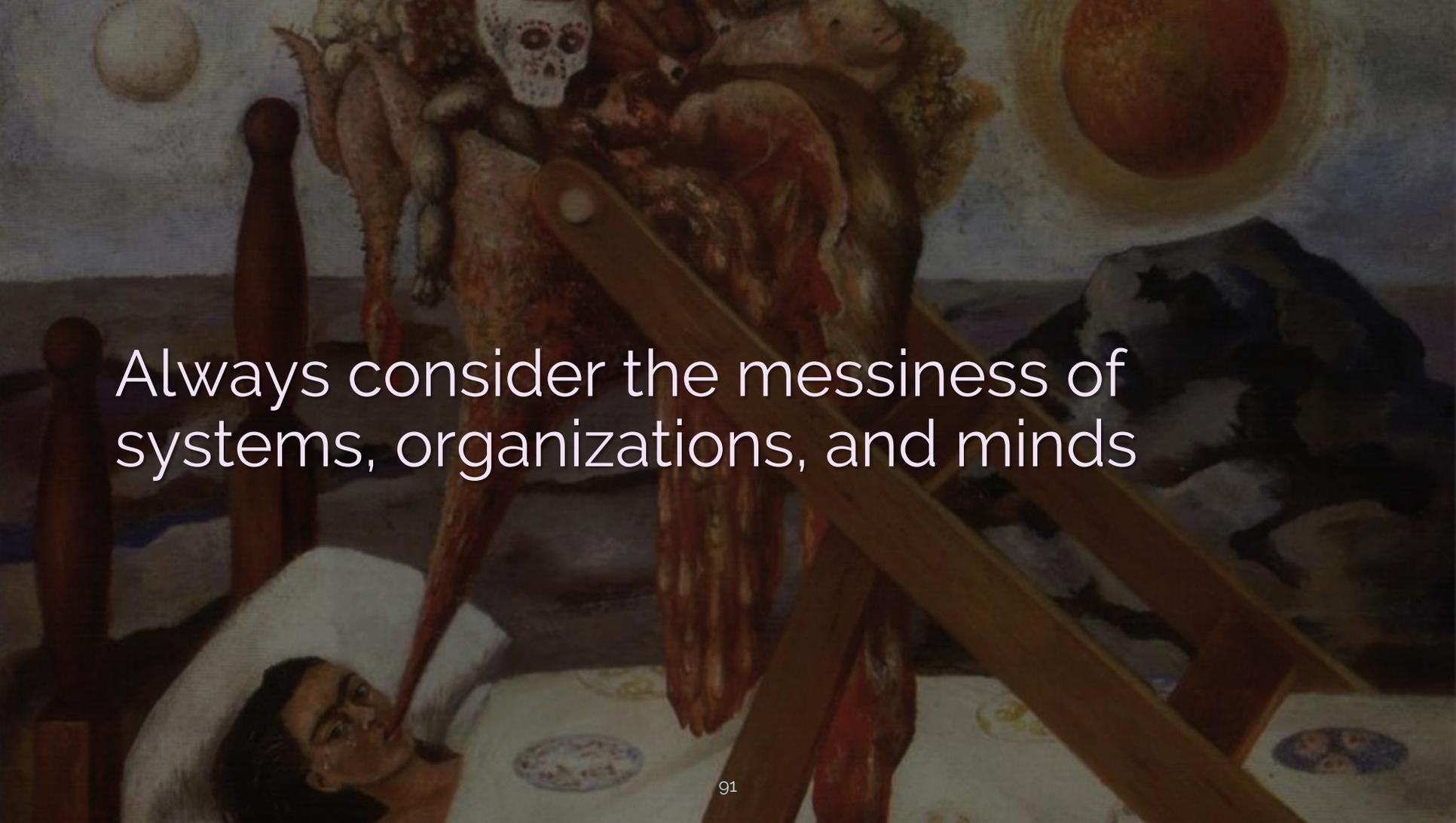
Spoiler alert: security chaos
engineering

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 forward with his right hand. The background is a dramatic, cloudy sky. The text "In Conclusion" is overlaid in white serif font on the left side of the image.

