

# Paint by Numbers: Resilience in Security

Kelly Shortridge (@swagitda\_)  
Square R00t 2018

A black cat is sitting behind a large orange pumpkin in a field of fallen autumn leaves. The leaves are a mix of yellow, orange, and red. The background is blurred.

Hi, I'm Kelly



“They always say time changes things, but you actually have to change them yourself.”

— Andy Warhol



Kelly Shortridge @ #DuraznoConf  
@swagitda\_



OH: "One thing I love about working in security: I get older, the problems stay the same"

9/21/18, 11:56

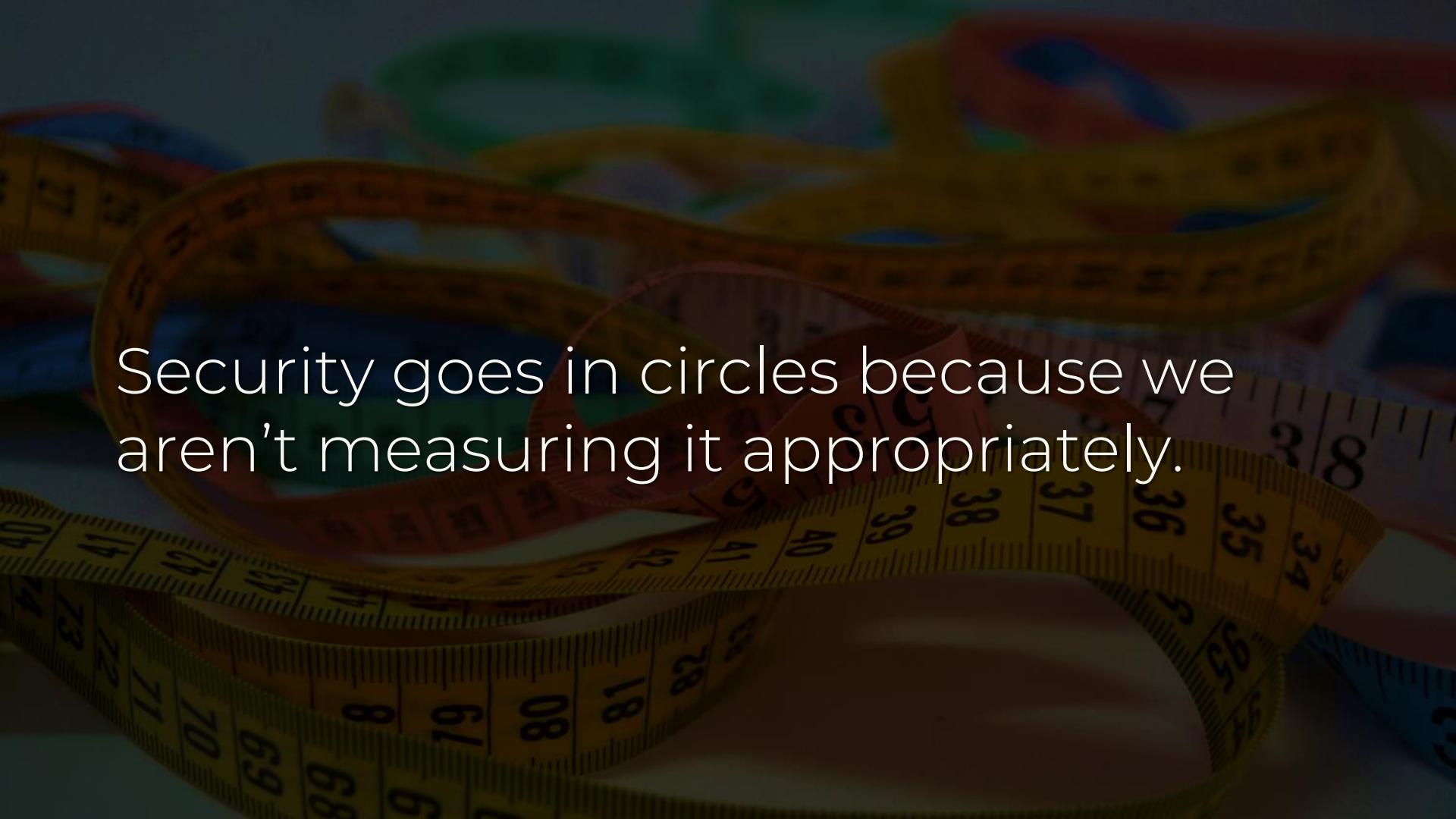
---

View Tweet activity

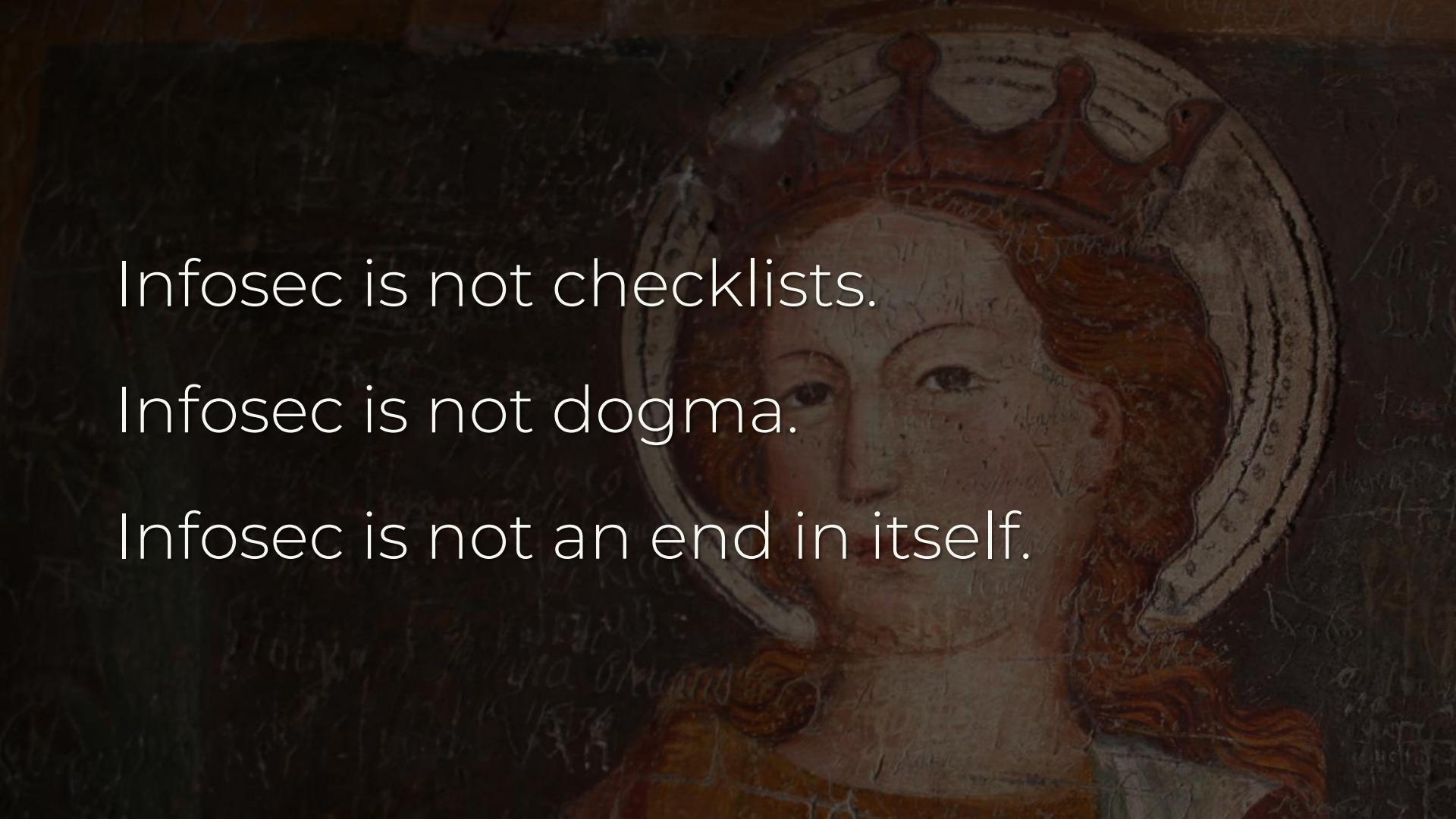
---

**74** Retweets **280** Likes

---

A stack of several colorful measuring tapes, primarily yellow and pink, are coiled together in a circular pattern. The tapes are marked with black numbers and smaller tick marks. The visible numbers range from 34 to 40. The background is dark, making the bright colors of the tapes stand out.

