RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **HUM-T02**

How Behavioral Economics Can Help Make Better Security Decisions

Kelly Shortridge
Senior Principal Product Technologist
Fastly
@swagitda_

Sounil Yu
CISO & Head of Research
JupiterOne
@sounilyu

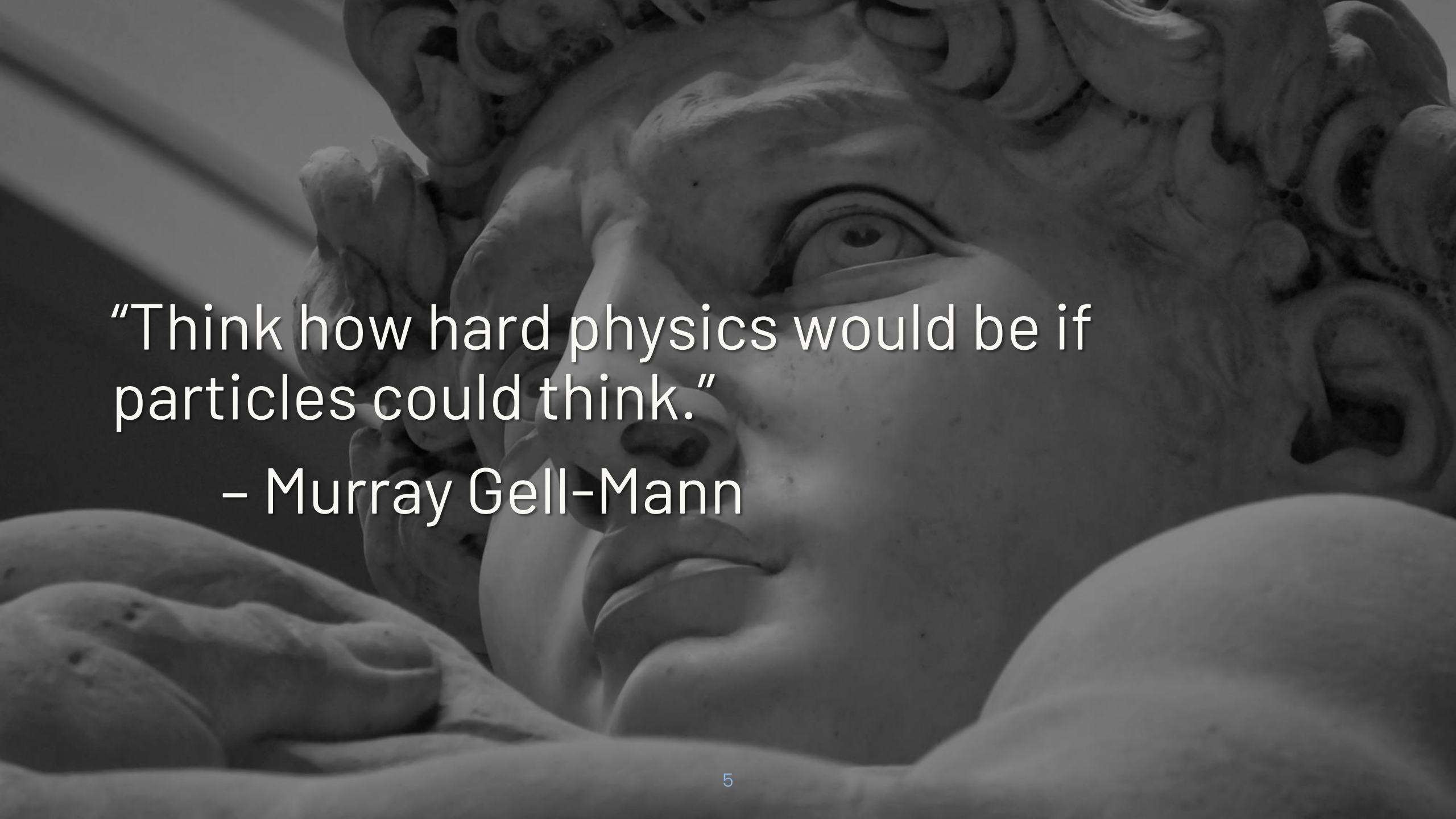
Disclaimer

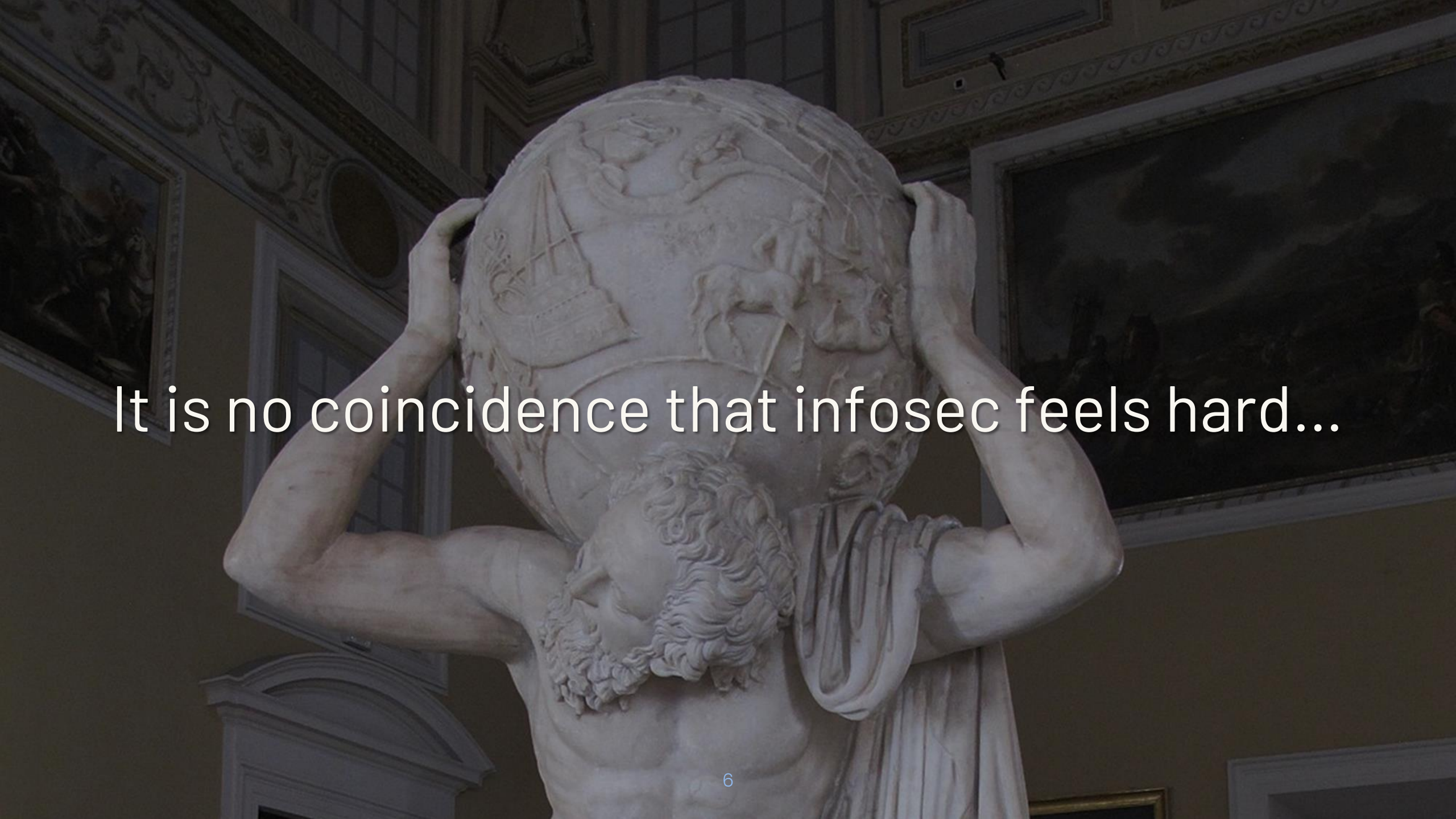
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

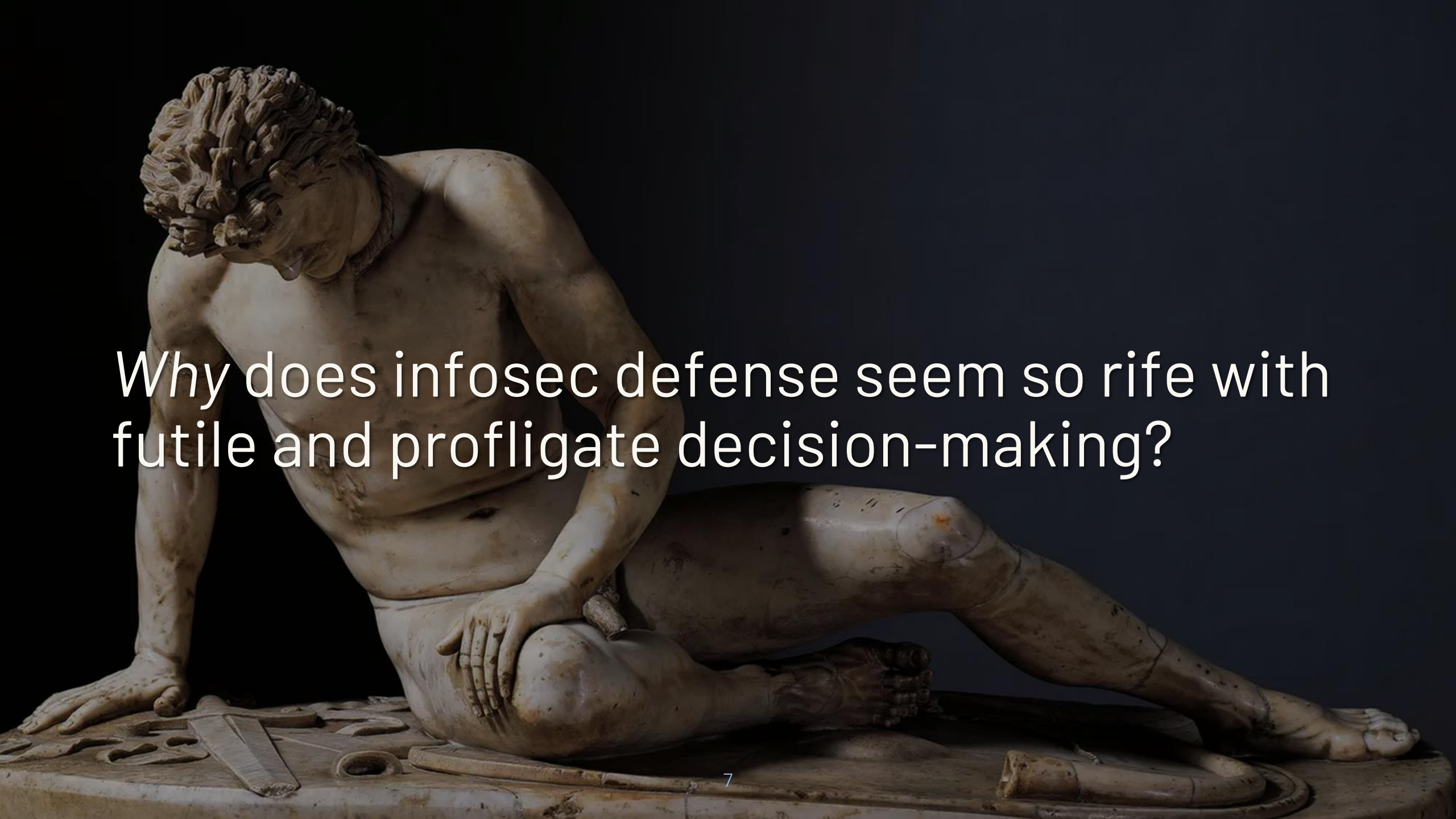
Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

