

An abstract painting with a grid of black lines. The background is a mix of grey, white, and dark blue. A large red rectangle is in the upper center. In the top left, the number '36' is written in black. In the bottom right, there is a black circle with a diagonal line through it. A vertical yellow bar is on the far right.

# Paint by Numbers: Resilience in Security

Kelly Shortridge (@swagitda\_)

DuraznoConf 2018

A brown tabby cat is lying on a wooden table, surrounded by several ripe peaches. The cat is looking down at the fruit. The peaches are arranged in a semi-circle in front of the cat. The table is made of light-colored wood. In the background, there is a wooden chair and a wooden deck. The text "Hi, I'm Kelly" is overlaid on the image in white font.

Hi, I'm Kelly

“...time was not passing...it was turning  
in a circle...”

— Gabriel García Márquez





**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



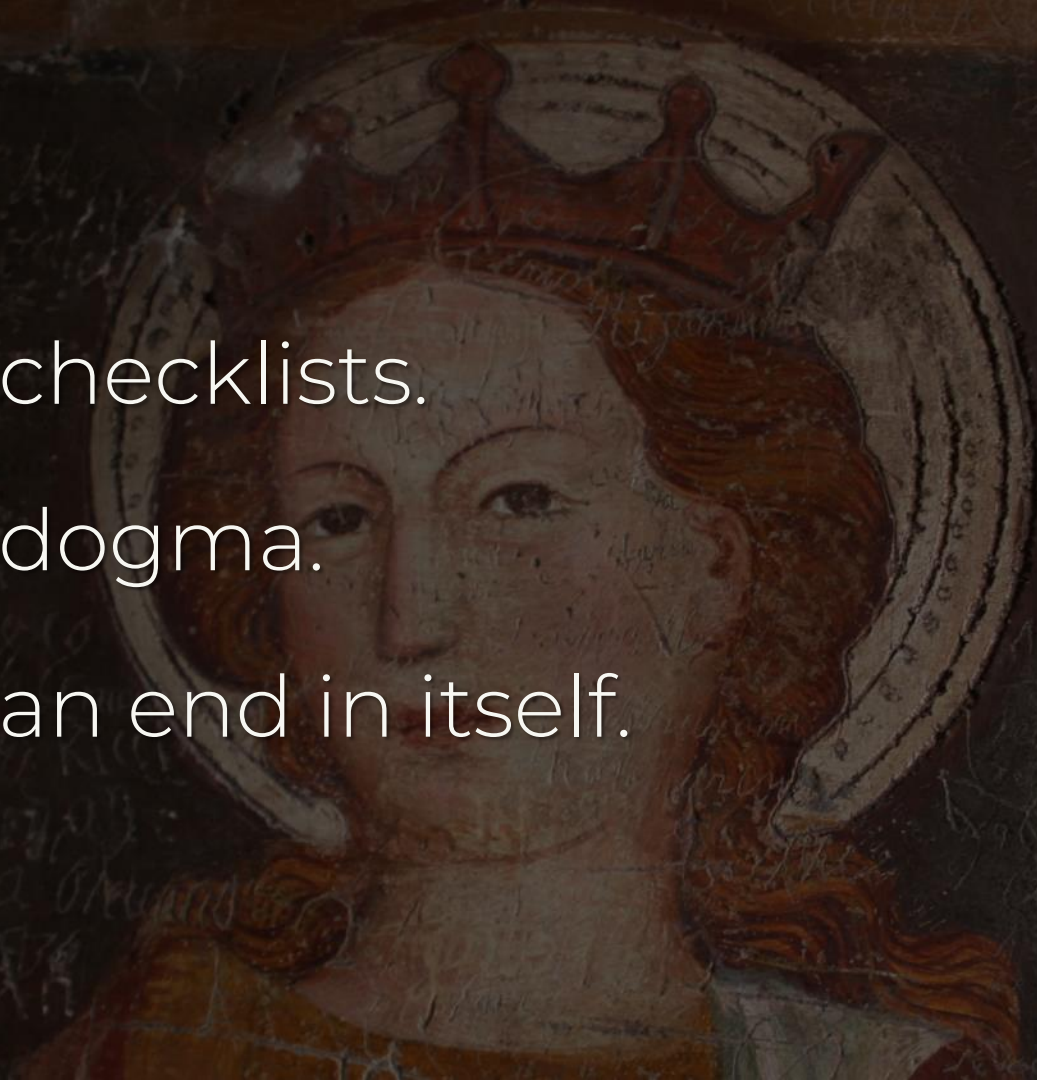


Security goes in circles because we aren't measuring it appropriately.