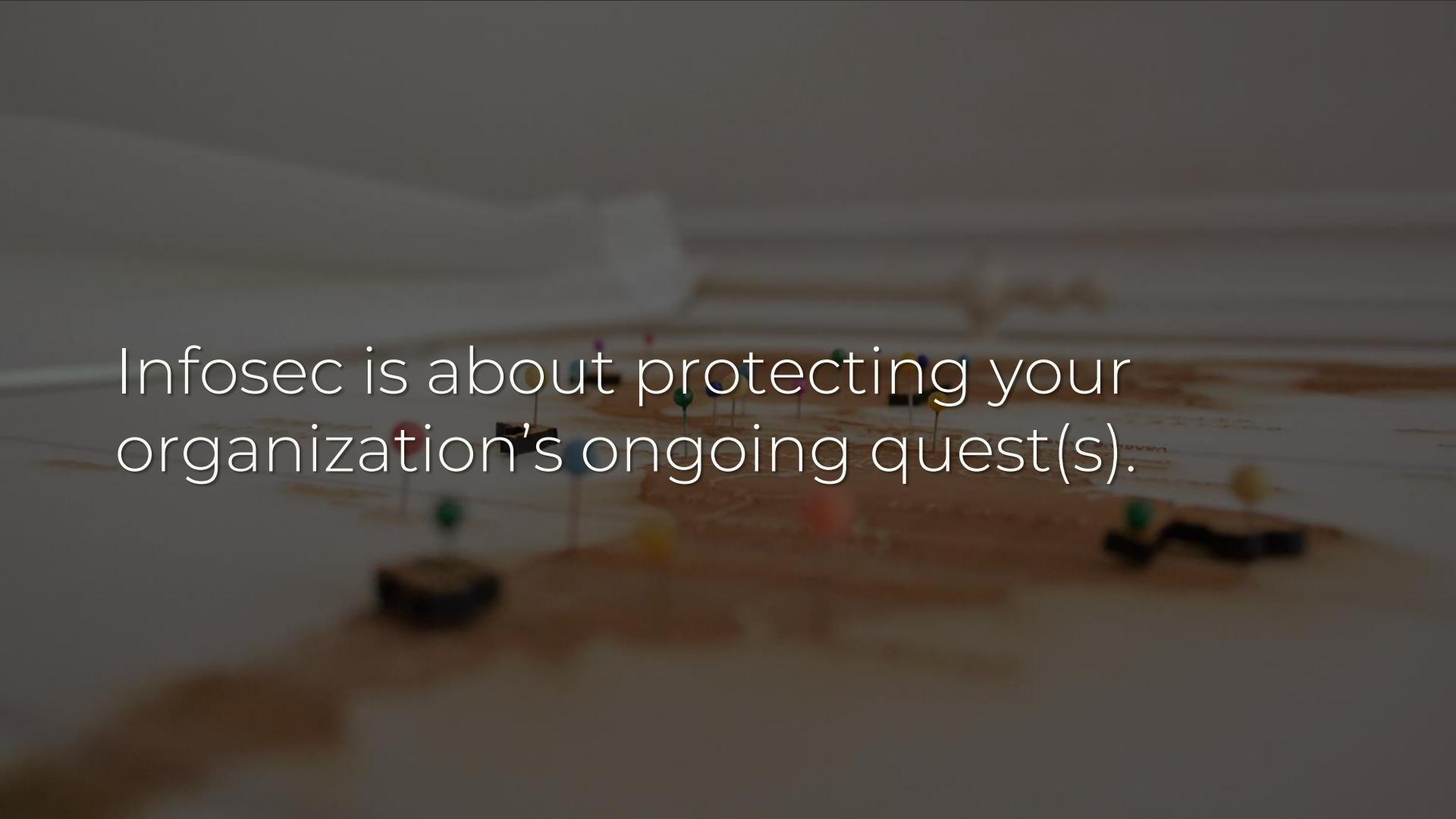
Security goes in circles because we  
aren't measuring it appropriately.

A faint, circular watermark or background image of a traditional oil lamp with a flame, centered behind the text.

Infosec is not checklists.

Infosec is not dogma.

Infosec is not an end in itself.



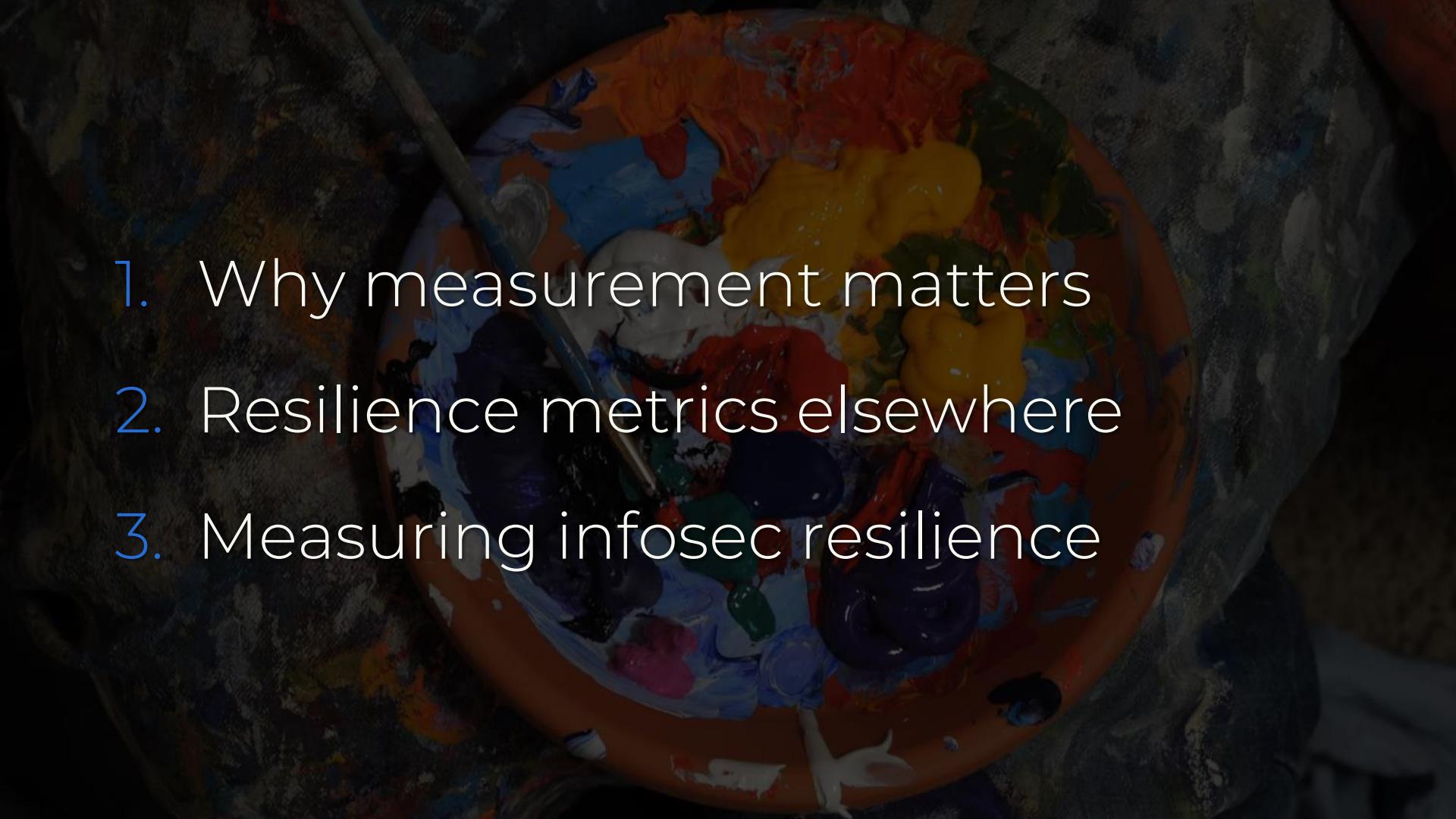
Infosec is about protecting your organization's ongoing quest(s).