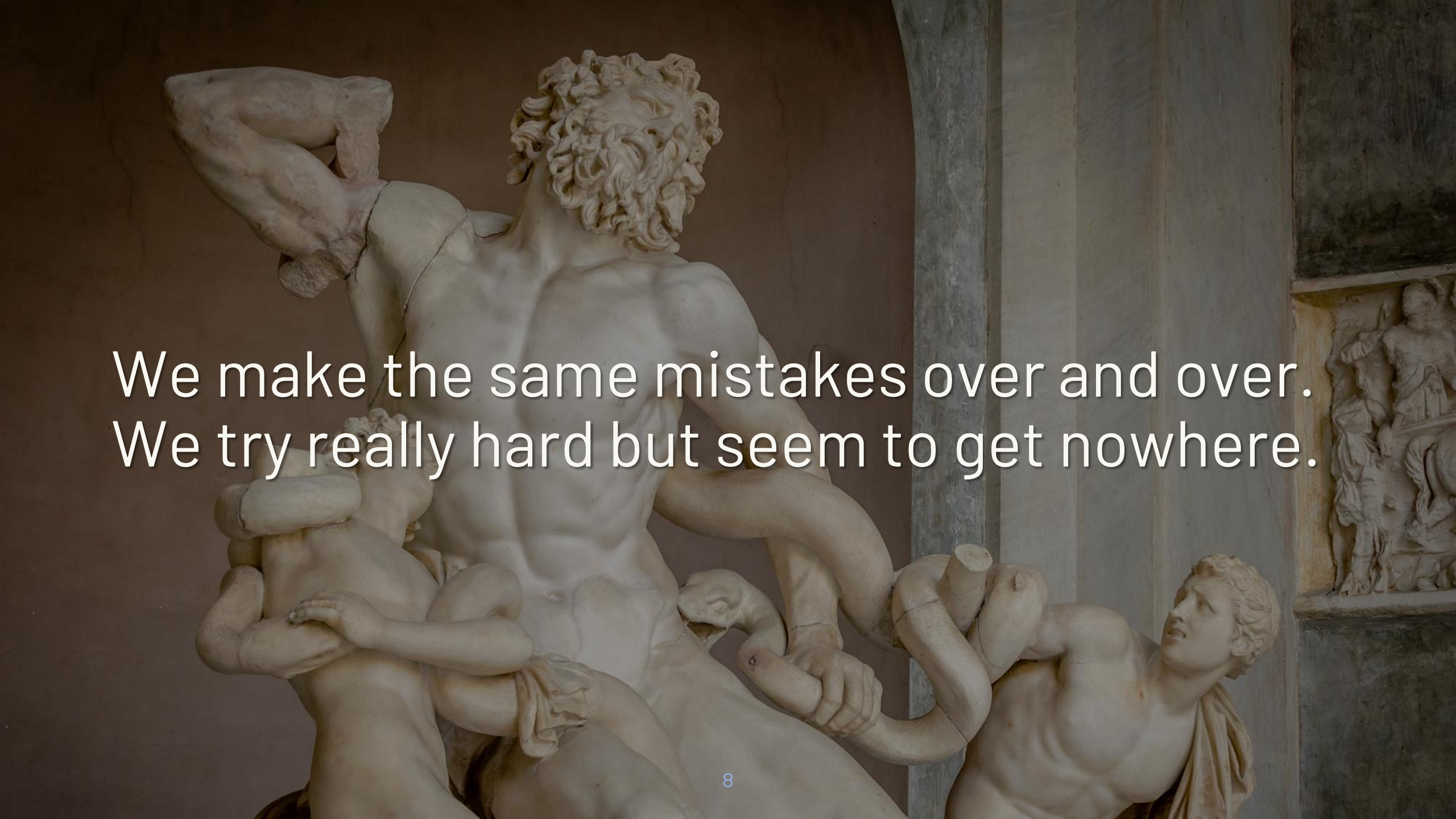

Hi, I'm Kelly
fastly


Hi, I’m Sounil
JupiterOne

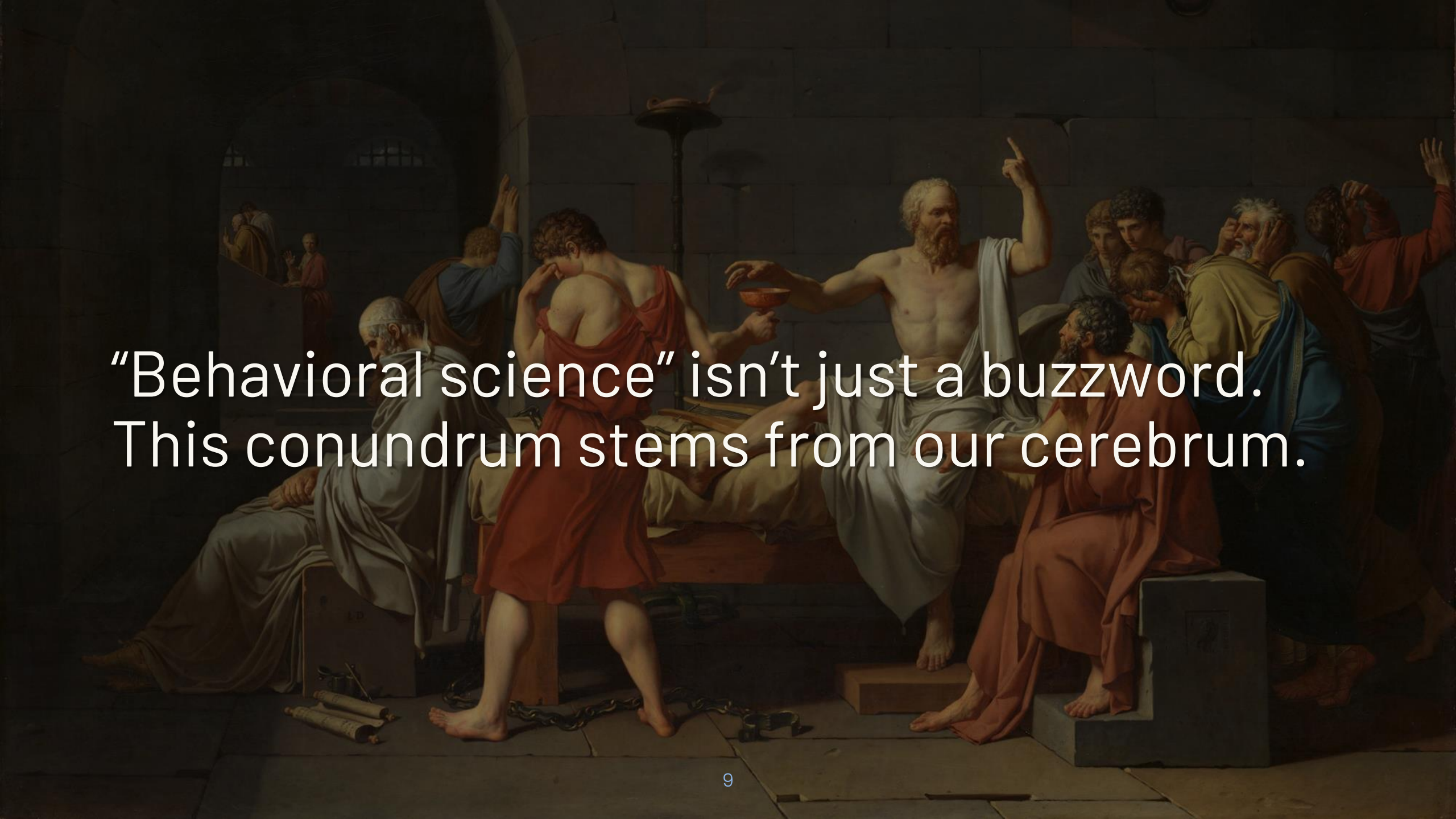

“Think how hard physics would be if particles could think.”
– Murray Gell-Mann


It is no coincidence that infosec feels hard...

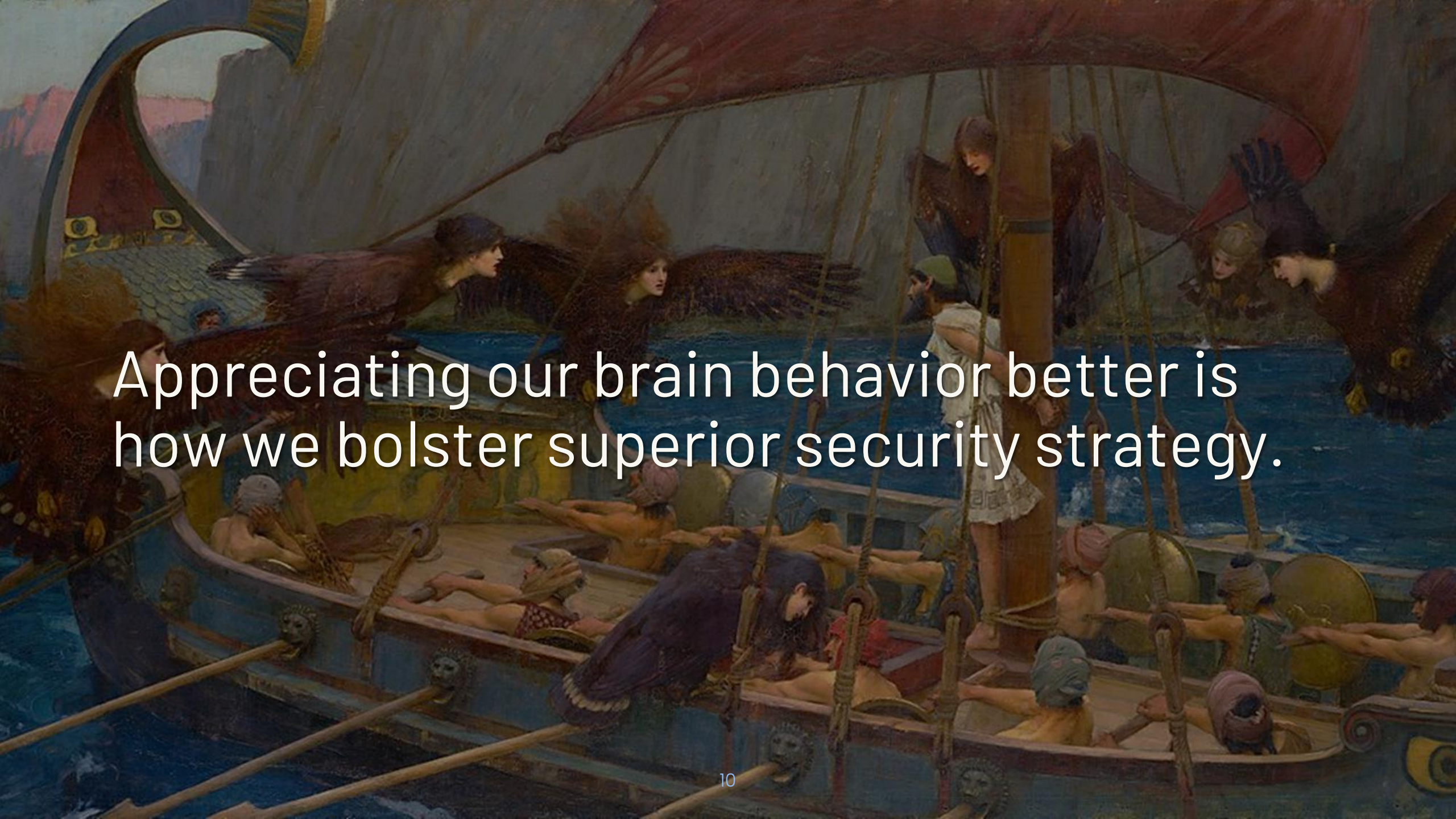

Why does infosec defense seem so rife with futile and profligate decision-making?



We make the same mistakes over and over.
We try really hard but seem to get nowhere.



“Behavioral science” isn’t just a buzzword.
This conundrum stems from our cerebrum.