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).



A dense collection of various capsules and pills in different colors (blue, purple, green, yellow, red) and patterns (stars, stripes, speckles) scattered across a dark red background. The text is overlaid in the center.

Doctors treat patients – they can't  
lock up charts & throw away the key.





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

A person wearing a colorful, paint-splattered cap and a dark jacket is painting graffiti on a wall. The wall is covered in various graffiti tags and words, including "WAK", "EXPTIES", "TRUTH", and "WINNER TO PR". The person is using a spray can to apply red paint to a tag. The overall scene is dimly lit, with the person's face in shadow.

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

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






Why is measurement  
important?



Generally we do something in order to achieve a certain result

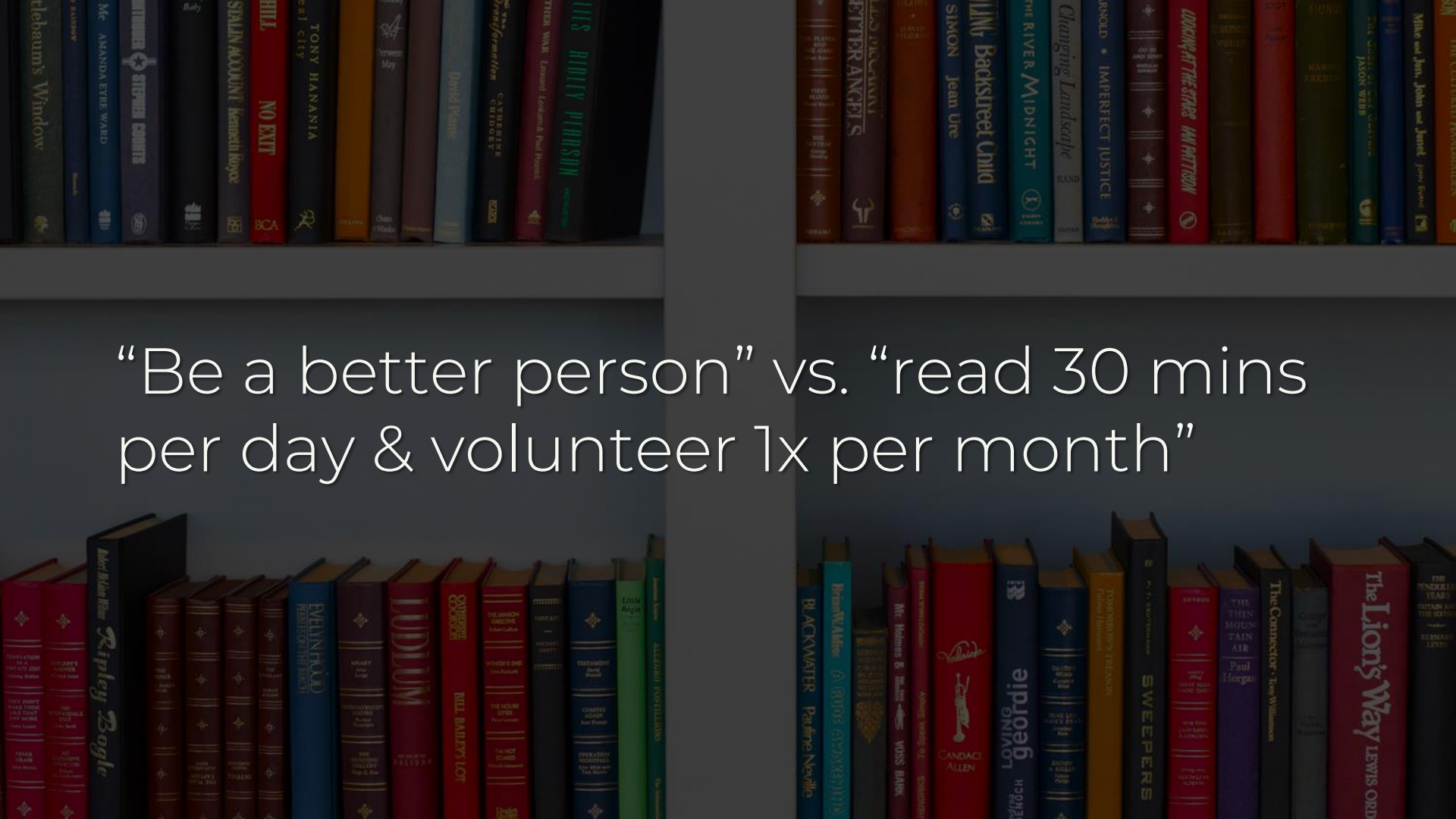
Process: “a series of actions taken in order to achieve a particular end.”