The background of the slide features a dark, abstract design. It includes several glowing, translucent spheres in shades of orange, yellow, green, and blue, some with internal patterns. These spheres are set against a backdrop of dark, angular geometric shapes, possibly representing a futuristic or digital environment.

Infosec resilience means a flexible system that can absorb an attack and reorganize around the threat.



How can we measure resilience so you can paint an infosec vision?

- 
1. Why measurement matters
  2. Resilience metrics elsewhere
  3. Measuring infosec resilience

The background of the slide features a vibrant, abstract pattern of organic shapes in various colors, including shades of orange, yellow, red, blue, and green. These shapes resemble cells, neurons, or perhaps a microscopic view of a tissue sample, creating a complex and textured visual field.

Why is measurement  
important?

Generally we do something in order  
to achieve a certain result

Process: “a series of actions taken in order to achieve a particular end.”

A close-up photograph of a person's hands holding a smartphone. The phone has a vibrant, abstract patterned case featuring shades of orange, yellow, green, and blue. The background is dark and out of focus.

You cannot people or technology  
your way out of bad processes

Metrics are quantifiable measures to track & assess status

“Be a better person” vs. “read 30 mins per day & volunteer 1x per month”





Success metrics create the numbers  
by which you paint your vision

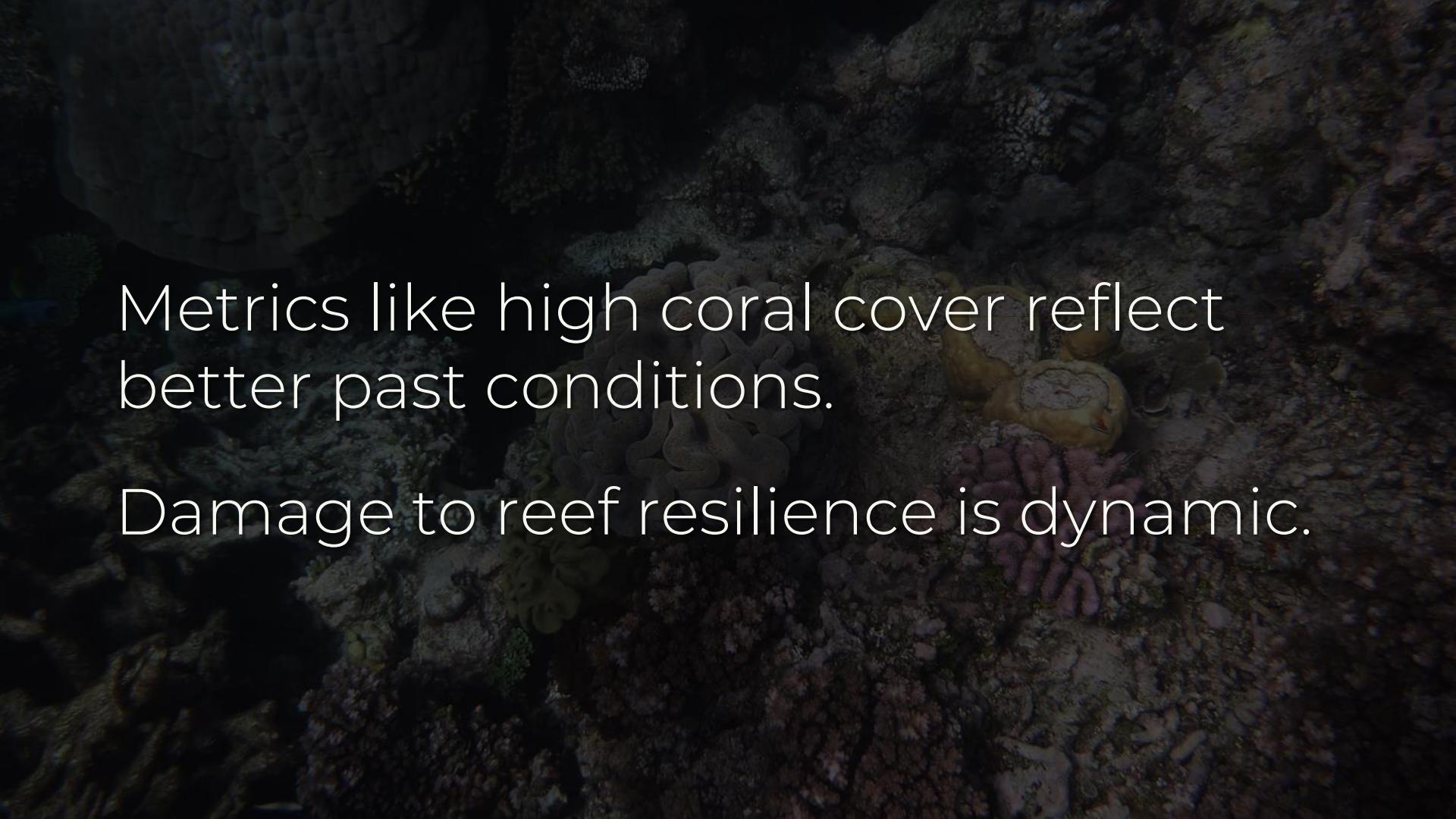
# Resilience Metrics Elsewhere

Resilience is a *journey*, not a singular,  
final destination

A dramatic painting depicting a shipwreck at sea. In the foreground, a small boat with several figures is visible, struggling against large, white-capped waves. The sea is depicted with dark, turbulent brushstrokes. In the background, a dark, silhouetted city or castle sits atop a hill, partially obscured by smoke or fog. The overall mood is one of despair and the power of nature.

Natural disaster resilience must  
assume failure of controls

What % of human development is in known at-risk disaster areas?