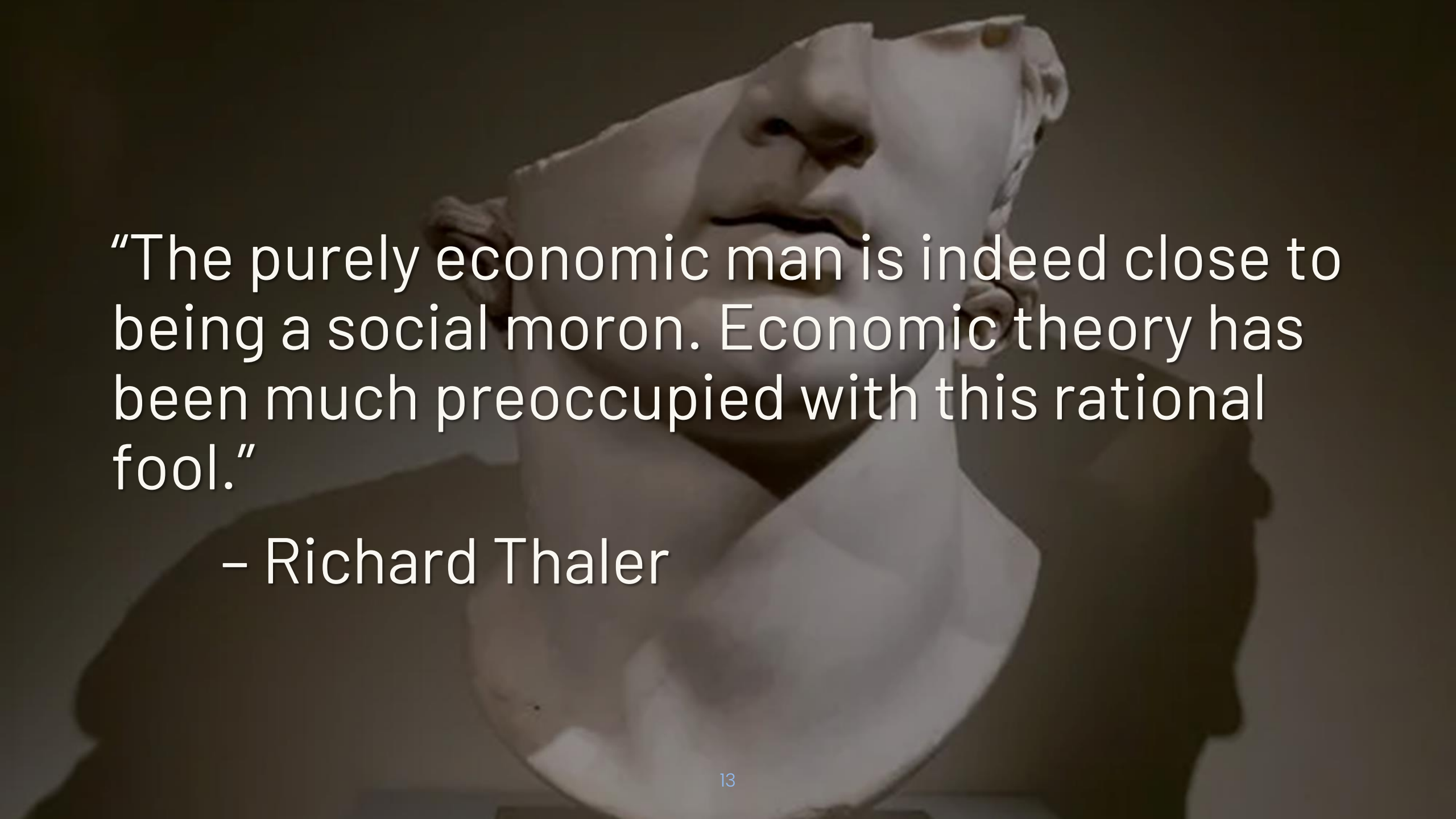
Appreciating our brain behavior better is how we bolster superior security strategy.

I. How do our brains work?

II. Lizard Brain vs. Philosoraptor

III. Making better decisions

I. How do our brains work?



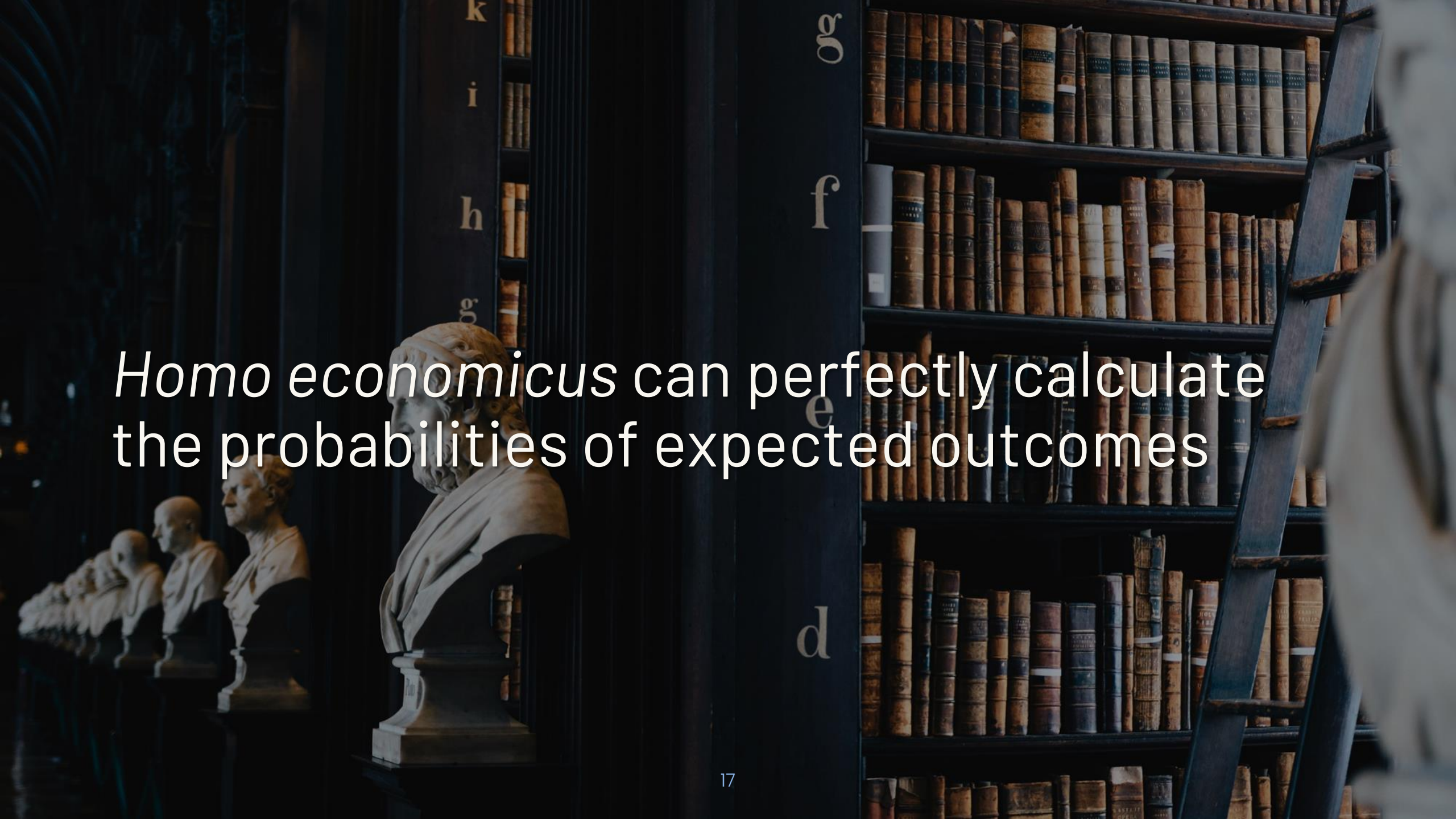
“The purely economic man is indeed close to being a social moron. Economic theory has been much preoccupied with this rational fool.”

– Richard Thaler

So, what do we mean by rationality here?

Behavioral economics studies how people *actually* make decisions vs. classical theory

In theory, every human makes choices to maximize their payoff (expected “utility”)



Homo economicus can perfectly calculate the probabilities of expected outcomes

In reality, information, attention, and time are all limited. Our rationality is “bounded.”

Every human (even you!) is only *locally* rational — *global* rationality is a fantasy.

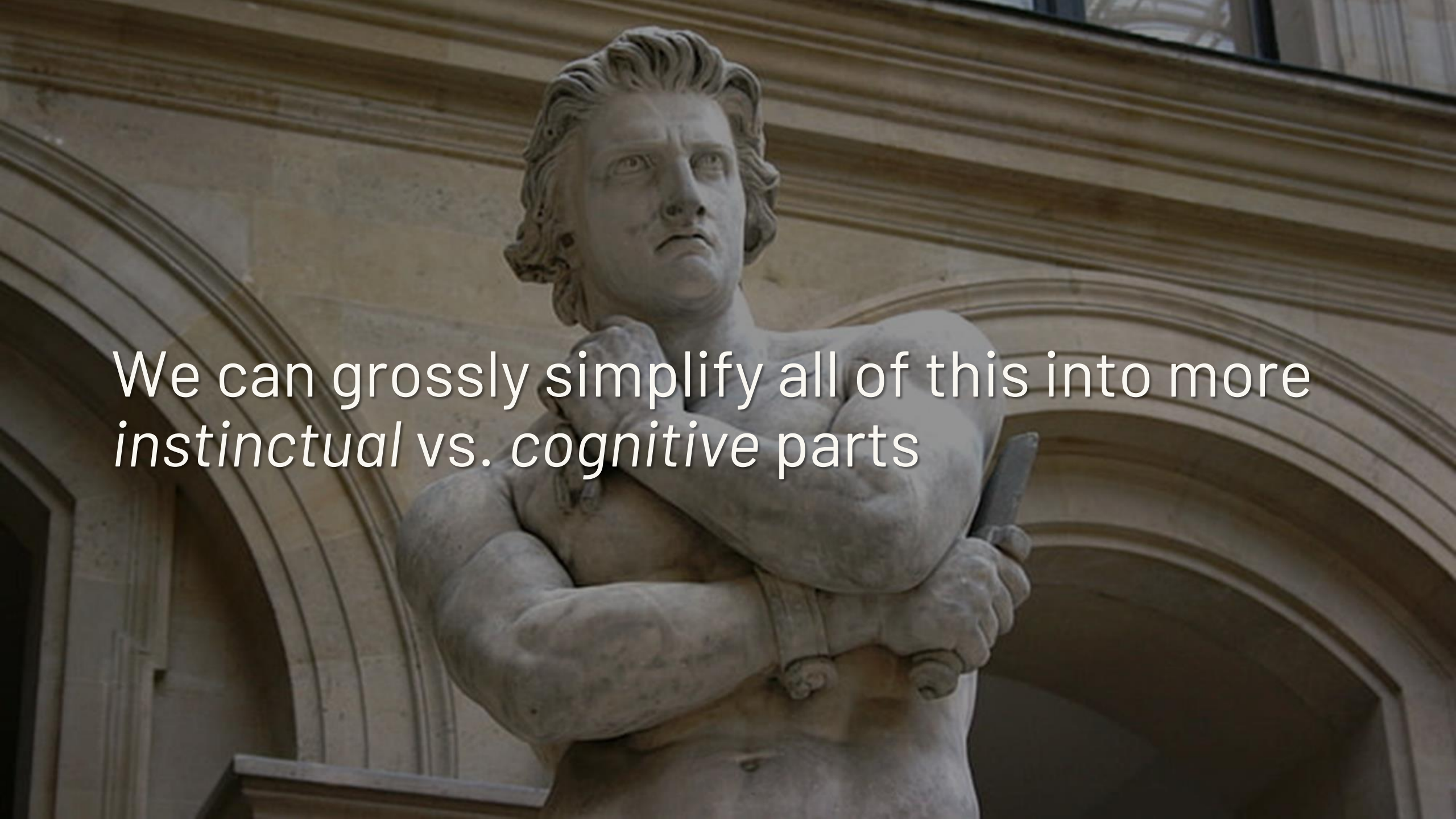
Spoiler: a *lot* of “human error” is a violation of what’s considered “globally” rational…

Understanding how our behavior deviates from *Homo economicus* matters for infosec


Evolution designed our brains for efficiency,
not for pure logic (or we'd die in the wild)

We were once very simple creatures with very simple functions (eat food! run away!)

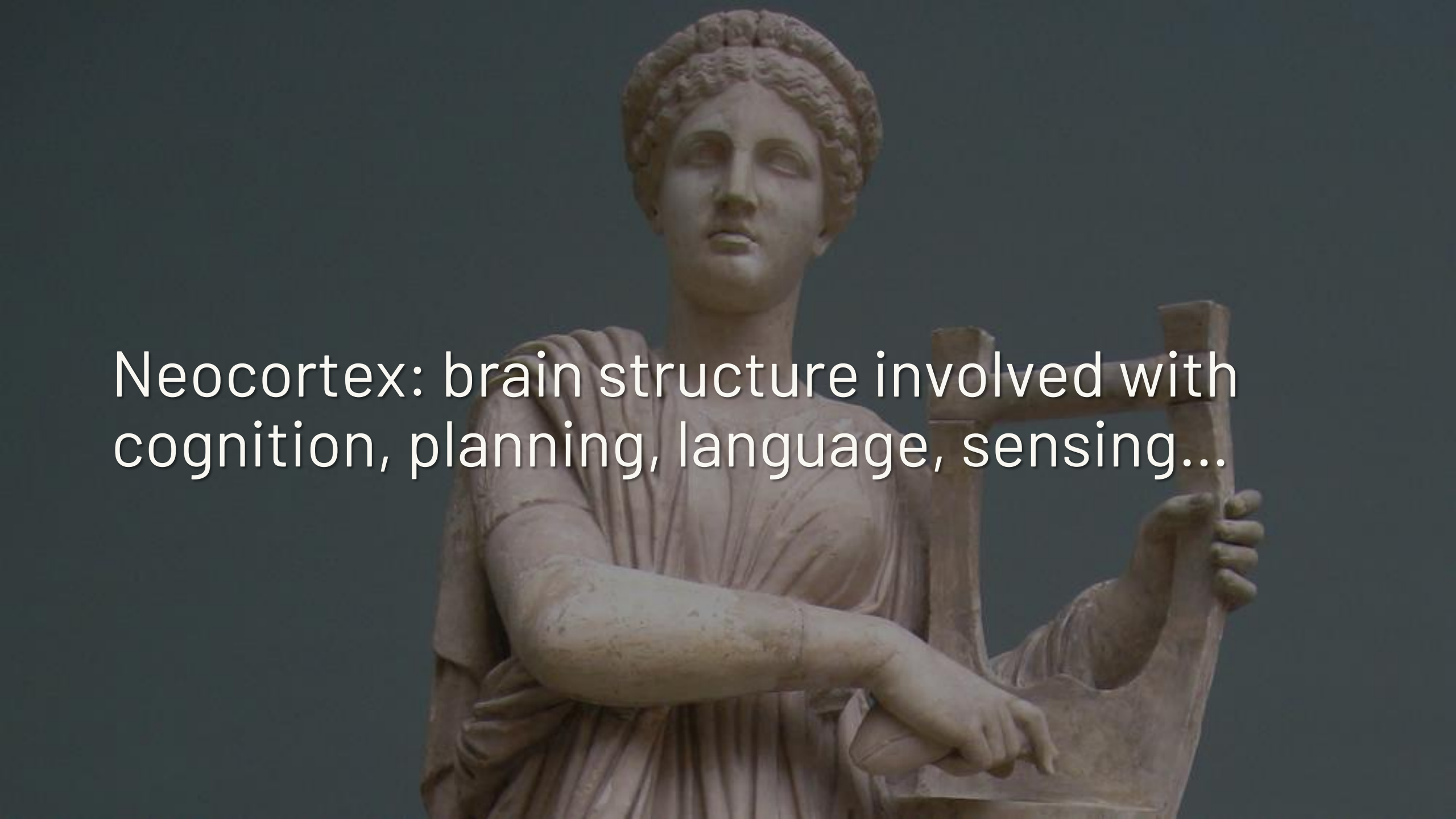

Then we evolved more complex processing
(gossip with tribe! envision the future!)


