

Paint by Numbers: Resilience in Security

Kelly Shortridge (@swagitda_)

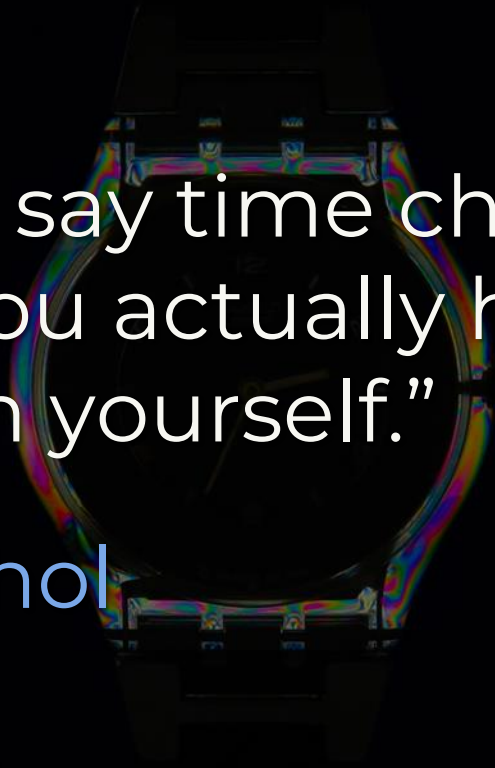
Square R00t 2018

A black cat is sitting in a pile of autumn leaves, with a large orange pumpkin behind it. The text "Hi, I'm Kelly" is overlaid on the image.

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

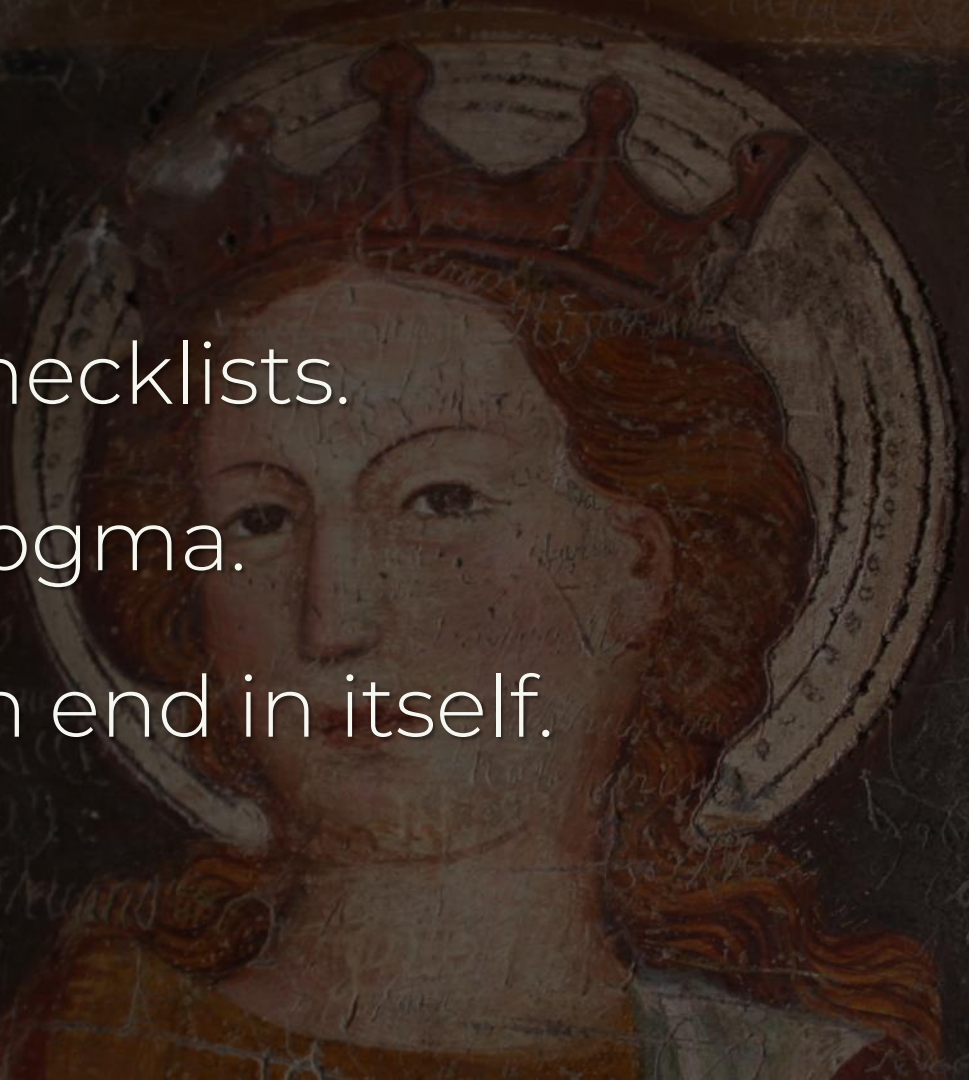


Security goes in circles because we
aren't measuring it appropriately.