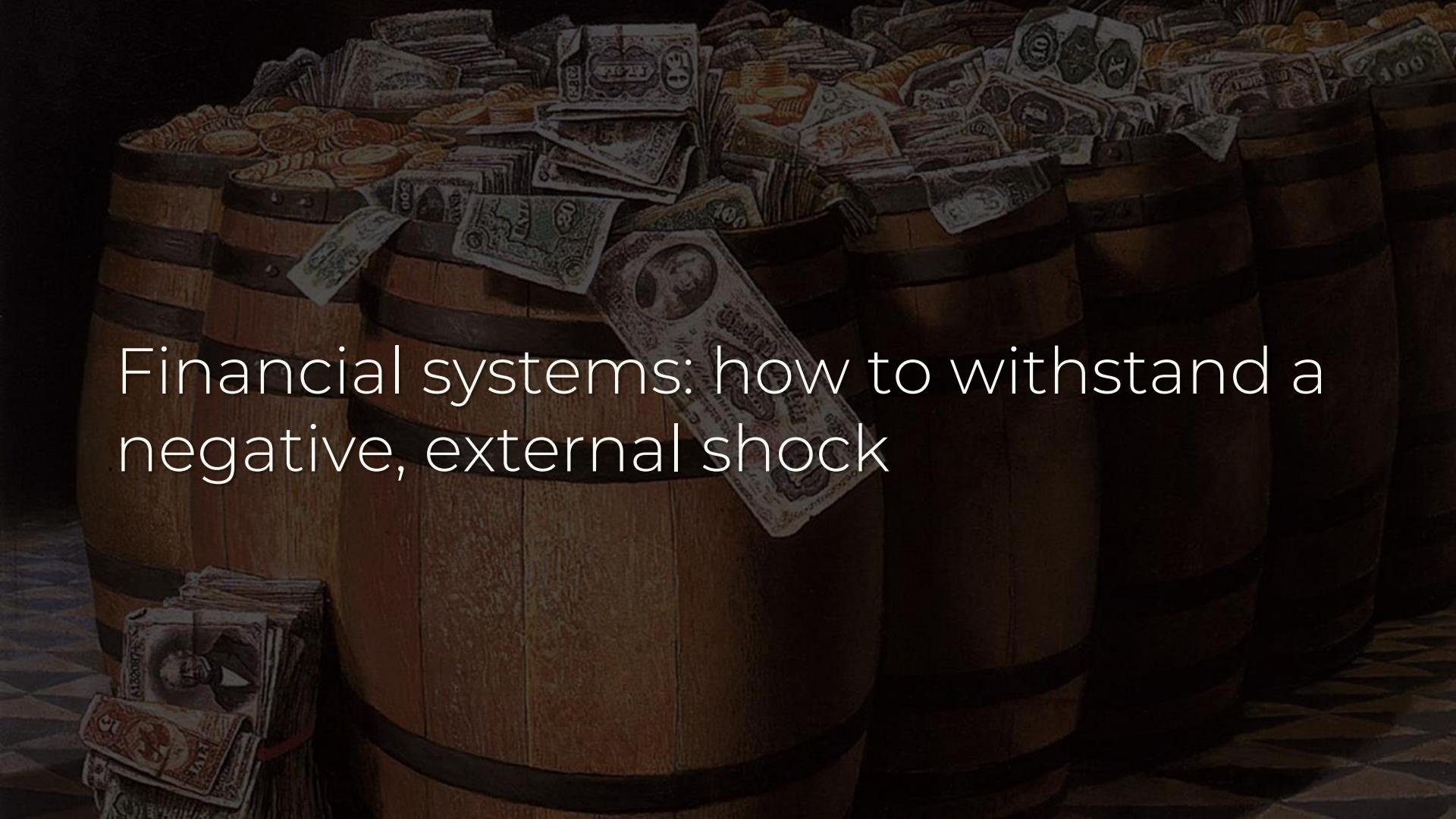


Metrics like high coral cover reflect  
better past conditions.

Damage to reef resilience is dynamic.

Ongoing stress like ocean warming  
makes coral less resilient to cyclones

How many ongoing stressors exist?  
How frequent are acute stressors?



Financial systems: how to withstand a negative, external shock

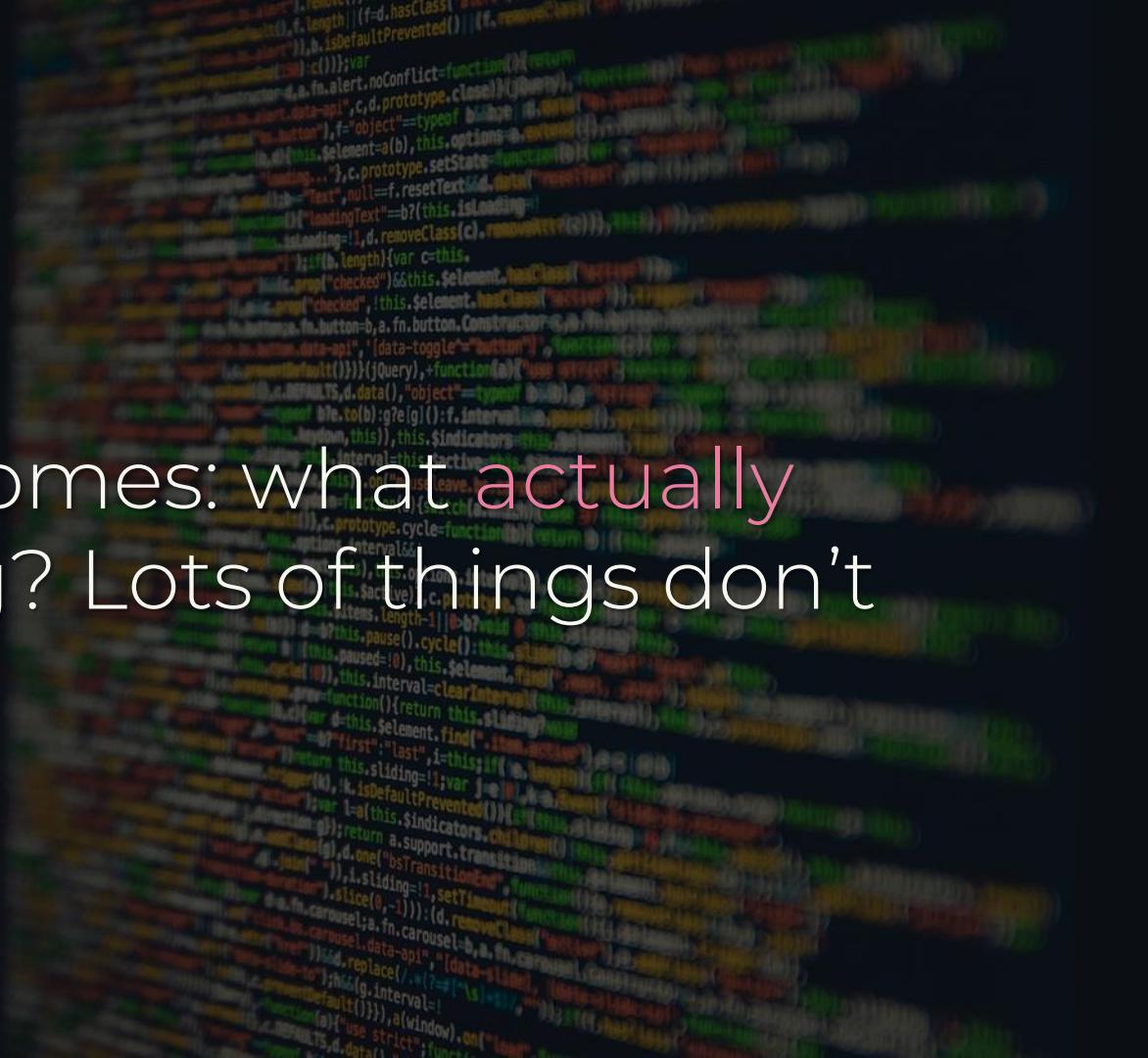
In a financial network, at what point does one default lead to a cascade?



High connectivity & large fraction of  
contagious links = riskiest nodes

Interconnectivity helps financial systems... until it hurts.