You cannot people or technology  
your way out of bad processes

Metrics are quantifiable measures to track & assess status



A background image of a bookshelf filled with various books. The books are arranged in two rows. The top row includes titles like 'The Window', 'M.A. Eyre Ward', 'Stephan Courts', 'No Exit', 'Tony Hanania', 'The Transformation', 'The War', 'The Bitter Person', 'The River', 'Backstreet Union', 'Imperfect Justice', 'Looking at the Stars', 'The Connector', and 'The Lion's Way'. The bottom row includes titles like 'Ripley Bogie', 'Elinor Hood', 'Juddum', 'The Connector', 'The Lion's Way', and 'The Lion's Way'. The text is centered over the bookshelf.

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

A collection of colored pencils is arranged in a row at the top left of the image. Below them, a spiral-bound notebook is open, showing a page with a detailed black and white line drawing of a rabbit and various flowers. The notebook's metal spiral binding is visible on the right side. The entire scene is overlaid with a semi-transparent dark grey filter.

Success metrics create the numbers  
by which you paint your vision

The background is a piece of marbled paper with a complex, organic pattern. The colors are primarily dark blues, greys, and blacks, with some lighter blue, green, and red accents. The pattern consists of swirling, cell-like shapes that resemble marbled paper or perhaps a microscopic view of tissue. A semi-transparent dark grey or black overlay covers the entire image, making the text stand out.

# Resilience Metrics Elsewhere

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



A dramatic, dark landscape painting. In the foreground, a small boat with a single figure is struggling in turbulent, dark water. The middle ground shows a coastal town with buildings and a prominent tower or castle on a cliffside. The background features a vast, stormy sea under a dark, cloudy sky. The overall mood is one of peril and resilience.

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?

A row of wooden barrels overflowing with stacks of various banknotes and coins, including US dollars and Euro coins. The barrels are arranged in a line, and the money is piled high, spilling out of the tops. The scene is dimly lit, with a checkered floor visible in the foreground.

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 painting depicting two dragons breathing fire. The dragons are rendered in vibrant green and blue scales, with their heads facing each other and mouths open, exhaling a bright orange and red flame. The background is a dark, textured wash of brown and red. In the lower right, a group of figures in yellow robes stands on a white, billowing cloud. The overall style is characteristic of traditional Chinese ink and wash painting with a focus on bold colors and dynamic movement.

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

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



The background image shows a white floor covered in a chaotic pattern of colorful paint splatters in red, blue, yellow, and green. Several tubes of acrylic paint are scattered across the floor, some lying on their sides. The tubes are labeled 'Acrylic' and 'Acrylic' in various colors. A paint palette with yellow and green paint is visible in the bottom right corner. A dark box with a barcode is in the top right corner. The overall scene is one of creative mess and artistic experimentation.

Failures are treated as learning opportunities for improvement.



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

The background of the slide is a piece of marbled paper with a complex, organic pattern of swirling colors including shades of purple, blue, green, orange, and pink. A dark, semi-transparent grey overlay covers the entire image, creating a moody atmosphere. The text is centered in the middle of the slide.

# Measuring InfoSec Programs



An abstract painting with a complex, layered composition. The background is a mix of dark blues, purples, and greens, with prominent brushstrokes and textures. A large, curved red stroke is visible in the upper left corner. The overall style is expressive and somewhat somber.

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?



A photograph of a dark wooden double door set within an arched frame on a light-colored wall. To the left of the door, there is a flowering bush with green leaves and small red flowers. The text "Locking yourself at home with tripwires to stop robbers isn't fun" is overlaid in white on the left side of the image.

Locking yourself at home with  
tripwires to stop robbers isn't fun

The background is a dark, textured image, possibly a painting or a photograph with a grainy, painterly quality. It features a central, dark, vertical shape that could be a person or a column, rendered in shades of blue, black, and dark brown. The overall tone is somber and moody. The text is overlaid in the center-left area.

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

Track ongoing stressors like  
complexity & legacy systems





Have you eliminated low-hanging fruit? (password = password...)

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?



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



A high-speed photograph of a water splash on a surface. The splash is centered, with several droplets captured in mid-air above the main impact point. Concentric ripples spread outwards from the center. The background is a dark, multi-colored gradient, transitioning from deep red on the left to dark blue and purple on the right, with green and yellow tones in the center. The overall mood is dynamic and visually striking.