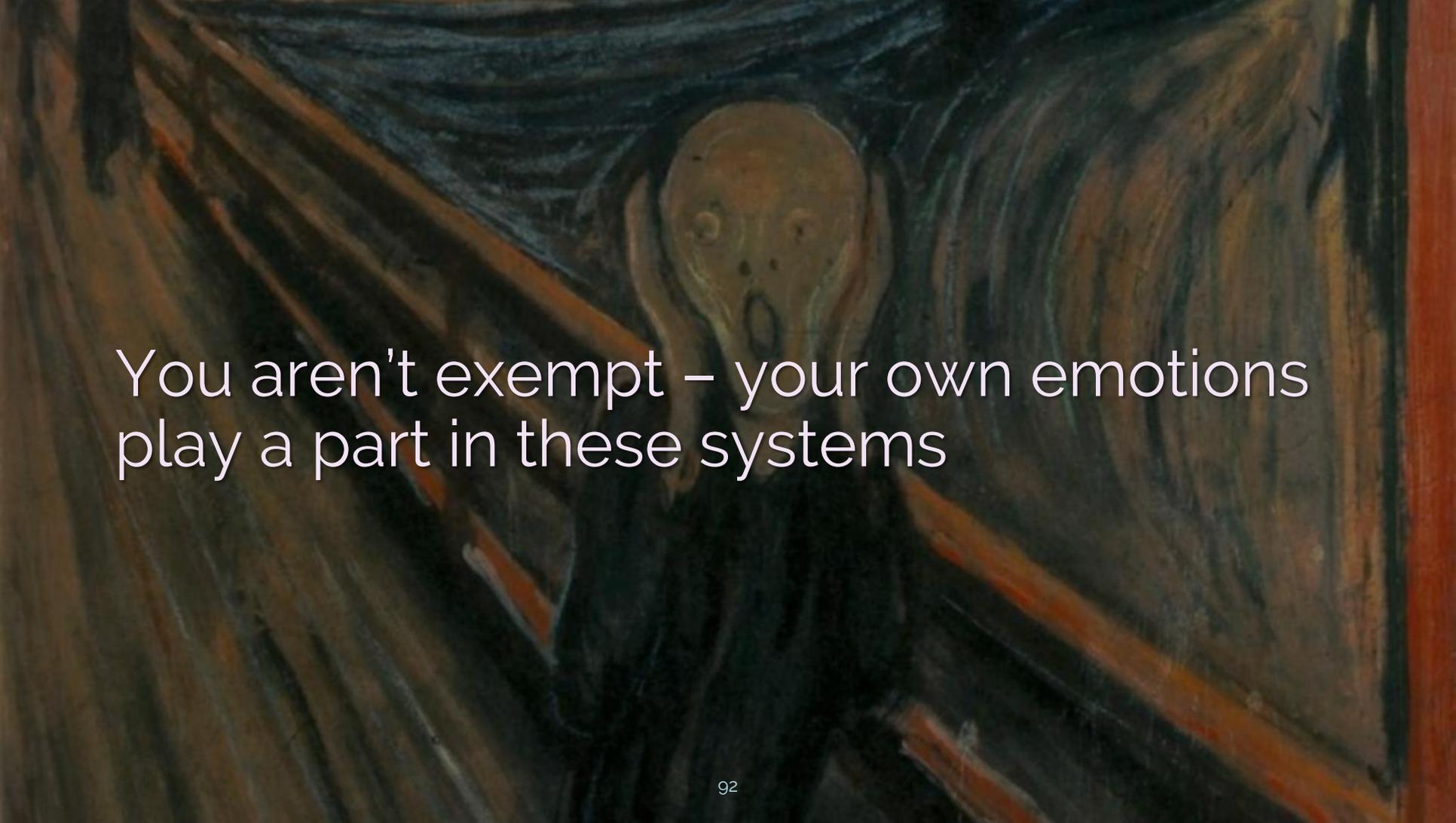
In Conclusion



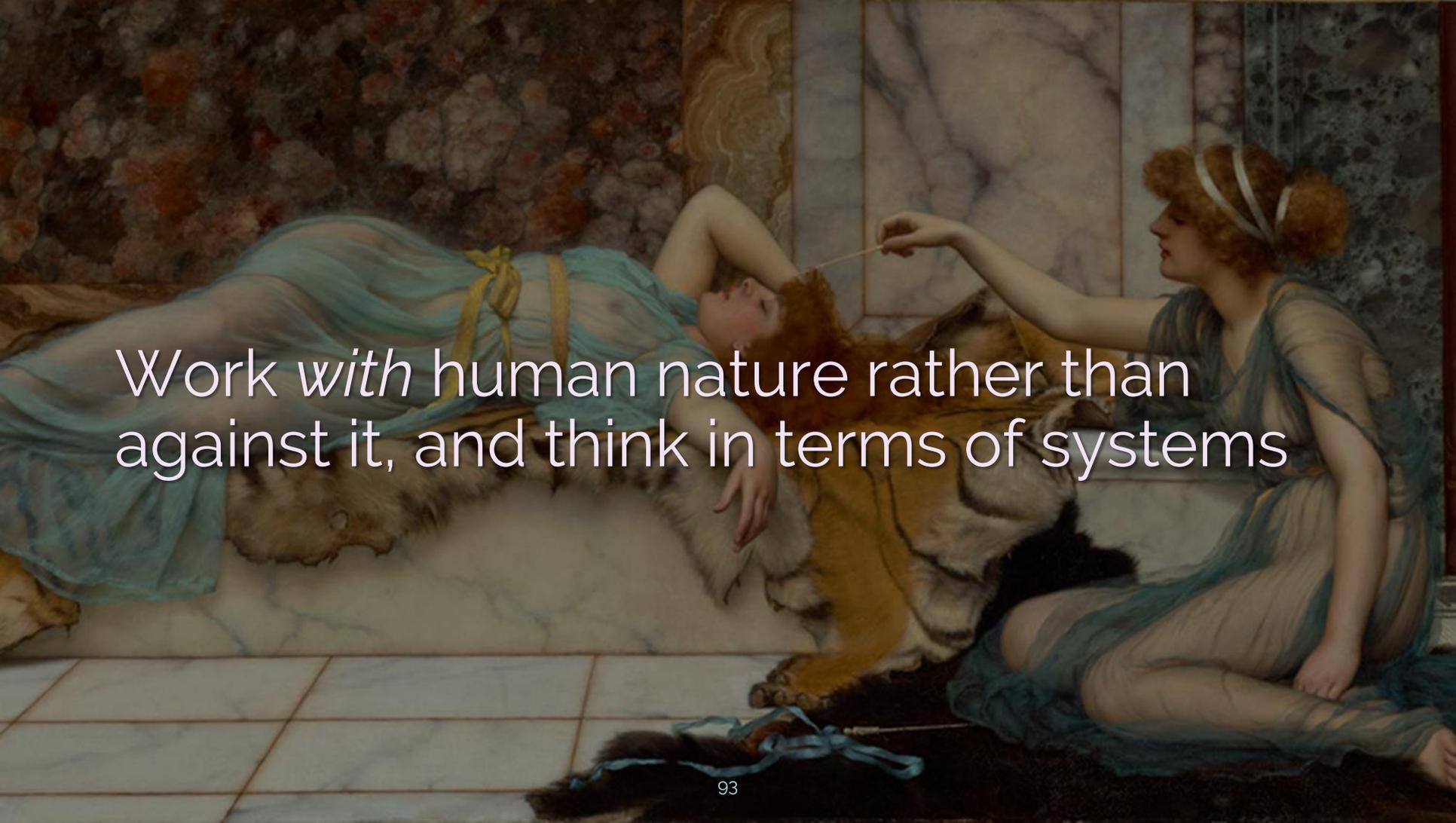
Discard the crutch of “human error” so
you can learn from failure