# DevOps Outcomes: what actually helps your org? Lots of things don't

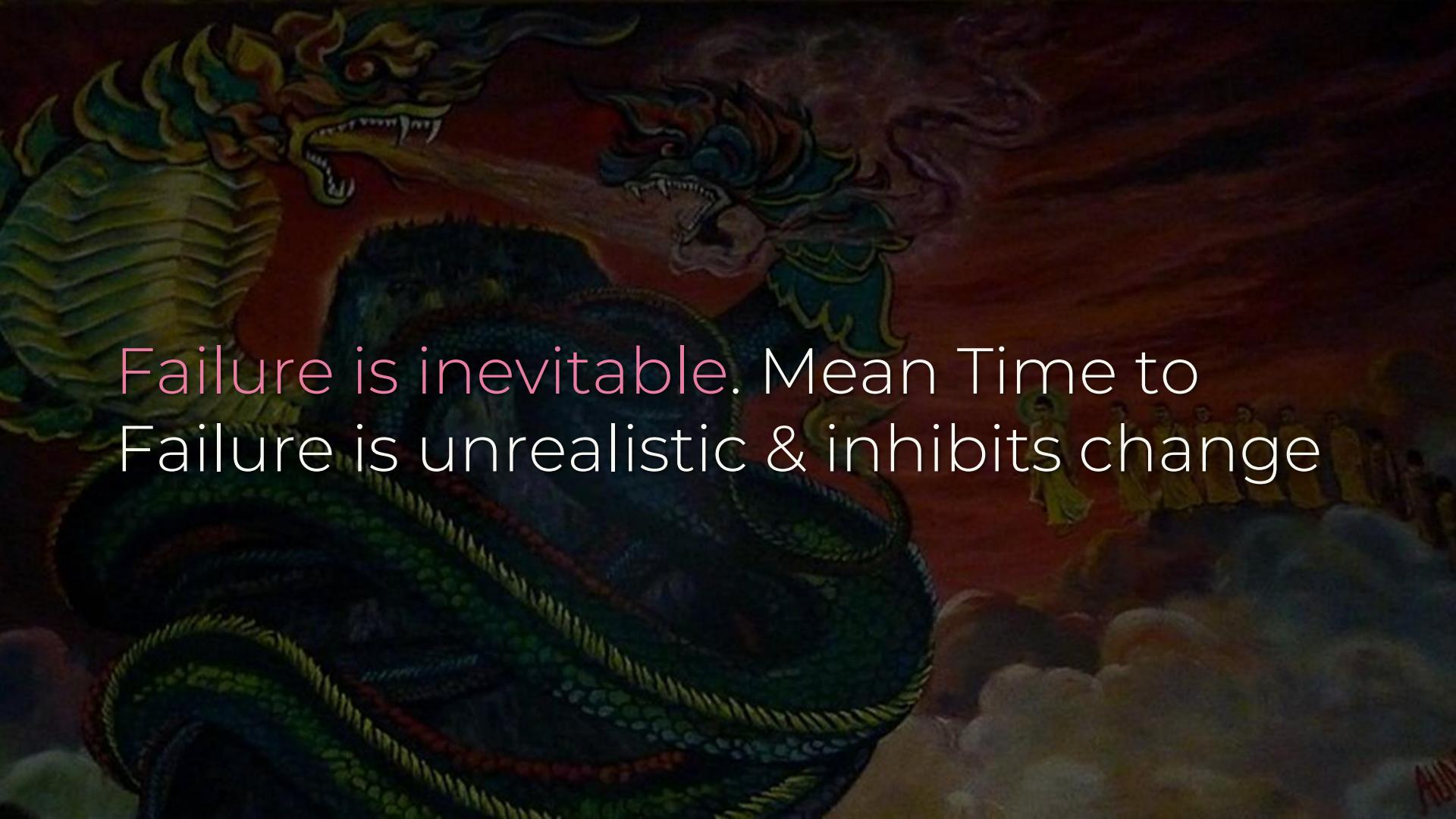


Elite DevOps performers:

Deploy frequency: on-demand

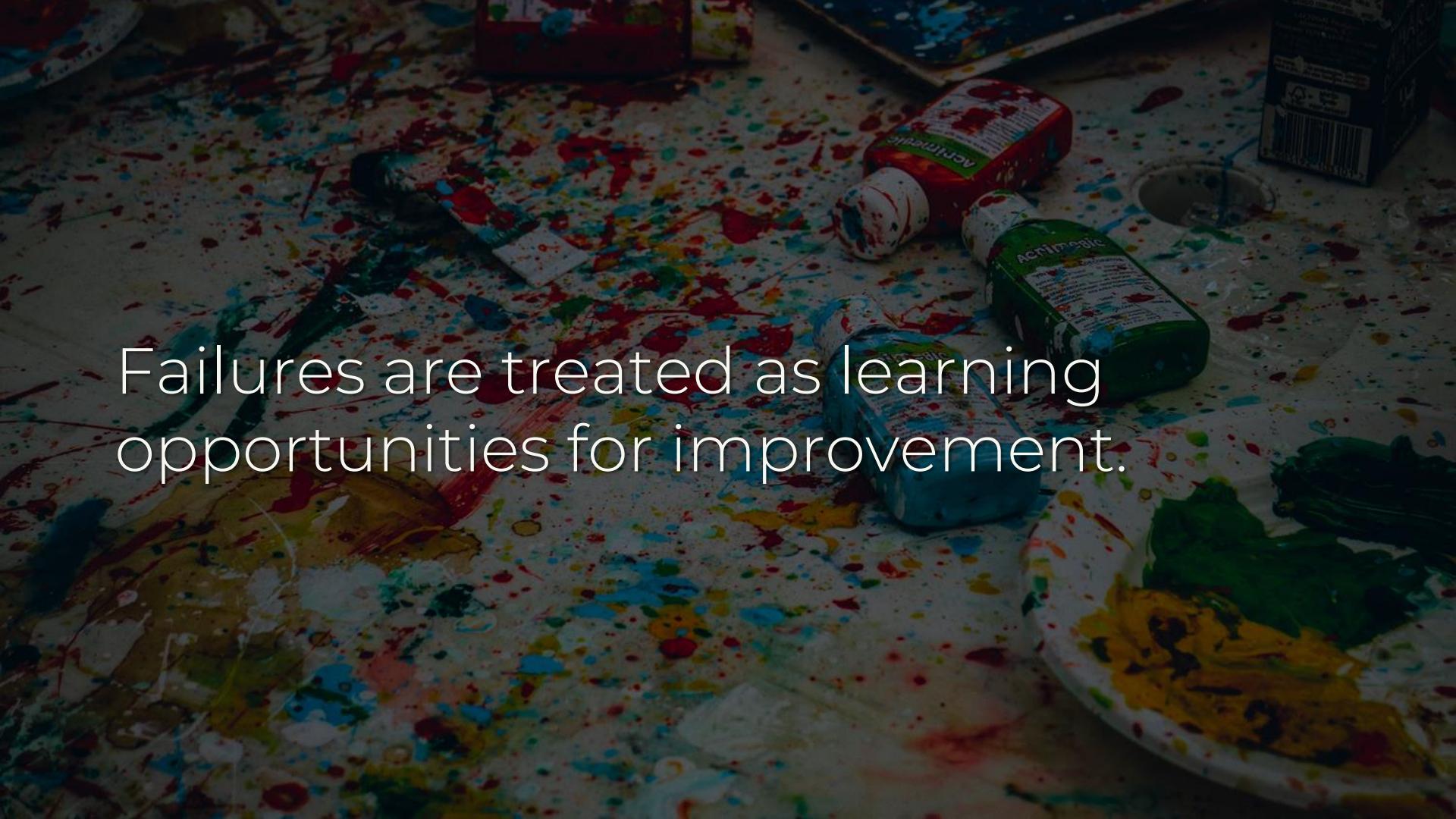
Lead time: <1 hour

MTTR: <1 hour

A traditional Chinese dragon painting, featuring two heads with open mouths and fangs, breathing fire or smoke. The dragon's body is long and winding, with scales in shades of green, yellow, and red. It is set against a dark, textured background.

Failure is inevitable. Mean Time to  
Failure is unrealistic & inhibits change

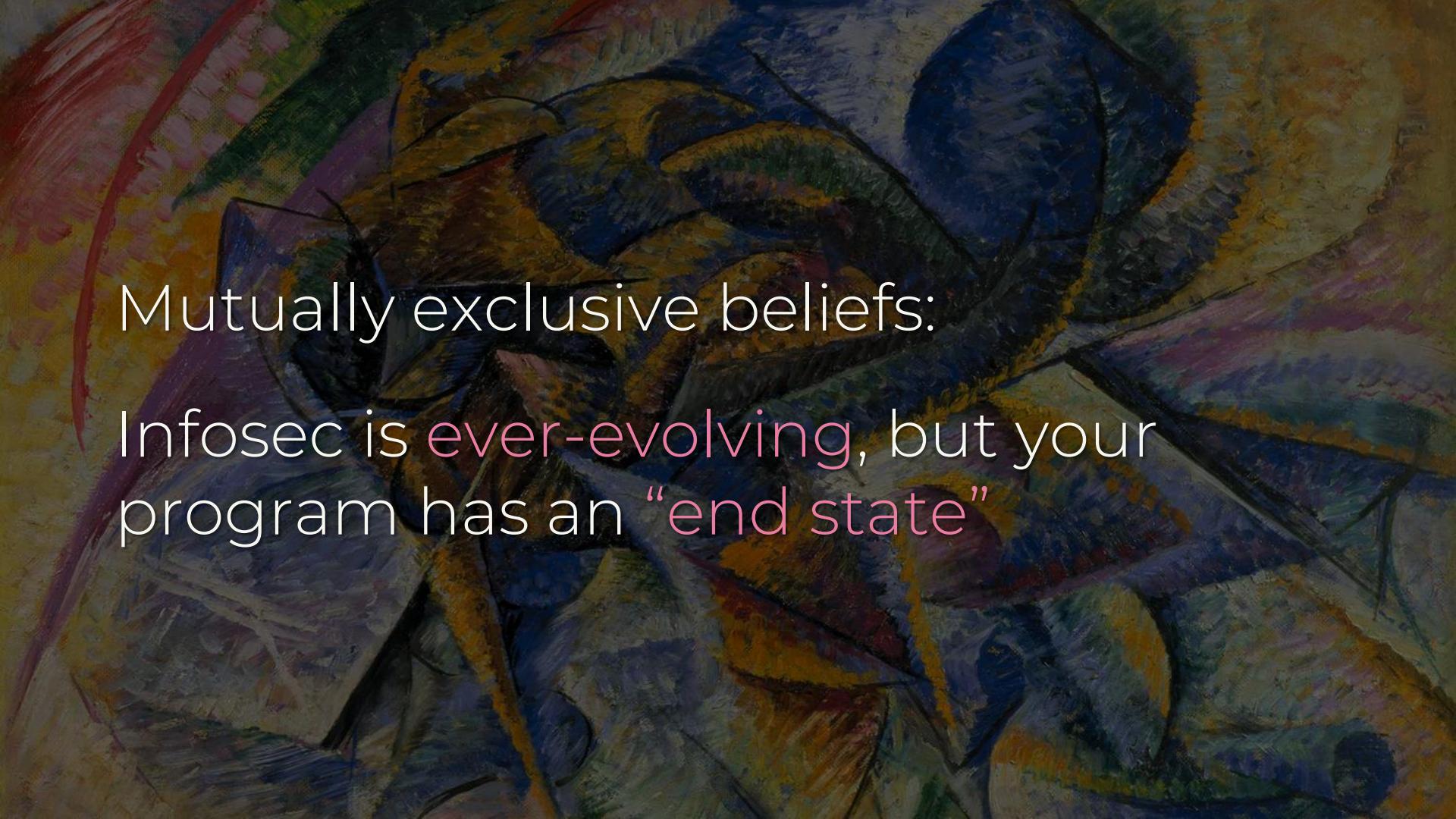
Westrum model of culture: power-,  
rule-, or mission-oriented