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).



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

A person wearing a paint-splattered cap and a dark jacket is painting graffiti on a wall. The wall is covered in colorful graffiti, including the words "WAK", "exptes", "PAIN", "TRUTH", and "WINNER TO PP". The person is wearing white earbuds and is focused on their work.

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?

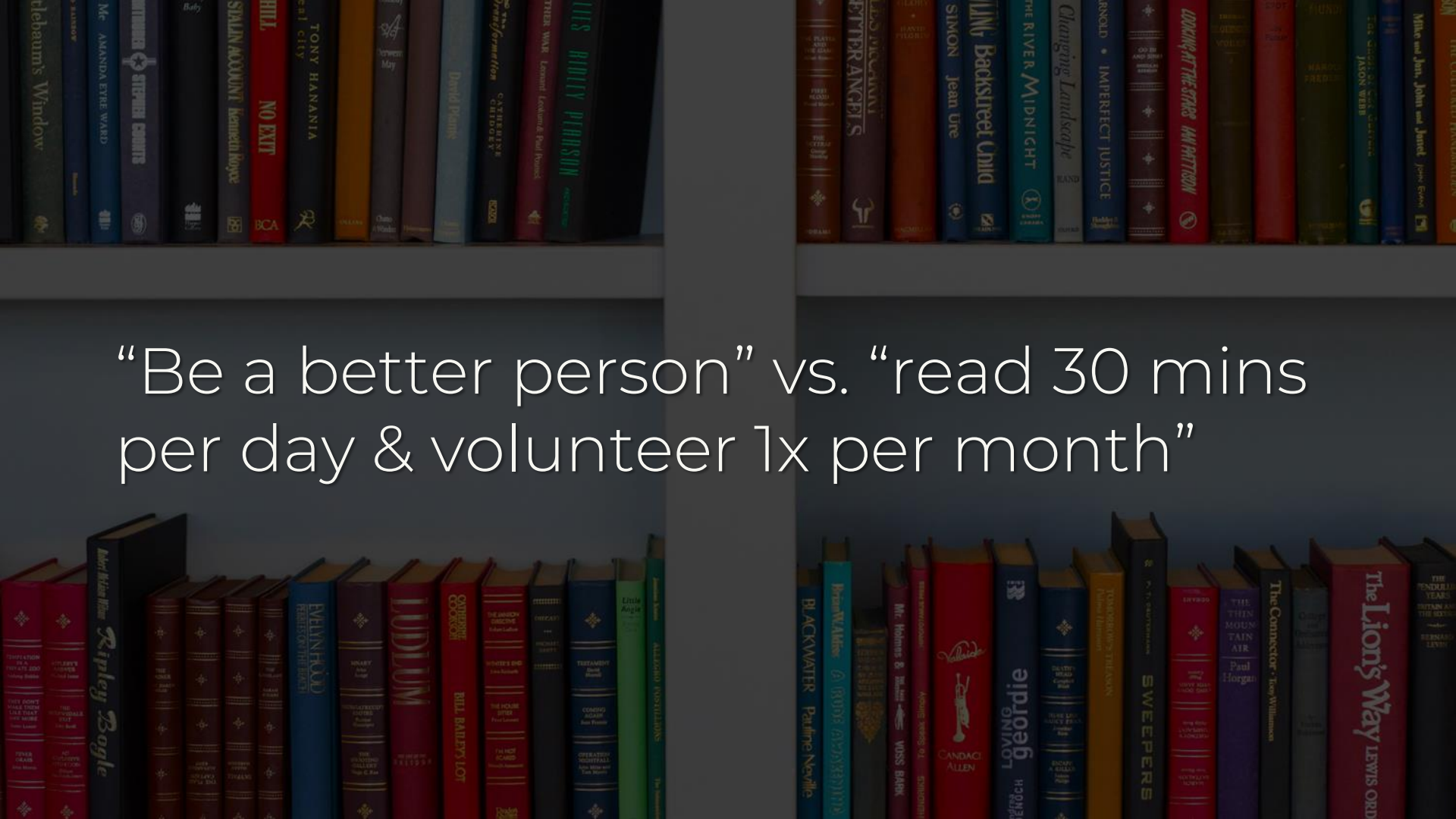
Generally we do something in order
to achieve a certain result

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

A close-up, dark, and grainy image of two hands, one with a ring, suggesting a struggle or a firm grip. The hands are positioned in the center of the frame, with fingers spread. The lighting is low, creating a somber and intense atmosphere. The background is a solid dark gray.