We can grossly simplify all of this into more
instinctual vs. *cognitive* parts

Our ability to imagine the future – and our future selves – is the most recently evolved


Protoreptilian brain: self-regulate biological functions to maintain stability for survival

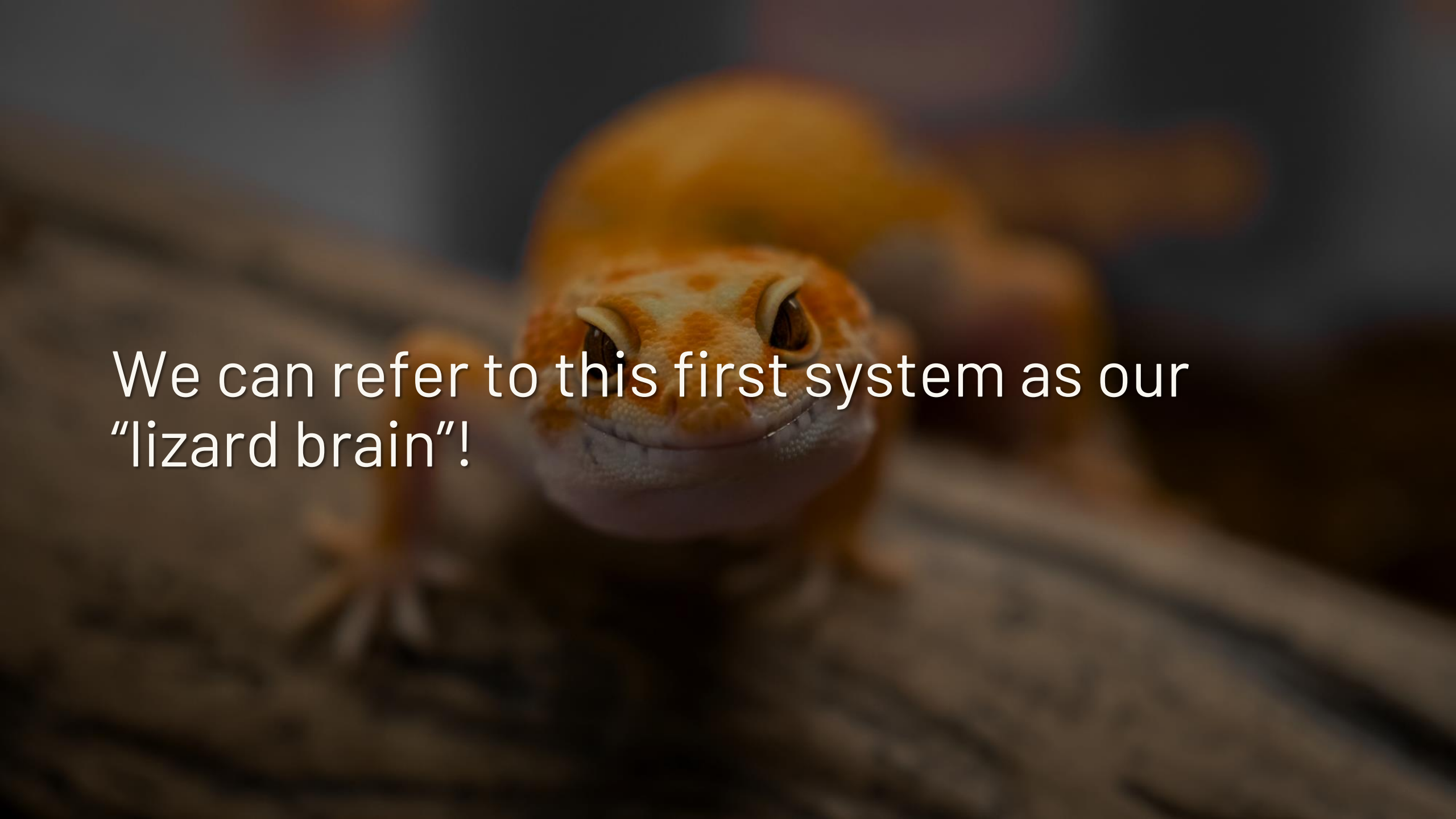
Limbic system: brain structures involved with survival behaviors (fight, feed, f...)

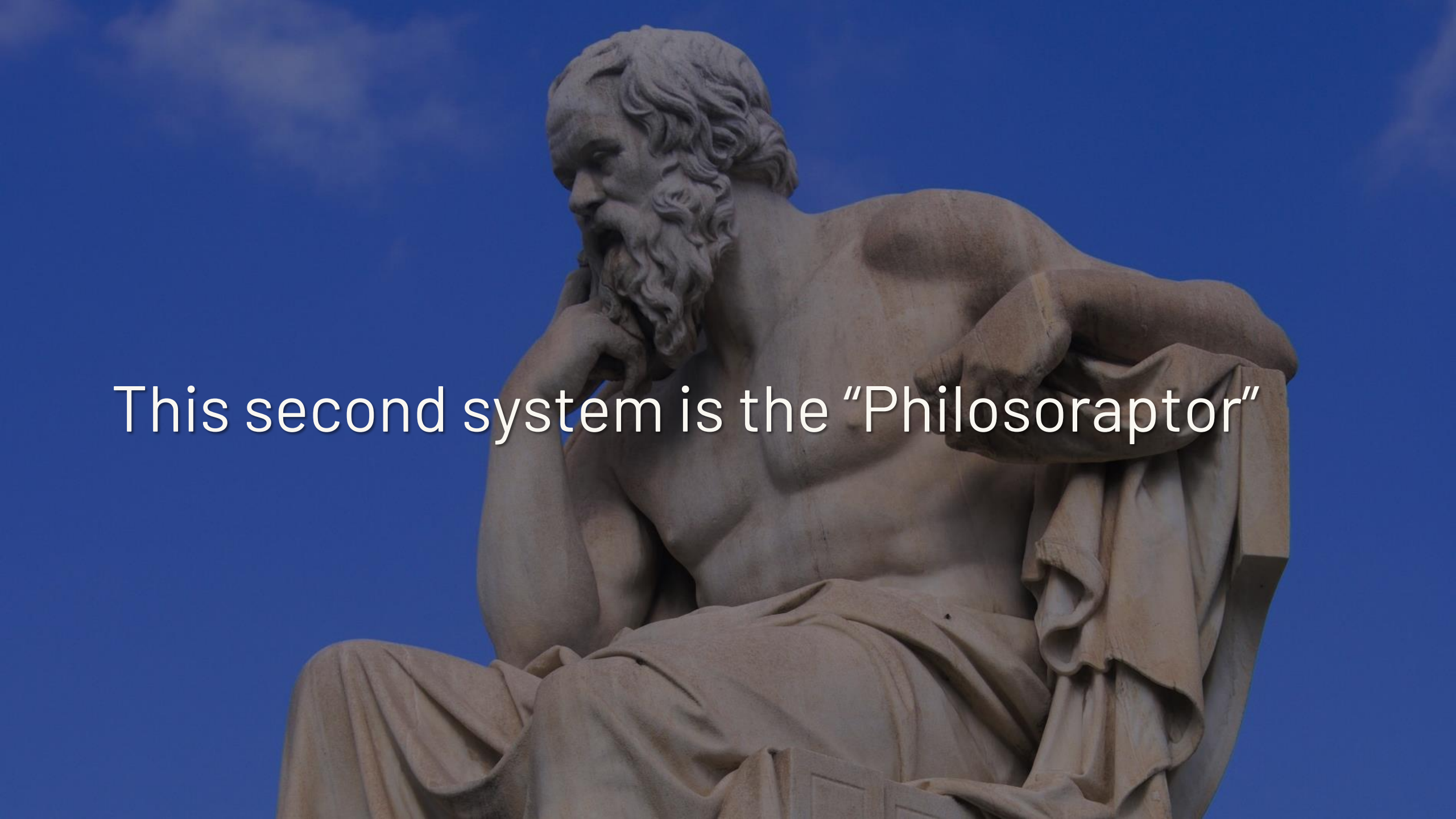

Neocortex: brain structure involved with cognition, planning, language, sensing...

But we usually simplify our brains into two systems for thinking: System 1 & System 2

System 1 = quick, automatic, unconscious; wants fast, easy, simple thinky thinky

System 2 = effortful thinky thinky; cognition and purposeful choices vs. instincts


We can refer to this first system as our
“lizard brain”!


This second system is the “Philosoraptor”

Lizard brain decides to stay up super late playing video games after a tough week.

Philosoraptor decides to go to bed early and have a refreshing workout in the morning.

As you might suspect, Lizard Brain and Philosoraptor disagree on infosec choices...

II. Lizard Brain vs. Philosoraptor

How do the Lizard Brain (LB) and Philosoraptor (PR) manifest in infosec?

LB: Heuristics, shortcuts, and folk wisdom

PR: Experimental evidence and analysis


LB: Vulns are predators! They threaten our survival! Eradicate them at all costs!

PR: Non-emotional framing of vulns, use of analogies, focus on impact vs. vague “risk”


LB: Success = no danger ever! Stay safe within the cave and never leave it

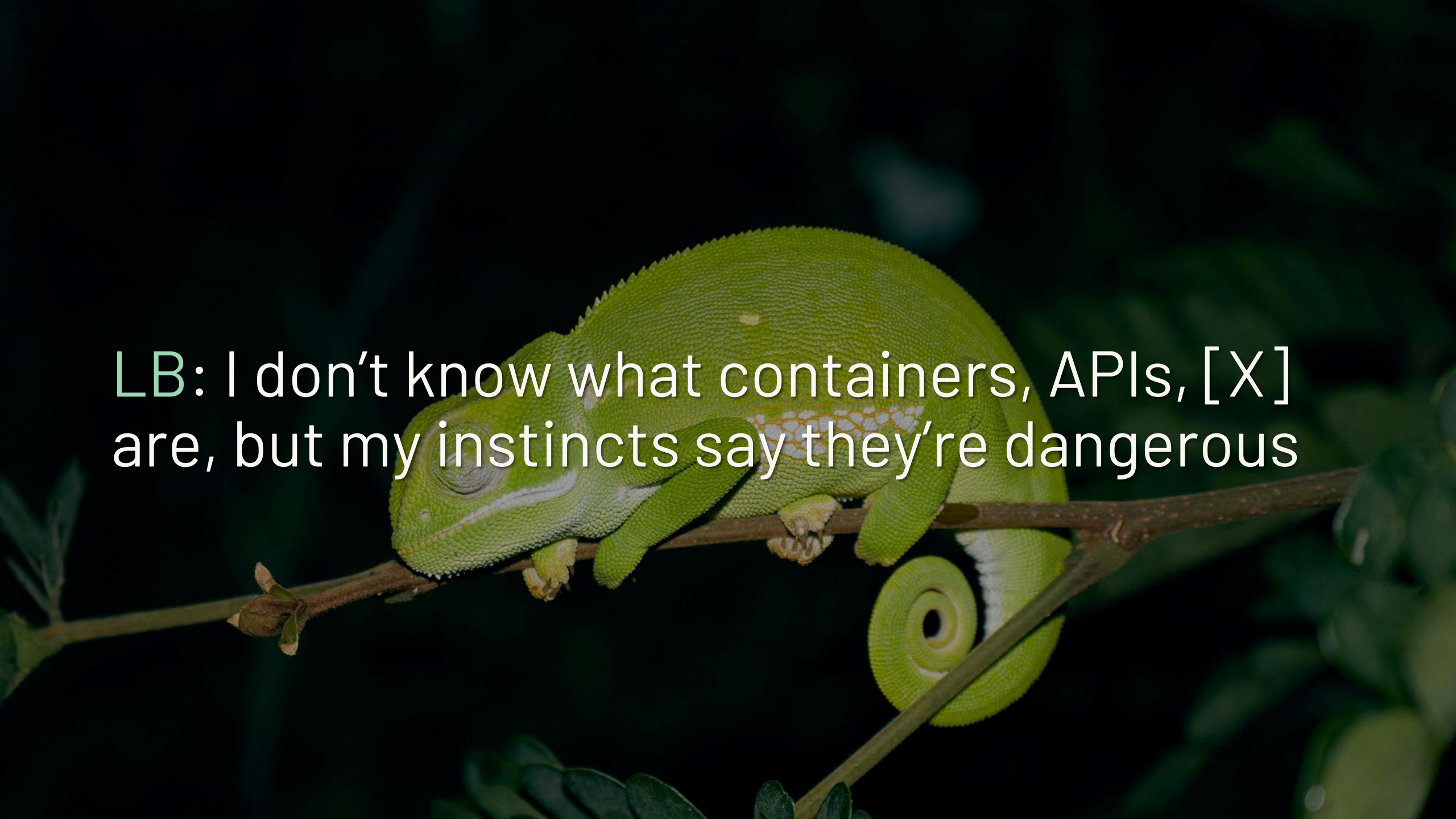
PR: Success = support adaptive cycles, enable sustainable growth and innovation