The background of the image shows a floor completely covered in a chaotic, colorful mess of paint splatters in various colors like red, blue, green, yellow, and white. Several plastic paint containers are scattered across the surface. In the center, there's a white bottle of 'Acrylic' paint, a red bottle, and a green bottle. To the right, a large white bucket is mostly submerged in the paint. In the top right corner, a cardboard box with a barcode and some text is visible.

Failures are treated as learning opportunities for improvement.

What resilience metrics can we take from this to use in infosec programs?

# Measuring InfoSec Programs

The background of the slide features a vibrant, abstract painting with thick brushstrokes. It consists of various colors including red, yellow, green, blue, and purple, creating a dynamic and textured composition.

Mutually exclusive beliefs:  
Infosec is ever-evolving, but your  
program has an “end state”

Your program's goal isn't maturity –  
it's org-level continuous resilience

Flexibility: can your security serve your org's needs in the way it needs?



Measure impact both ways: improved security vs. more friction

Positive: reduction in number of security fixes per project

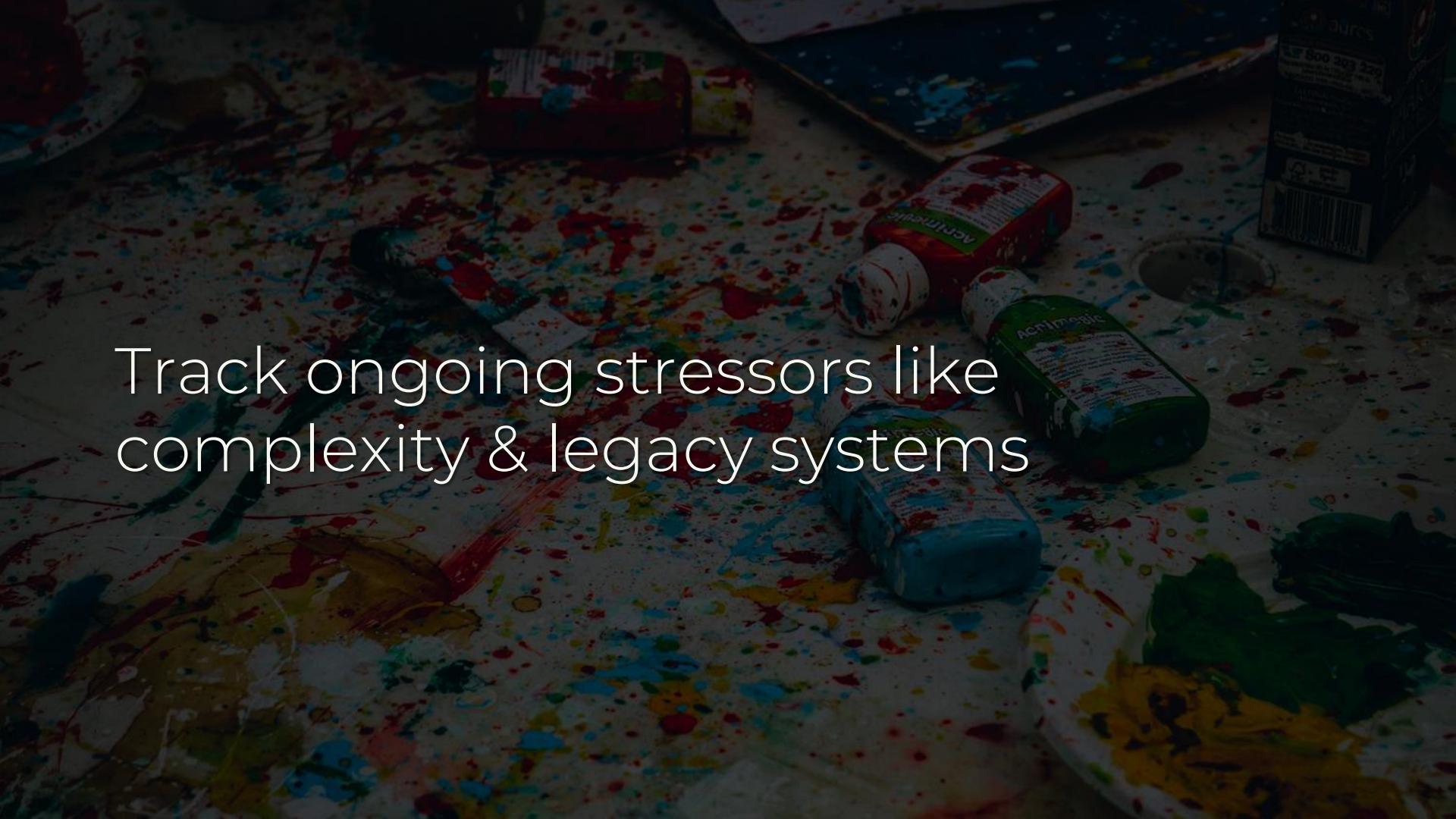
Negative: increase in employee time spent using security tools

“Elite performers build security in and can conduct security reviews & complete changes in just days.”

– State of Dev Ops 2018

Absorbing an attack: can you adapt  
efficiently?