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”

A collection of colored pencils is arranged in a fan shape at the top left of the image. Below them is a spiral-bound notebook. The notebook's cover features a detailed black-and-white line drawing of a rabbit surrounded by flowers and foliage, intended for coloring. The notebook is open to a page with a calendar or planner layout, showing dates and text such as "Good Friday (Western)", "Passover", "Easter Sunday (Australia - except Tas. & WA)", and "Easter (Western)". 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 of the slide is a piece of marbled paper with a complex, organic pattern. It features swirling, cell-like shapes in various shades of blue, green, brown, and red, creating a textured and artistic look.

Resilience Metrics Elsewhere

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

The background is a dark, atmospheric painting. It depicts a turbulent sea with white-capped waves crashing. In the lower-left foreground, a small, dark boat with a single sail is struggling against the waves. In the distance, a city or fortress is perched on a dark, craggy cliff. The sky is filled with heavy, dark clouds, with a patch of lighter, yellowish light breaking through near the horizon behind the cliff. The overall mood is one of danger and resilience.

Natural disaster resilience must
assume failure of controls

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

An underwater photograph of a coral reef. The scene is dimly lit, showing various types of coral, including some with yellowish and pinkish hues. The background is dark and textured with coral and rocks.

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 detailed painting of several large wooden barrels, each overflowing with stacks of various banknotes and coins. The barrels are arranged in a row, and the money is piled high, spilling out of the tops. The scene is dimly lit, with a checkered floor visible in the foreground. The overall tone is dark and somber, suggesting a hidden or underground vault of wealth.

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 featuring two dragons. The dragon on the left is green and yellow, breathing a stream of fire towards the right. The dragon on the right is blue and green, also breathing fire. The background is a dark, swirling red and orange, suggesting a fiery or stormy sky. In the lower right, a group of figures in yellow robes are visible on a cloud. The text "Failure is inevitable. Mean Time to Failure is unrealistic & inhibits change" is overlaid in the center.

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 close-up of a workspace covered in colorful paint splatters. Several tubes of acrylic paint are lying on the surface, some with their caps removed. A paint palette with various colors is visible in the lower right corner. The overall scene suggests a creative and experimental environment.

Failures are treated as learning opportunities for improvement.

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



Measuring InfoSec Programs

An abstract painting with a complex, layered composition. It features bold, expressive brushstrokes in a variety of colors including deep blues, purples, yellows, and reds. The forms are organic and somewhat chaotic, with some areas appearing more defined than others, creating a sense of depth and movement. The overall texture is rich and painterly.

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 dark, moody oil painting of two bottles on a table. The bottle on the left is dark and slender, while the one on the right is shorter and wider. The background is a textured, dark brown and grey wash. The lighting is low, creating deep shadows and highlighting the forms of the bottles. The overall tone is somber and contemplative.