LB: Thoughtful metrics are hard; therefore, let’s use shallow ones for less thinky thinky

PR: Nuanced view of metrics that considers context and complexity of systems

LB: Tribal mindset – Gatekeeping other tribes, hoarding knowledge, bottlenecks

PR: Village mindset – neocortex brain seeks connection and collaboration to build things


LB: I don’t know what containers, APIs, [X]
are, but my instincts say they’re dangerous

PR: Seeks evidence, asks questions with an open mind, ponders new ways to do things

LB: Familiarity = importance. I've heard it a lot and can recall it easily, so it must be true.

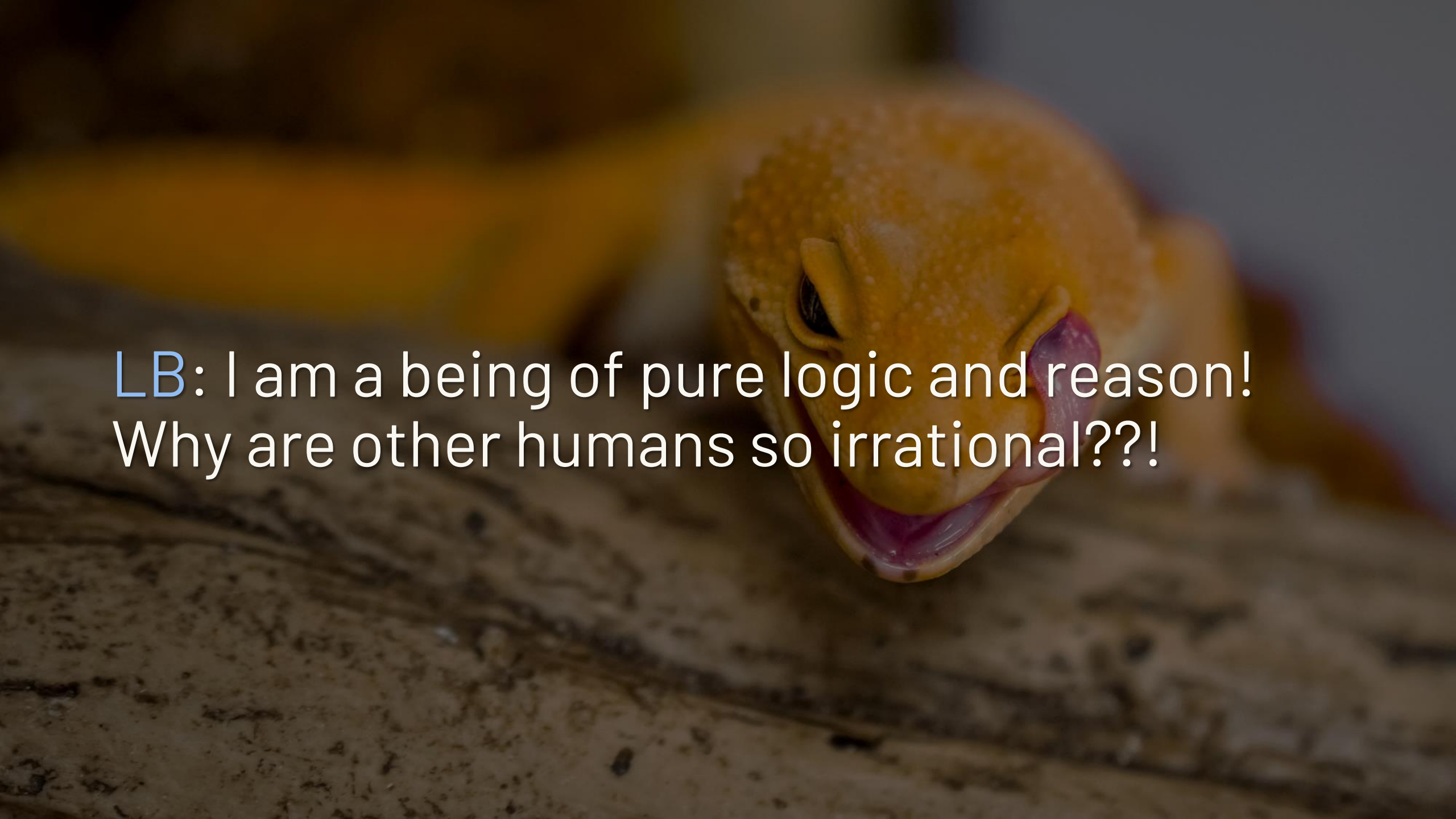
PR: Familiarity is successful marketing and doesn't indicate importance or truthfulness.


LB: Autonomic nervous system triggers
fight or flight response

PR: Rest and digest response – mindful handling of stress (psychological resilience)

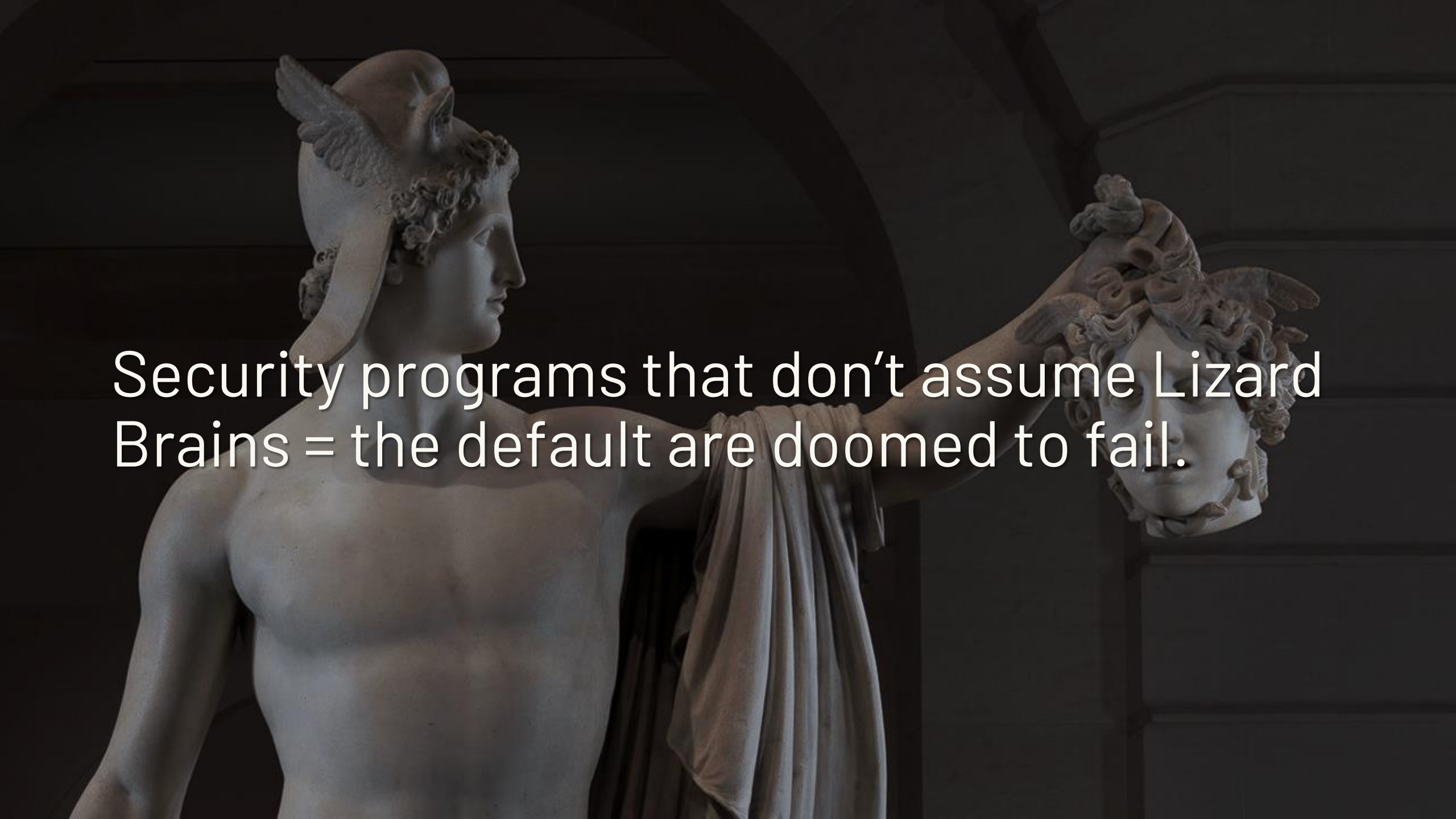

LB: Perfect prevention of failure is the way

PR: Nothing is perfect; what matters is preparing for recovery

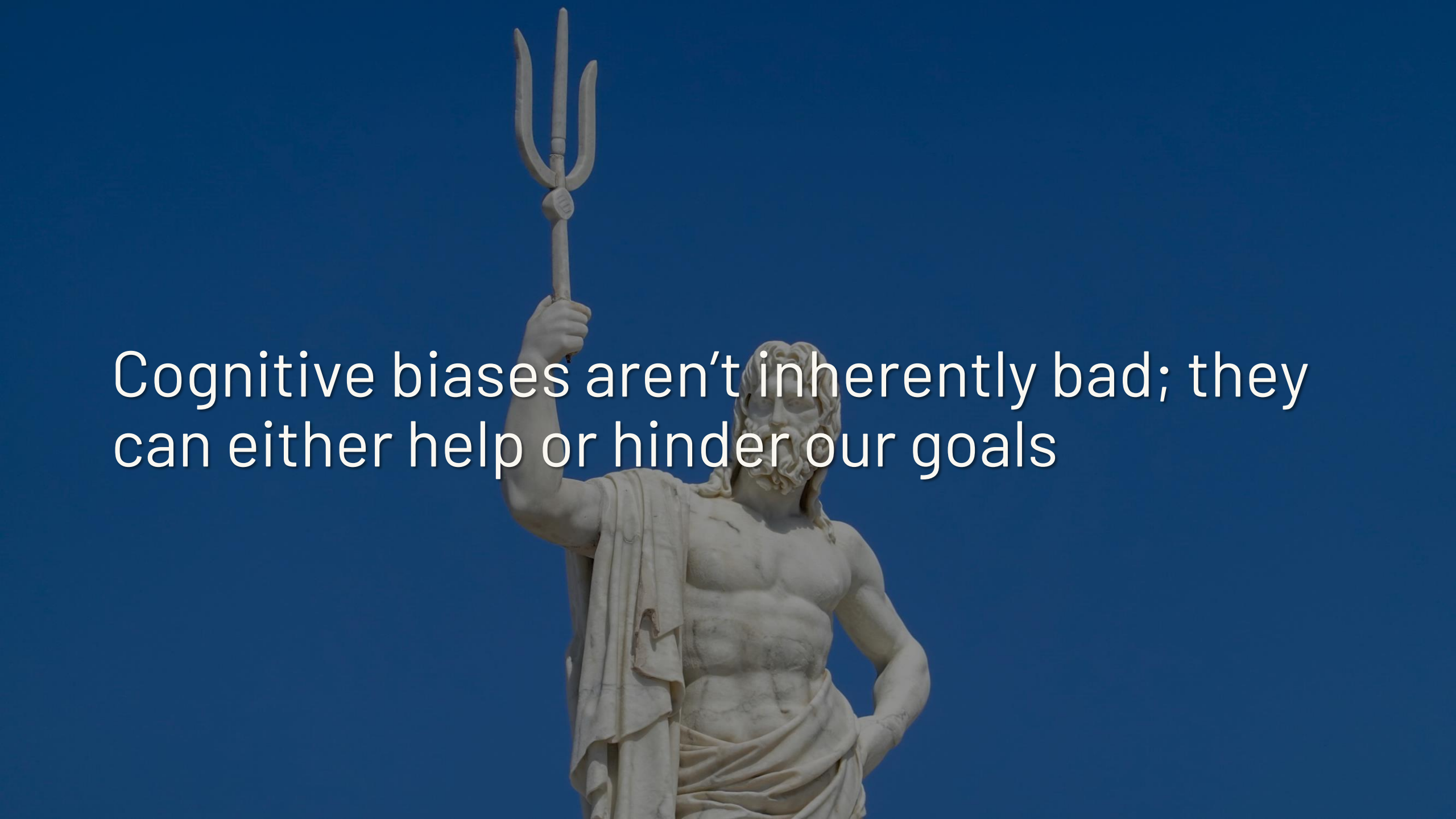

LB: I am a being of pure logic and reason!
Why are other humans so irrational??!