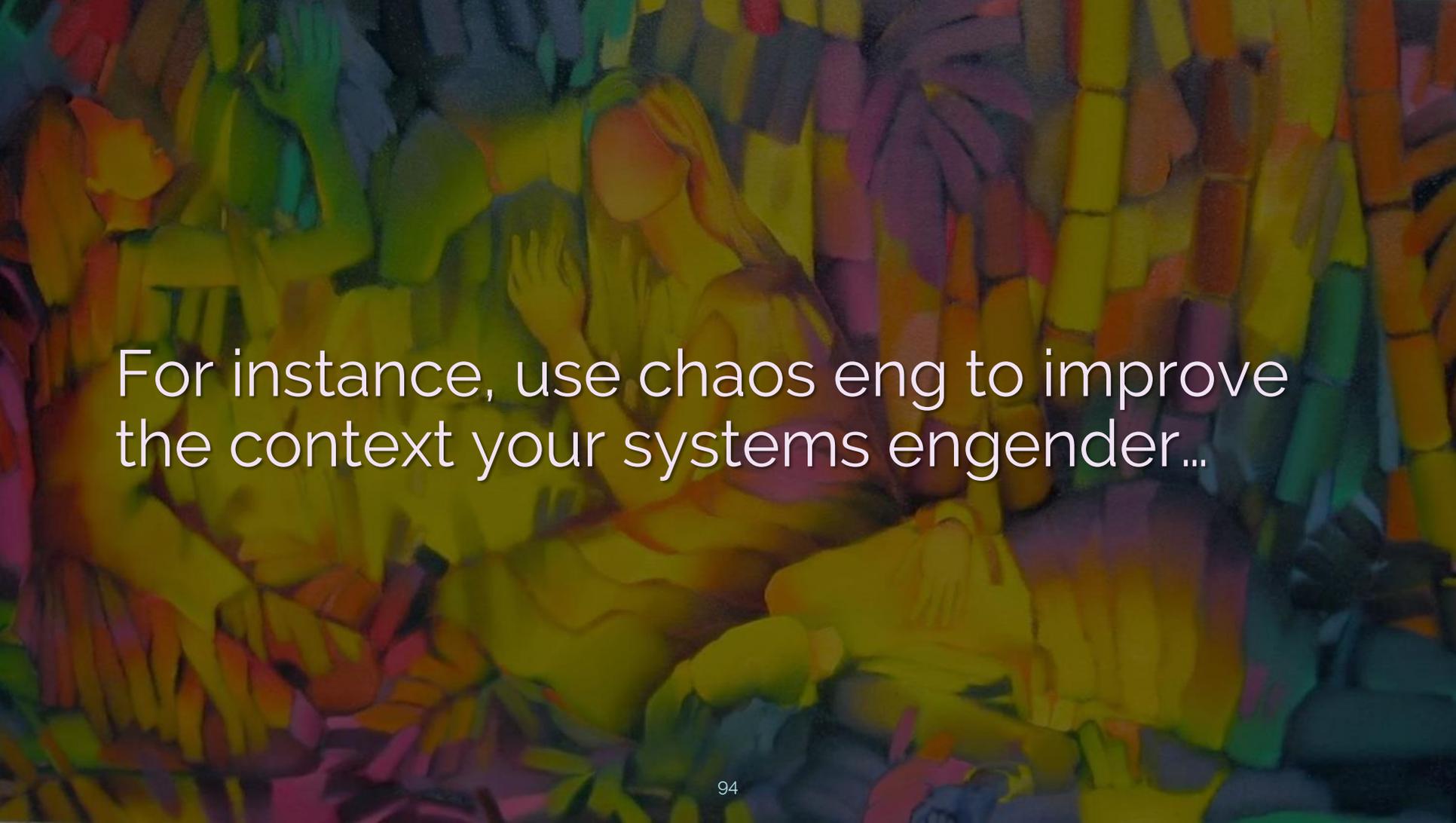
Always consider the messiness of
systems, organizations, and minds

The background of the slide is a reproduction of the painting 'The Scream' by Edvard Munch. It depicts a figure in the center, likely the artist, holding their head in their hands, surrounded by other figures in a turbulent, dark, and swirling environment. The overall mood is one of intense emotional distress and mental anguish.