Facebook Social Login breach was bad due to level of interconnectivity

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.

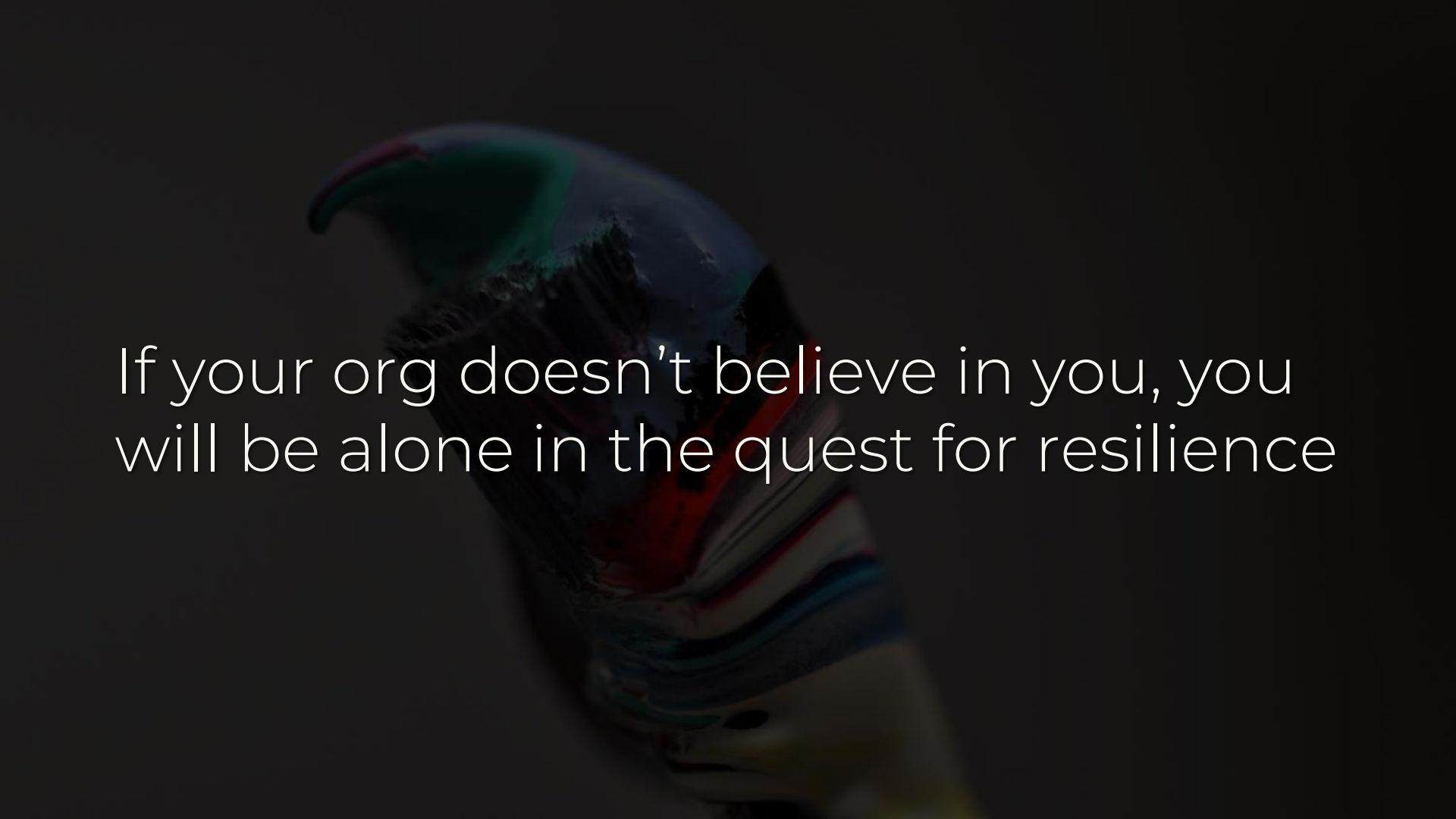
Don't do that.



It is never just one person or variable  
in a complex system

Net Promoter Score (NPS):  
Mathematical calc of satisfaction

Measure NPS among your colleagues  
& teams with whom you work

A close-up, low-angle shot of a colorful parrot, possibly a cockatiel, looking upwards. The parrot's head is the central focus, showing its vibrant blue, red, and yellow feathers. A clear reflection of a dense forest with tall trees is visible on the top of its head, as if it were a mirror. The background is dark and out of focus, making the parrot stand out. The overall mood is contemplative and resilient.

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