PR: Lizard brains are the default; we can't force humans to change their programming

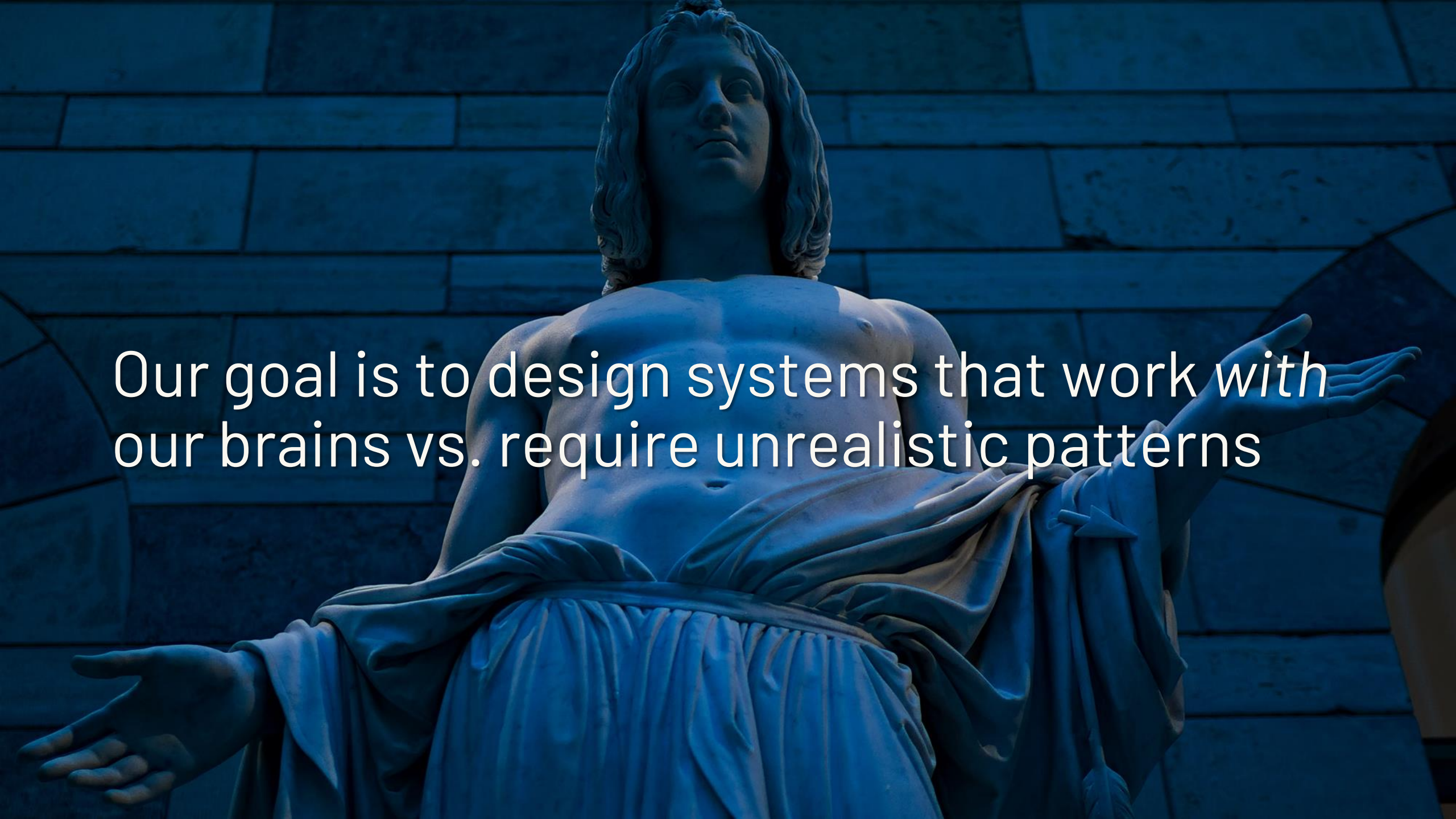
III. Making better decisions


Security programs that don’t assume Lizard Brains = the default are doomed to fail.

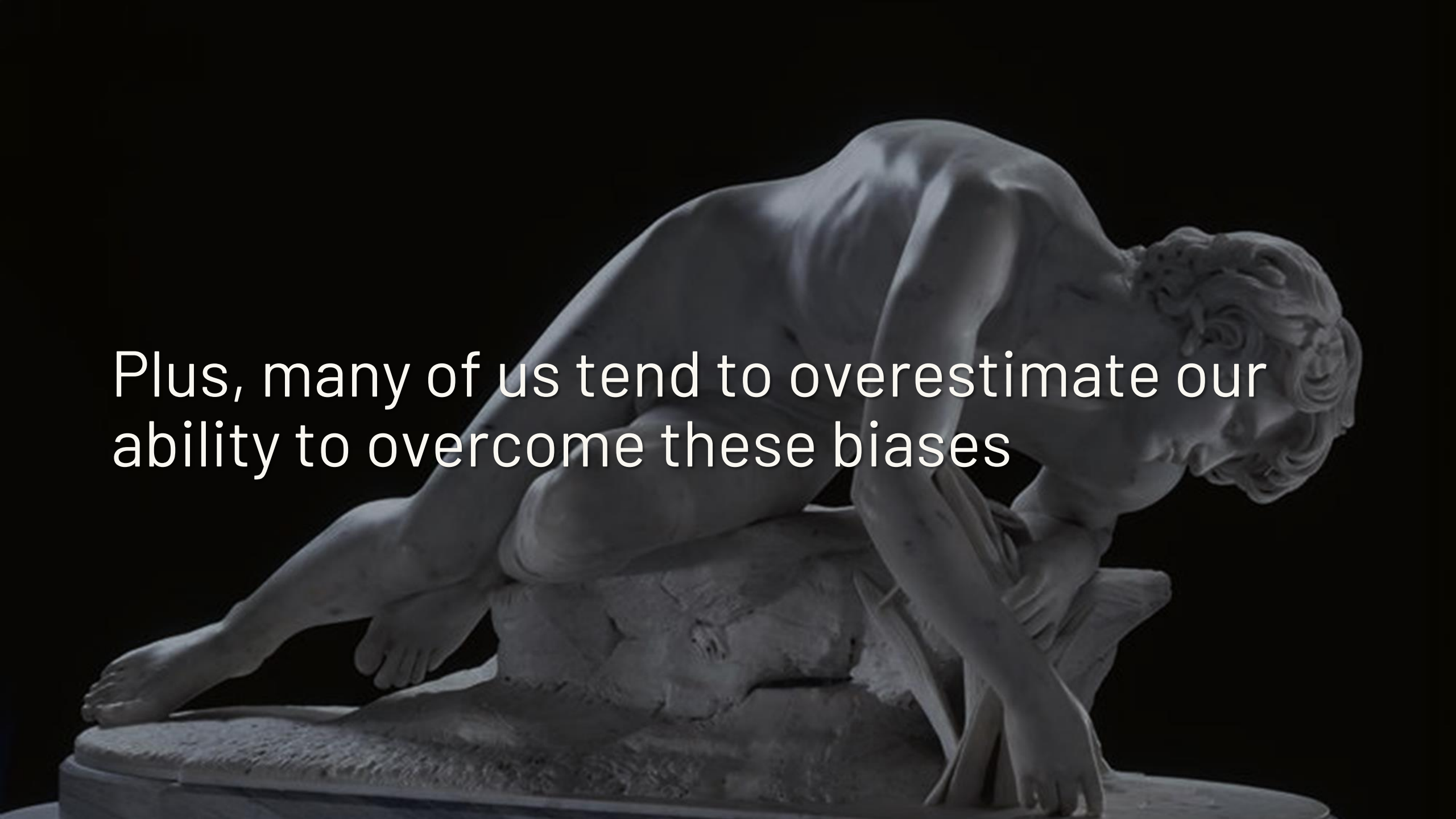
(And our Lizard Brains tell us that we really don’t want to fail!)


Cognitive biases aren’t inherently bad; they can either help or hinder our goals

Viewing instincts and emotions as “wrong” thinking will *also* distort decision-making


Our goal is to design systems that work *with* our brains vs. require unrealistic patterns

Being aware of cognitive bias isn't enough.
The human brain sucks at self-monitoring.


Plus, many of us tend to overestimate our ability to overcome these biases

(It’s still good to be on the lookout, so long as you remain aware you can be a fool, too)


We must make the “right way” compatible
with the lizard brain – simple, easy, fast

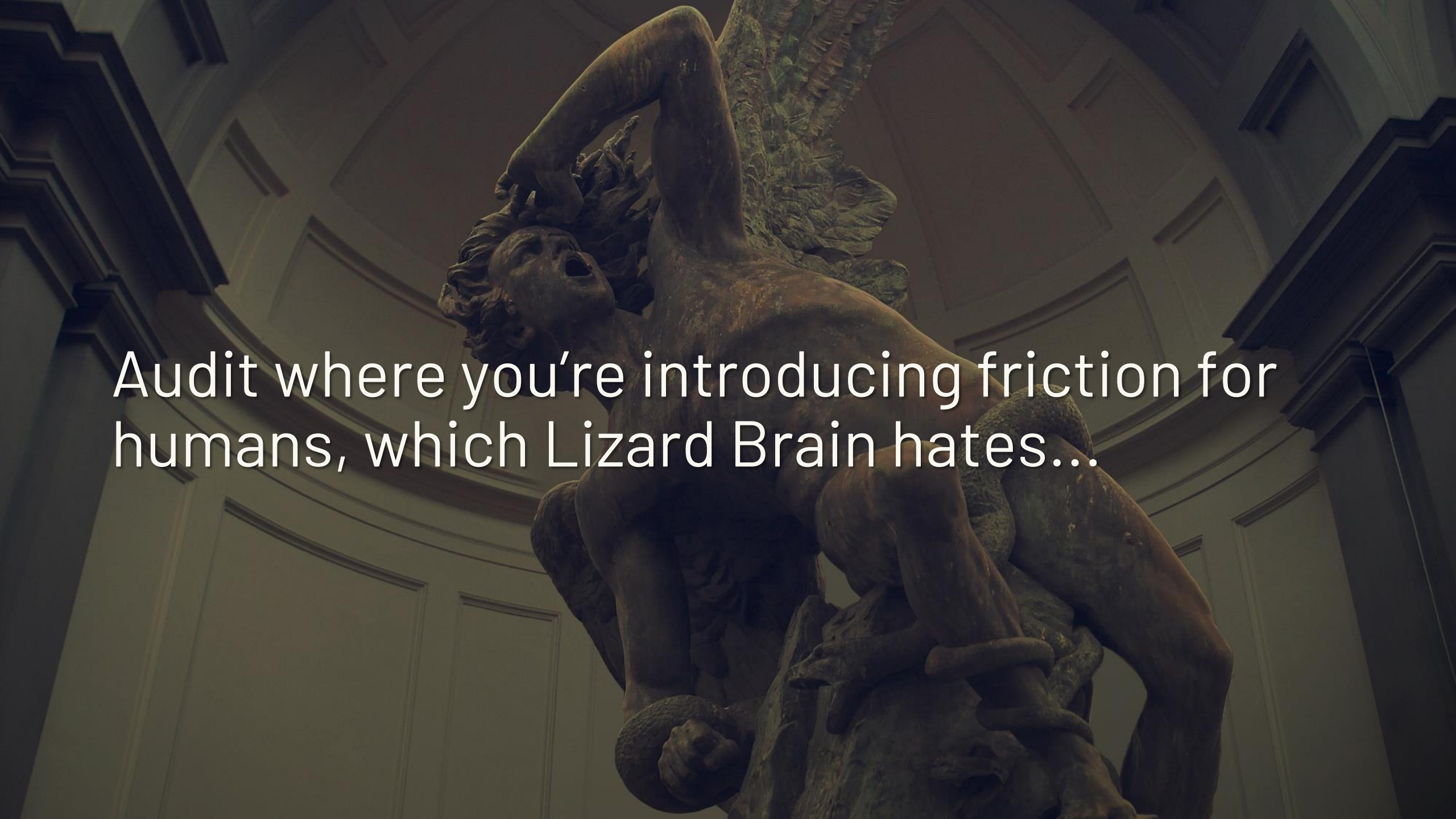
Repetition and practice turns tasks from Philosoraptor processes into LB instincts