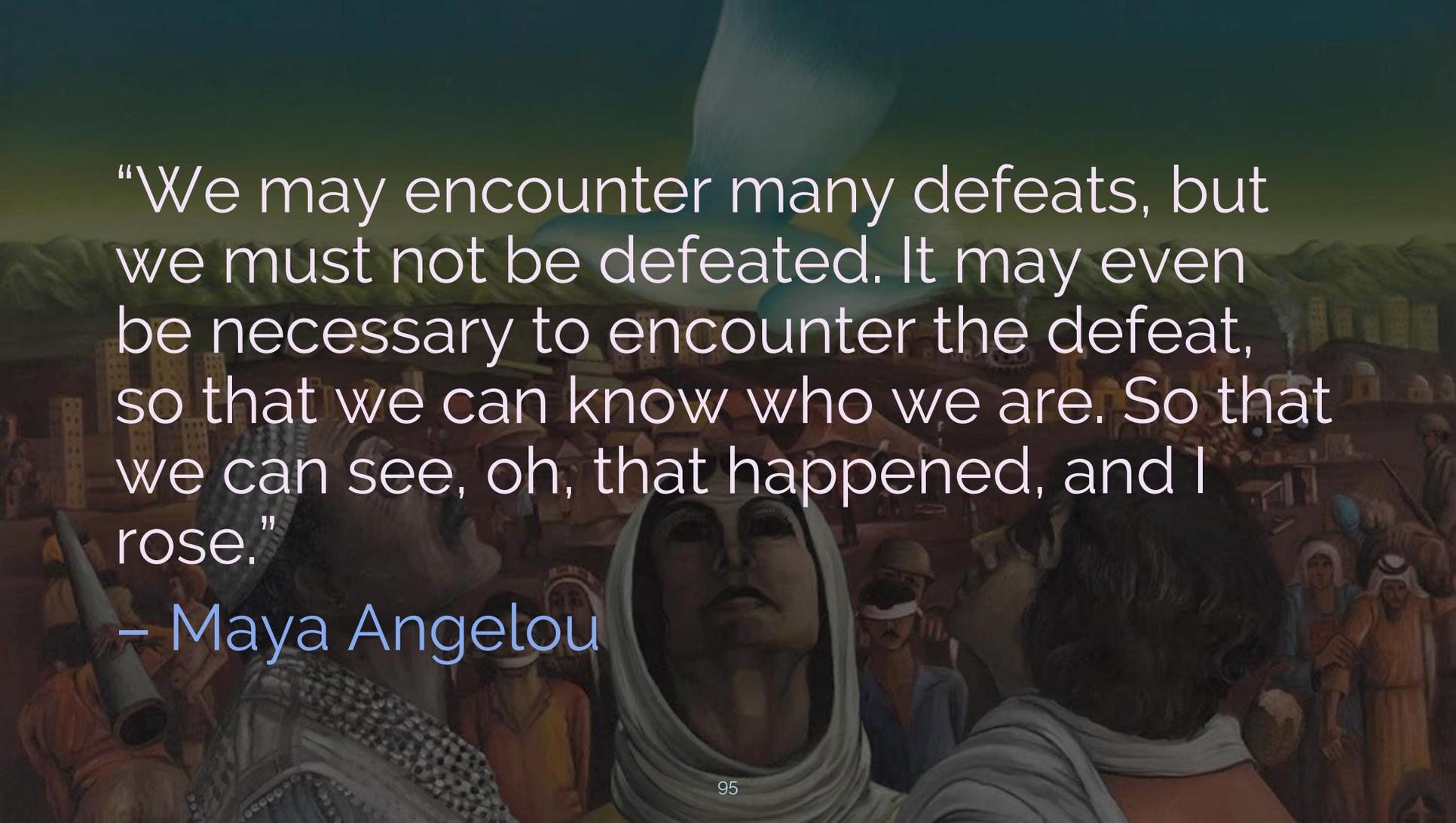
You aren't exempt – your own emotions
play a part in these systems

A classical painting depicting a woman in a blue dress lying on a lion's skin, while another woman in a blue dress sits on the floor, holding a small object towards the lion's head. The scene is set in a room with marble walls and a tiled floor. The woman lying down is wearing a light blue dress with a yellow sash. The woman sitting is wearing a darker blue dress with a white headband. The lion's skin is spread out on the floor, and the woman sitting is holding a small object, possibly a bone or a piece of food, towards the lion's head. The overall mood is one of domestication and control over nature.

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



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

A painting depicting a dense crowd of people in a city. In the foreground, a woman wearing a white headscarf looks upwards with a determined expression. To her left, another woman is seen from the side, holding a large, light-colored conical object. The background is filled with many other figures, some wearing head coverings, and buildings under a hazy, greenish sky. The overall mood is one of collective struggle or hope.

“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.