Impact of a new vulnerability  
depends on erosion by ongoing stress

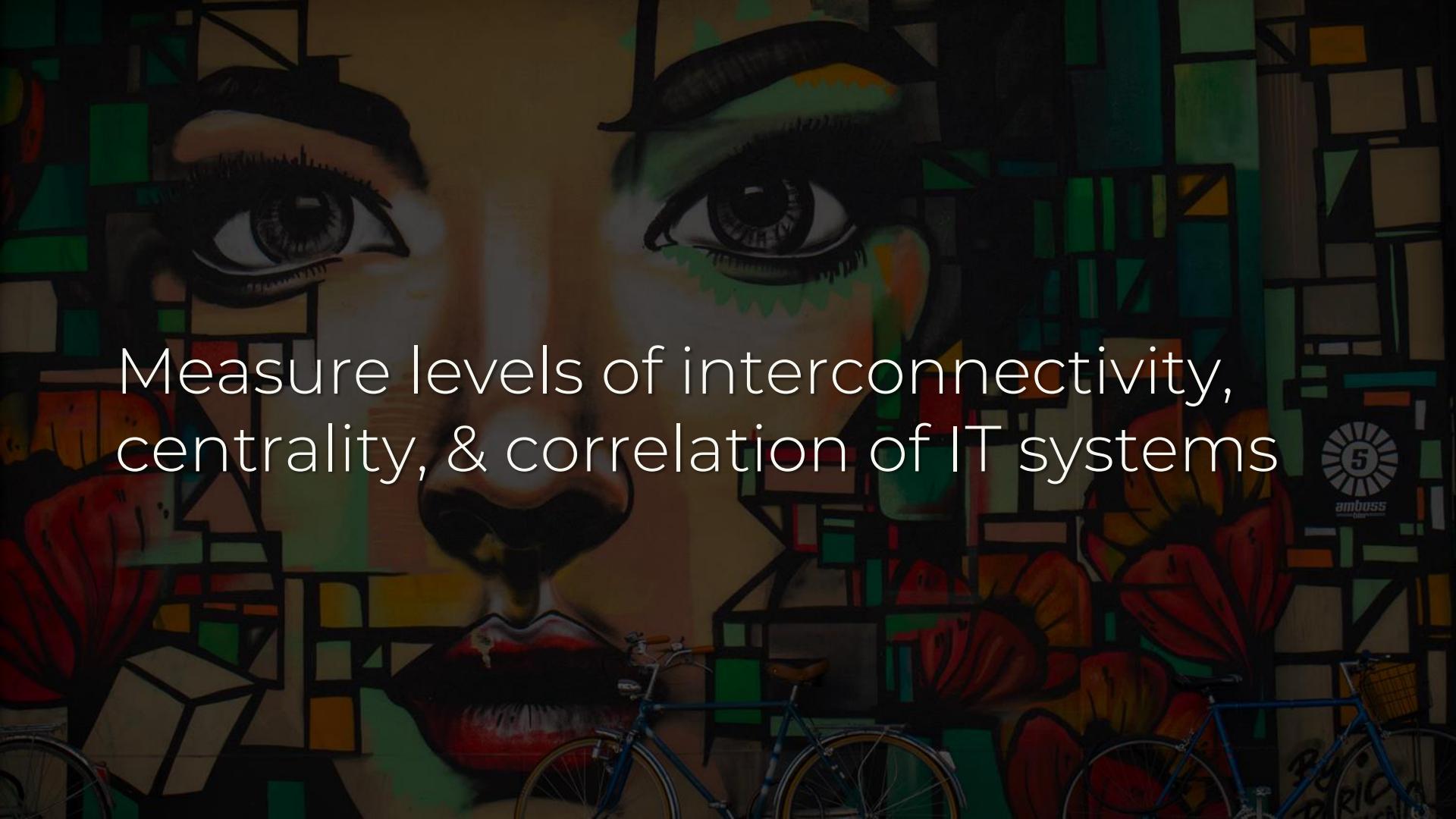
A photograph of a table covered in a chaotic, colorful mess of paint splatters in various colors like red, blue, yellow, and green. Art supplies are scattered across the surface, including several plastic bottles of acrylic paint in different colors, some with their labels partially visible. A paintbrush lies near one of the bottles. The overall scene conveys a sense of creative chaos or a lack of organization.

Track ongoing stressors like  
complexity & legacy systems

Mean Time to Remediation: how quickly do you resolve an incident?

Deploy frequency of security changes  
(patches, access control rules, etc.)

Reorganize around the threat: can you transform & innovate?

A vibrant mural on a building wall depicts a woman's face with large, expressive eyes. The background is filled with geometric shapes, colors, and a blue bicycle in the foreground.

Measure levels of interconnectivity,  
centrality, & correlation of IT systems



5  
amboss

Acute stress \* interconnectivity =  
potential propagation of pwn (PPP)

Unpatched databases without  
authentication = **high PPP**



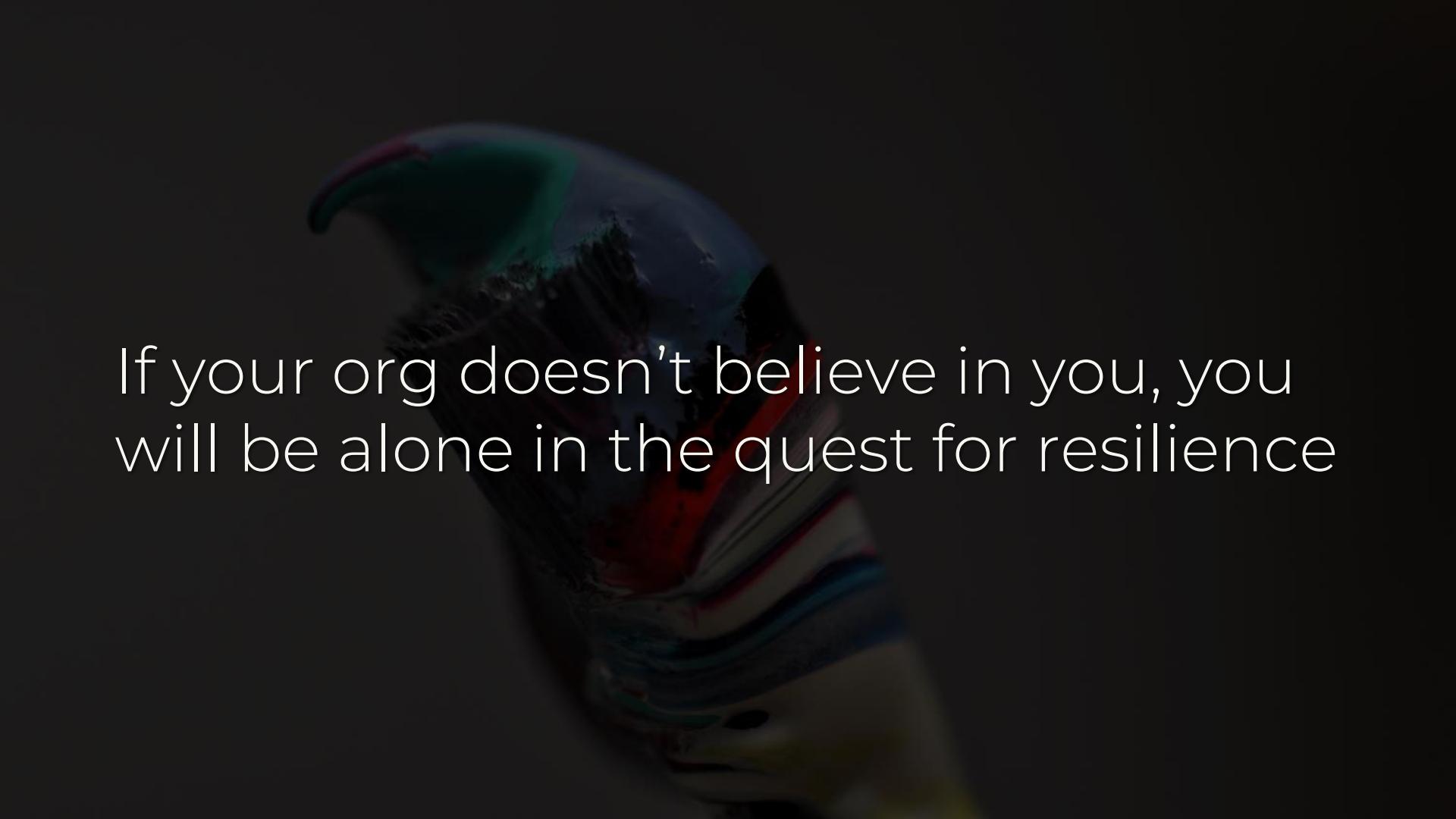
How strong is your culture? Are you  
actually mission-oriented?

Equifax blamed one person for failing to deploy a patch.

Don't do that.