But, repetition needs immediate feedback in order for it to satisfy the lizard brain

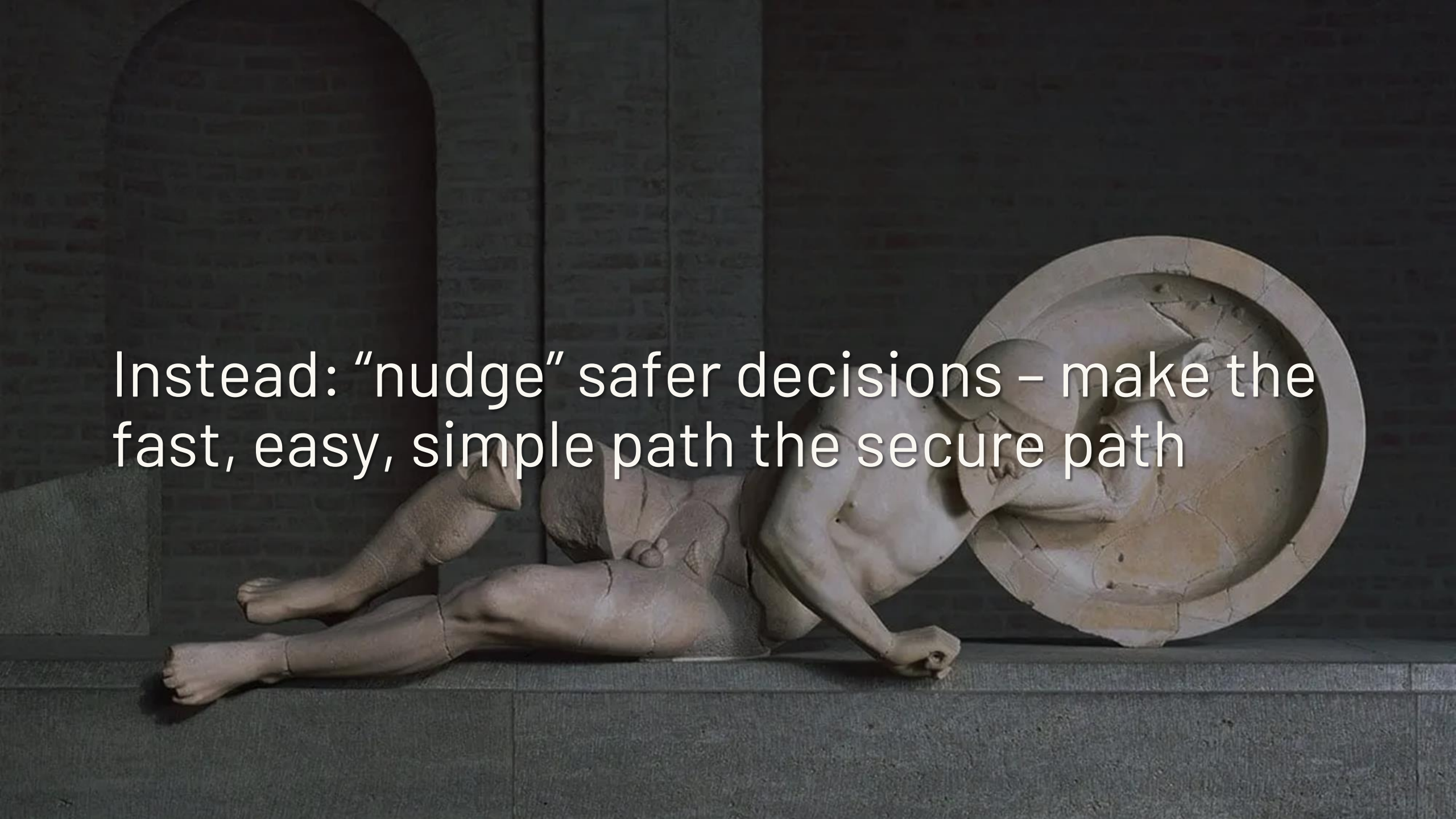
Exploit availability bias for good – ensure your messages are repeated and pithy

Create your own heuristics... just like we have with Lizard Brain vs. Philosoraptor :)

Opportunity cost consideration: the “null baseline” is a fast, easy, simple heuristic

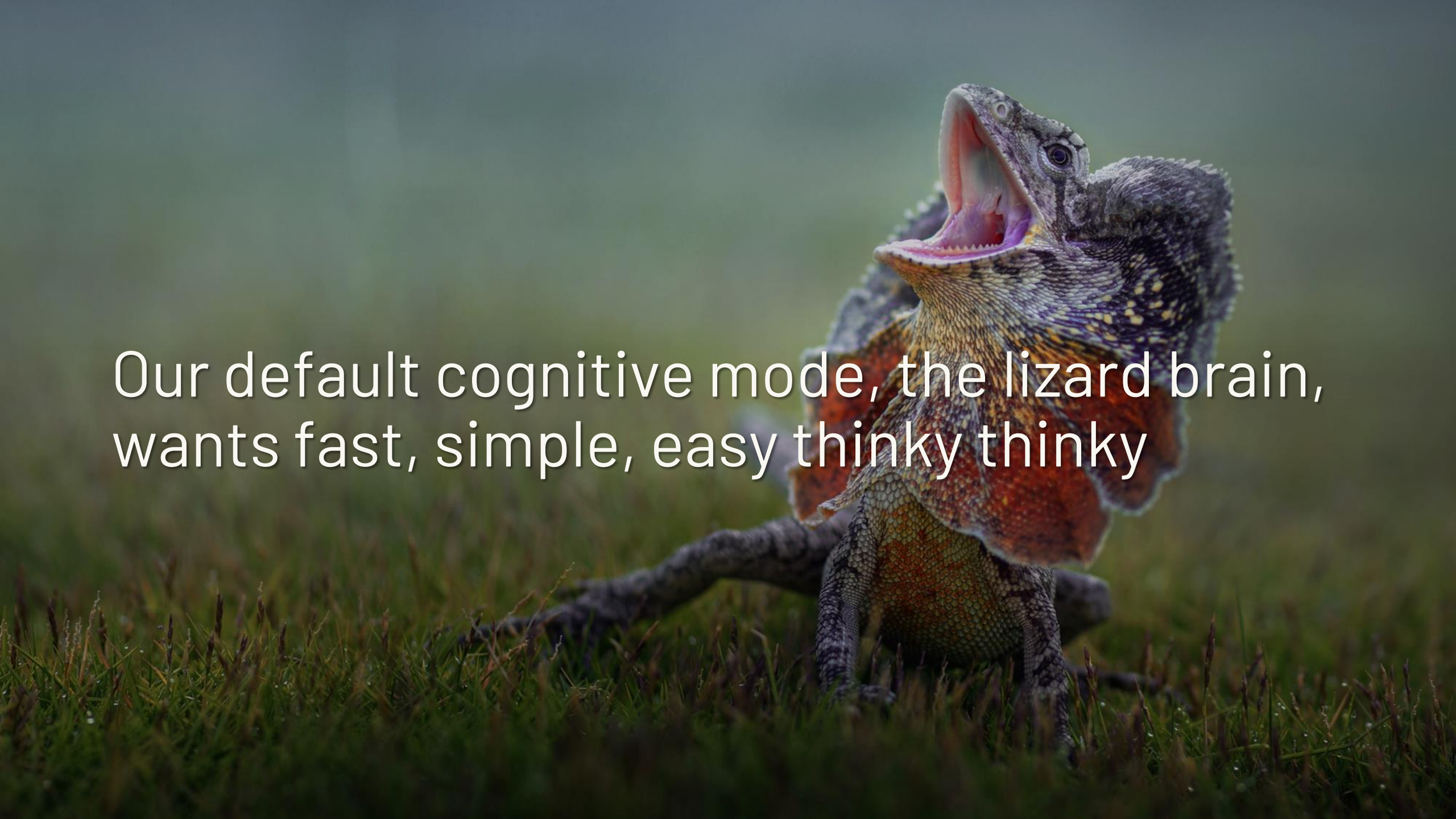

Audit where you’re introducing friction for humans, which Lizard Brain hates...

Per Richard Thaler: phishing warnings are “sludge”; it’s very natural to ignore them

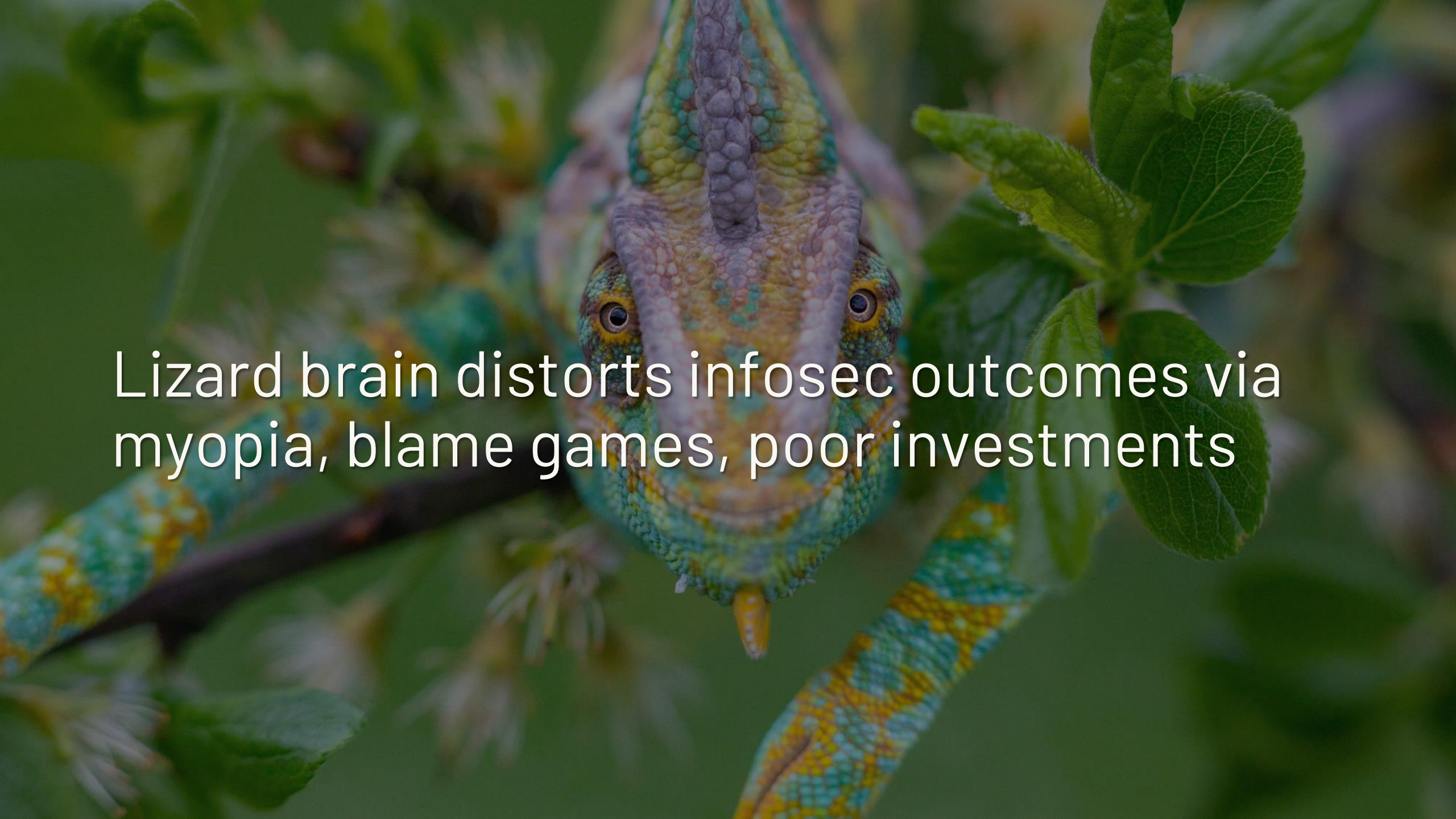

Instead: “nudge” safer decisions – make the fast, easy, simple path the secure path