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

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



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

Unpatched databases without authentication = high PPP

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

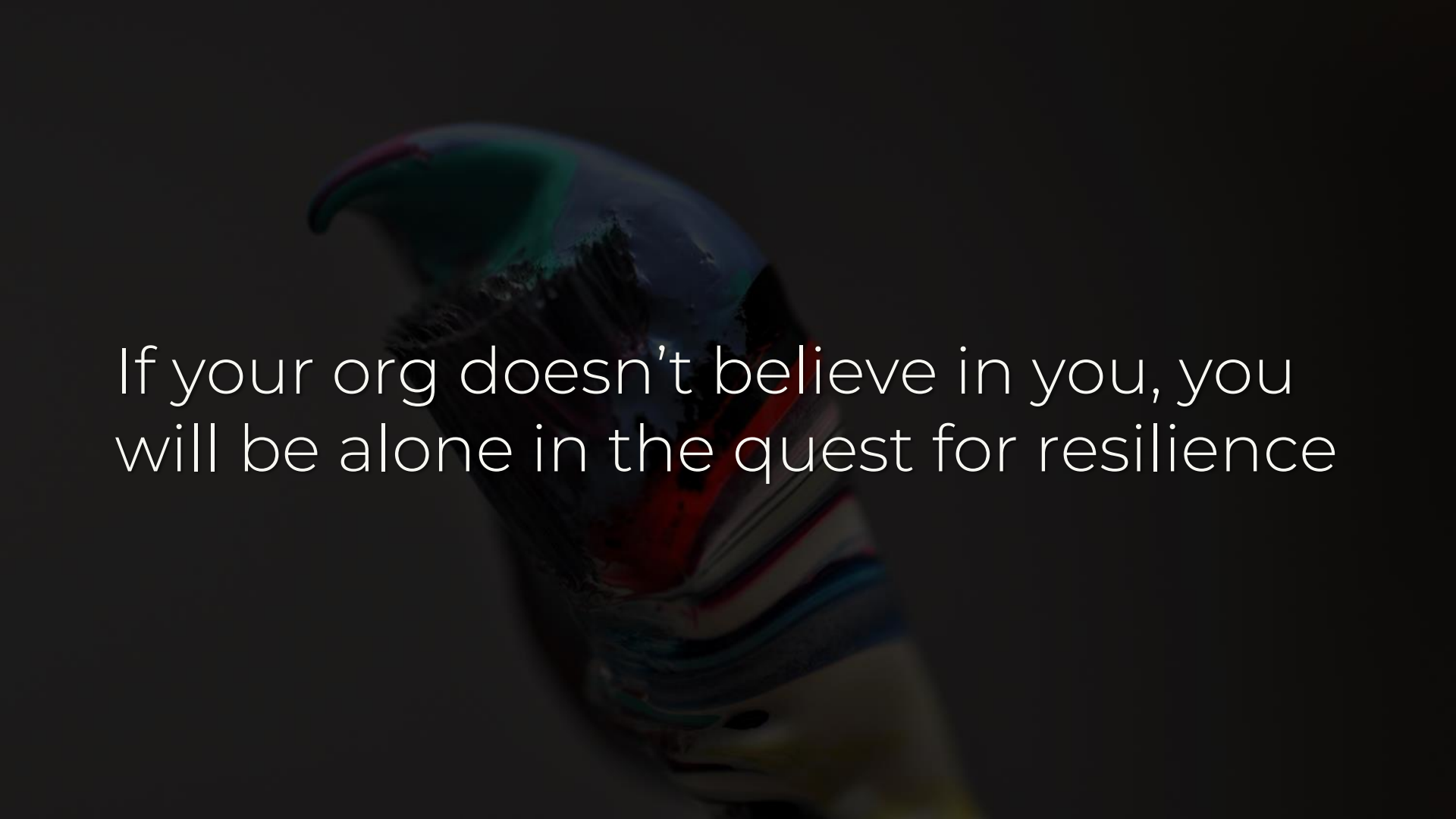


Equifax blamed one person for failing to deploy a patch.

Don't do that.

Net Promoter Score (NPS):
Mathematical calc of satisfaction

Measure NPS among your colleagues
& teams with whom you work

A vibrant parrot with a blue head, red beak, and multi-colored body (red, yellow, green, and blue) is perched on a dark branch. The parrot's head is turned back, looking over its shoulder. 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

The background of the slide is a photograph of a wall. The wall is covered with a grid of rectangular panels, likely made of wood or plaster. The panels are arranged in two rows. The top row has five panels, and the bottom row has six panels. The panels are painted in various colors: yellow, orange, red, dark brown, and blue. Some panels are dark and textured, while others are lighter and smoother. The wall itself is aged and shows signs of wear, with some peeling paint and discoloration. The word "Conclusion" is written in white, sans-serif font across the middle of the image.

The background of the slide is a close-up photograph of marbled paper. The paper features a complex, organic pattern of swirling colors, including deep blues, greens, and earthy browns. The texture appears slightly rough and uneven, with various ridges and valleys. The lighting is somewhat dim, giving the colors a muted, vintage feel.

Measure **resilience** – flexibility,
adaptability, transformability



Measure how security is helping your
organization & protecting its goals

The background is a dark, textured surface covered in a dense pattern of colorful heart shapes. The hearts are drawn in various colors including white, yellow, blue, red, and pink. Some hearts are solid, while others are outlines. There are also vertical streaks of paint or ink dripping down the surface, adding to the abstract and artistic feel.

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

A circular artwork, possibly a ceramic plate or a framed painting, featuring a dark blue, textured background. Overlaid on this are several golden, branching, vein-like patterns that spread across the surface, resembling natural mineral inclusions or perhaps a stylized representation of a celestial body like a planet or a nebula. The patterns are irregular and organic in shape.

“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