Net Promoter Score (NPS):  
Mathematical calc of satisfaction

Measure NPS among your colleagues  
& teams with whom you work

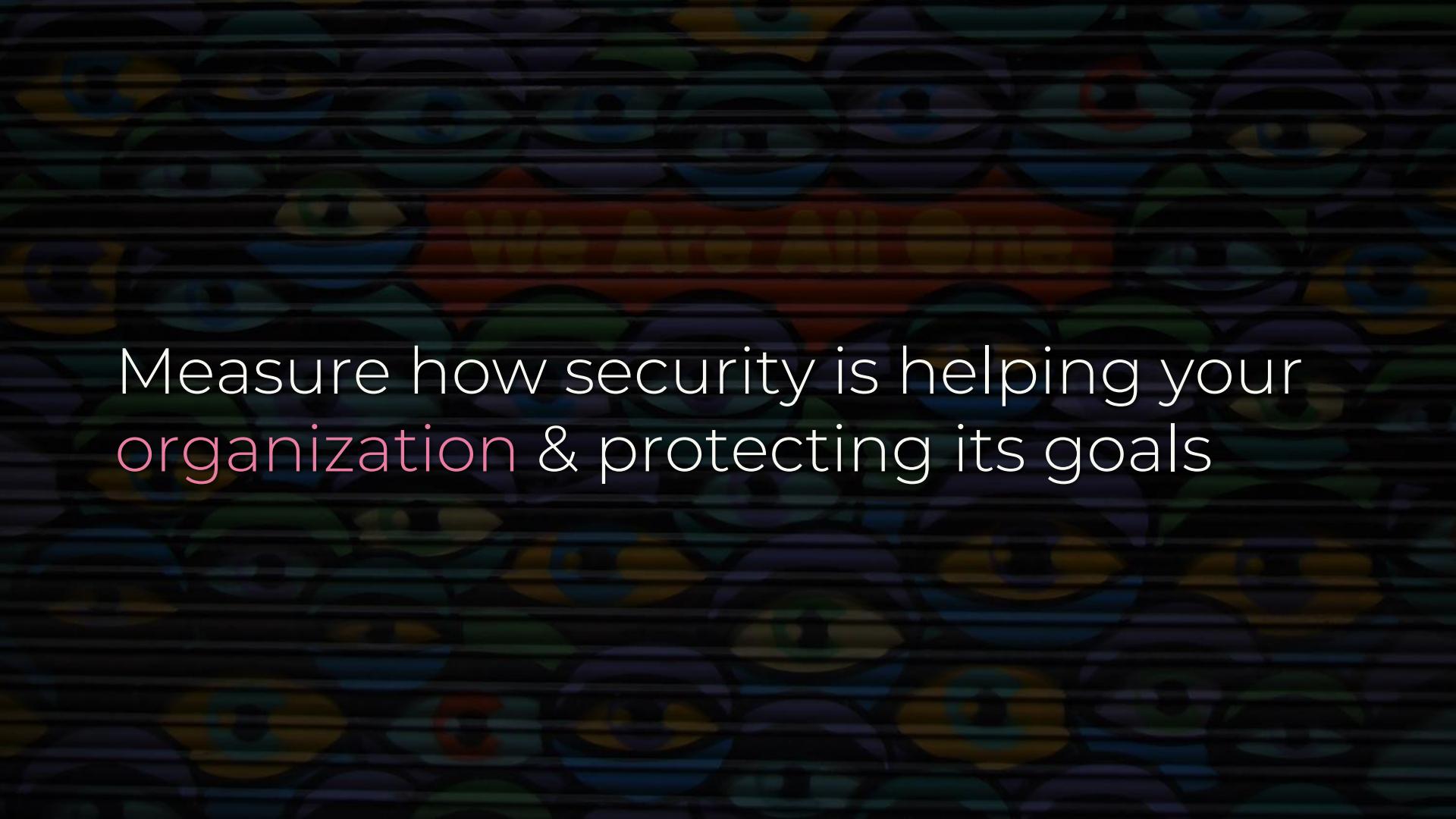
A person is shown from the chest up, wearing a dark-colored hoodie. They have their hands clasped together in front of them. A colorful, patterned headband is visible on their head, featuring shades of green, blue, and red. The background is dark and out of focus.

If your org doesn't believe in you, you  
will be alone in the quest for resilience

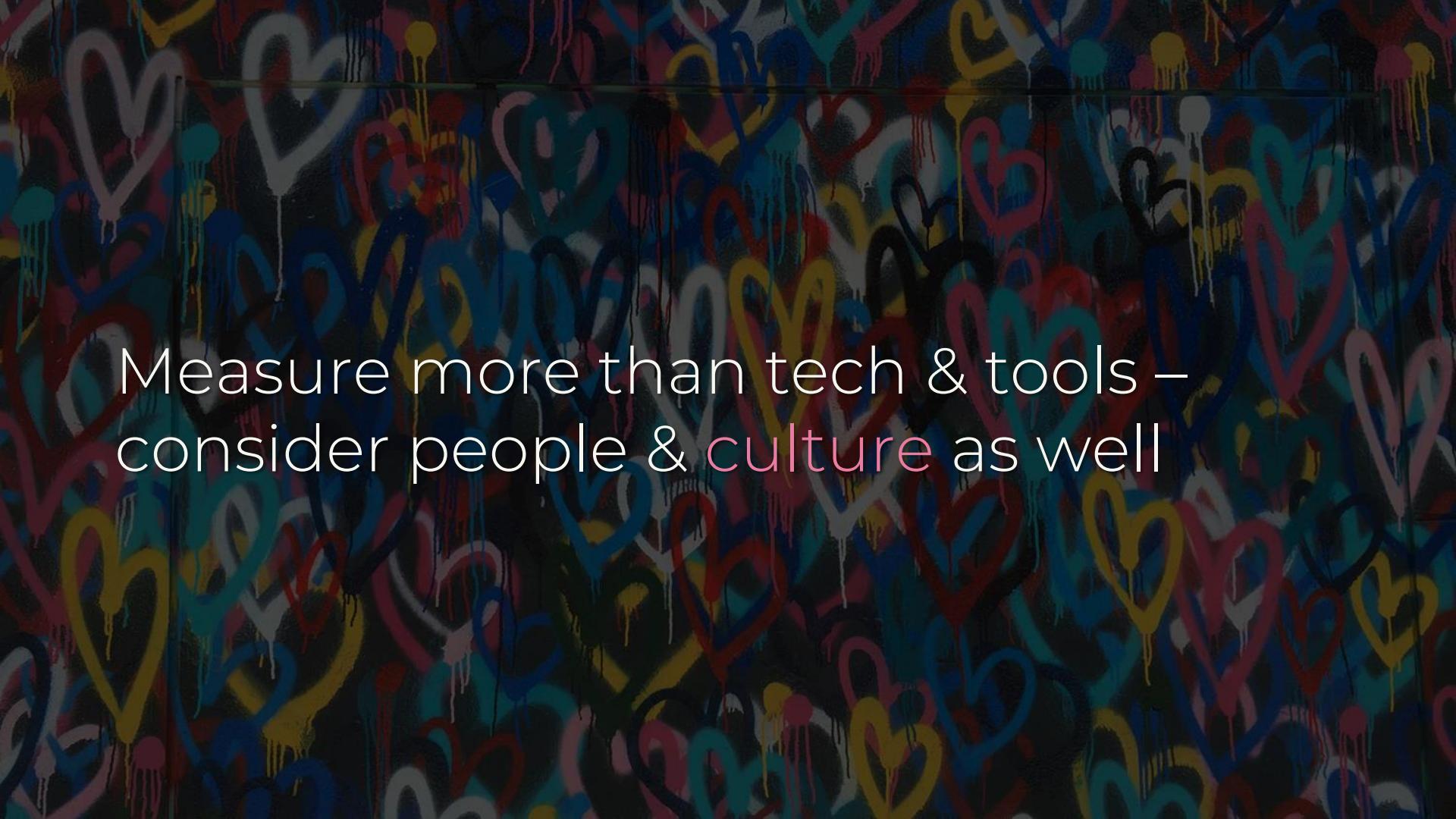
# Conclusion



Measure resilience – flexibility,  
adaptability, transformability



Measure how security is helping your organization & protecting its goals



Measure more than tech & tools –  
consider people & culture as well



“Have no fear of perfection – you'll never reach it.”

– Salvador Dalí



@swagitda\_



/in/kellyshortridge



kelly@greywire.net

# Suggested Reading

- [Accelerate](#) by Forsgren, et al., 2018
- [“Accelerate: State of Dev Ops 2018,”](#) DORA, 2018
- [“Are We There Yet? Signposts On Your Journey to Awesome,”](#) Forsgren, 2017
- “Incentivizing Resilience in Financial Networks,” Leduc & Thurner, 2016
- [“It’s Not Just Semantics: Managing Outcomes Vs. Outputs,”](#) HBR, 2012
- “Operationalizing resilience for adaptive coral reef management under global environmental change,” Anthony, et al., 2015
- [“Red Pill of Resilience,”](#) Shortridge, 2017
- [“Red teaming probably isn’t for you,”](#) Kohlenberg, 2017
- “Resilience to Contagion in Financial Networks,” Amini, et al., 2013
- “A strategy-based framework for assessing the flood resilience of cities: a Hamburg case study,” Restemeyer, et al., 2015
- “Systemic Risk and Stability in Financial Networks,” Acemoglu, et al., 2015