Cognitive biases are chronic, not acute – so solutions must *manage* rather than "fix"

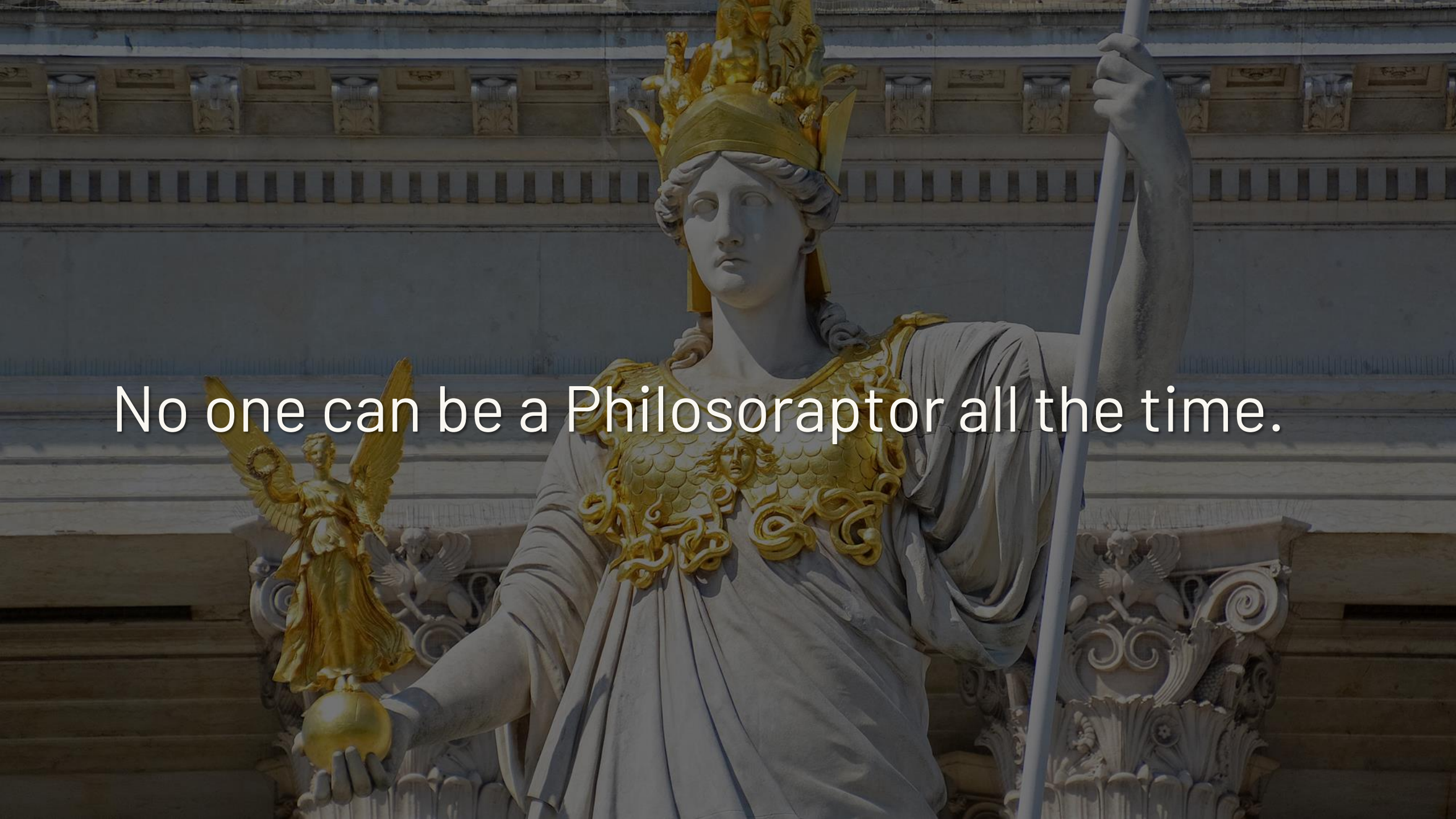
IV. Conclusion

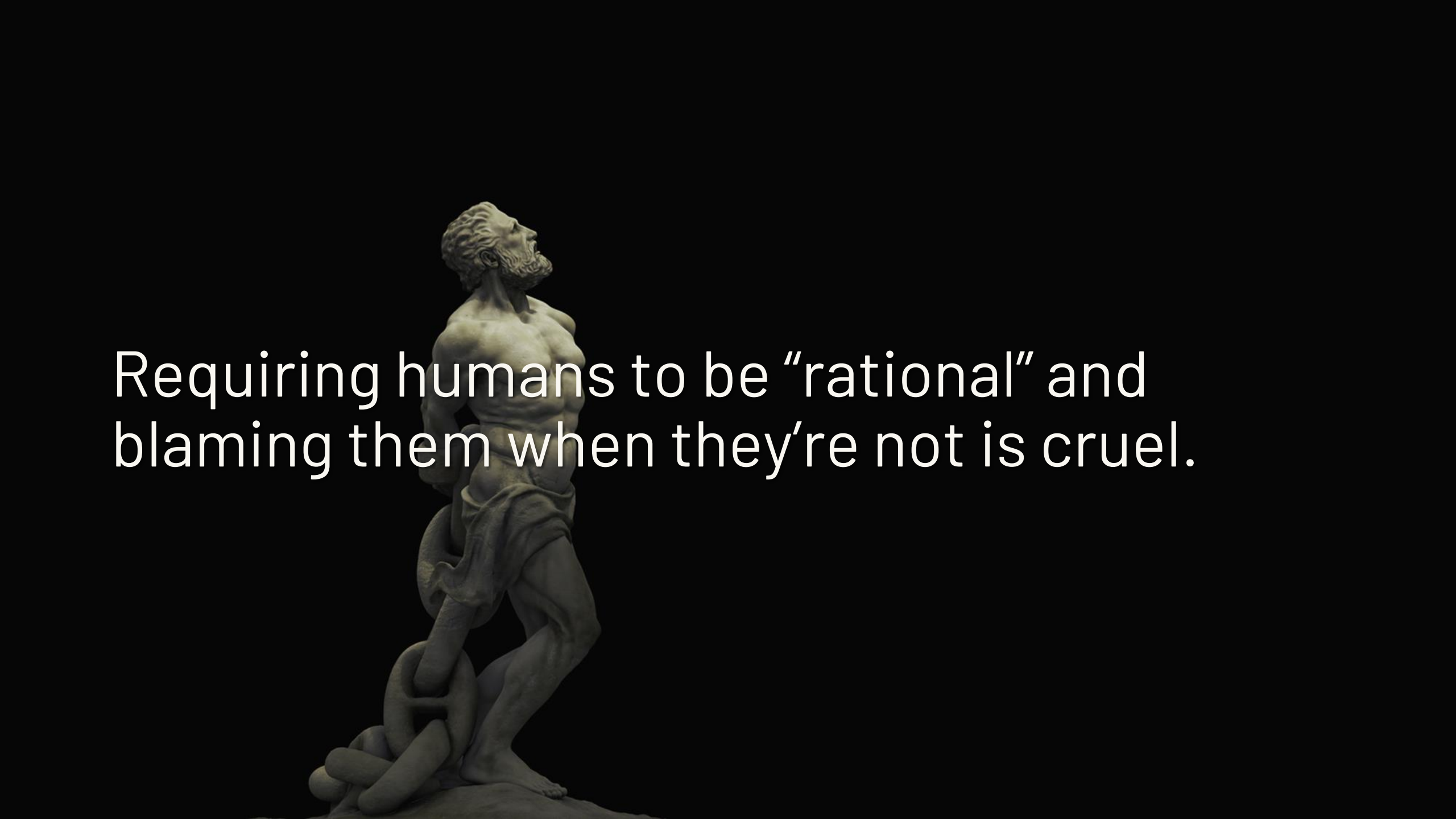

Our default cognitive mode, the lizard brain,
wants fast, simple, easy thinky thinky


Infosec decision making involves a lot of lizard brain because of stress and F.U.D.



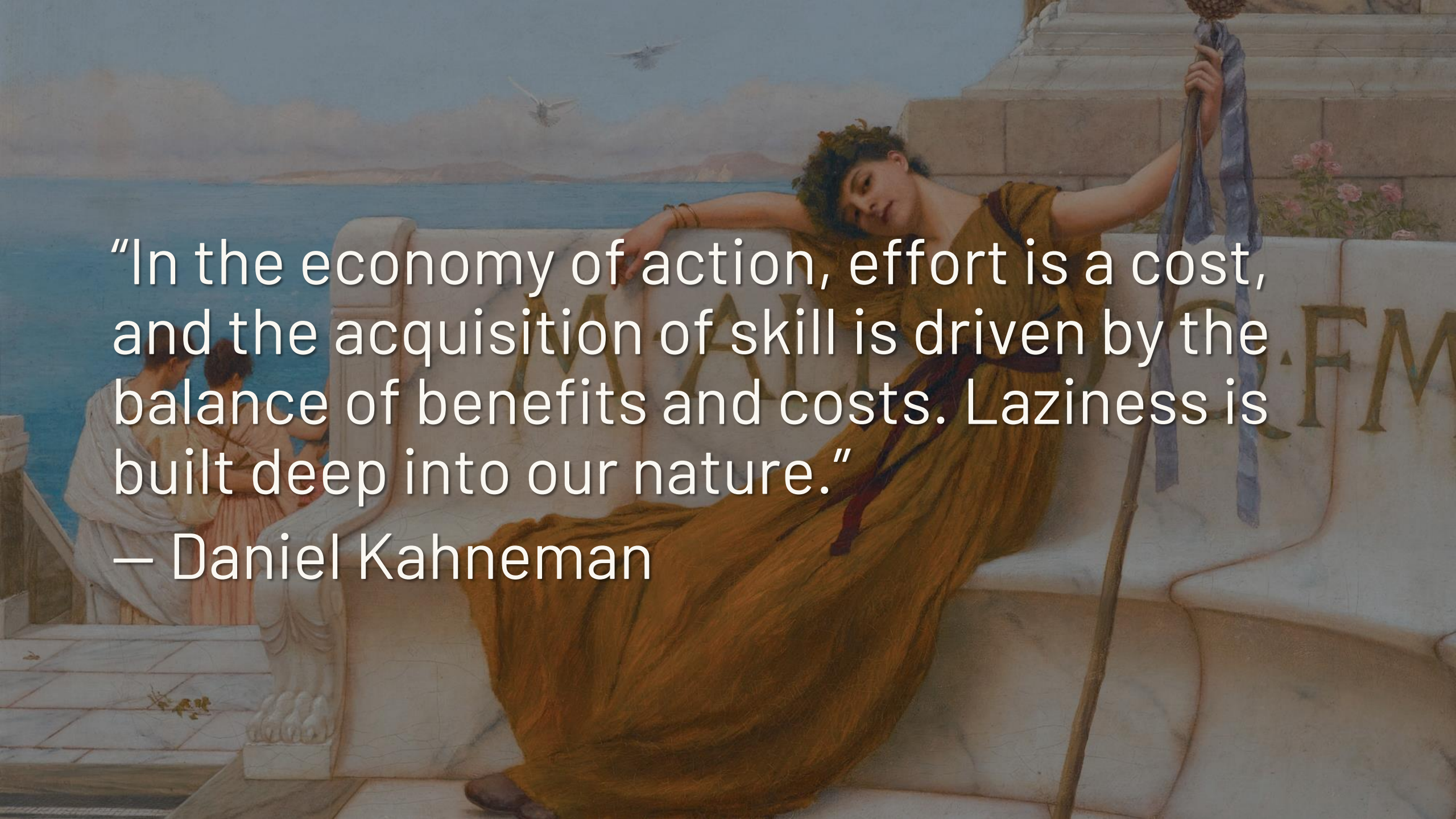
Lizard brain distorts infosec outcomes via myopia, blame games, poor investments


No one can be a Philosoraptor all the time.


Requiring humans to be “rational” and
blaming them when they’re not is cruel.


We need to design security programs,
policies, and tools for lizard brains instead


As security leaders, understand your lizard brain to optimize your own behavior



“In the economy of action, effort is a cost, and the acquisition of skill is driven by the balance of benefits and costs. Laziness is built deep into our nature.”

— Daniel Kahneman

@swagitda_

@sounilyu

/in/kellyshortridge

/in/sounil

info@kellyshortridge.com

cyberdefensematrix.com