

The background of the slide features a close-up of two hands clasped together in a firm grip. The lighting is dramatic, with a strong red glow on the right side and a blue glow on the left side, creating a high-contrast, moody atmosphere. The hands are the central focus, with the fingers interlaced.

# The Red Pill of Resilience

Kelly Shortridge (@swagitda\_)

COUNTERMEASURE 2017



Hi, I'm Kelly



SecurityScorecard



“The oak fought the wind and was broken,  
the willow bent when it must and survived.”



“The more you sweat in peace, the less you bleed in war.”

A person's back is shown from behind, with two circular cutouts. The cutout on the left shows a man's face holding a red pill. The cutout on the right shows the same man's face holding a blue pill. The background is dark and blurry.

Resilience is about accepting reality, and  
building a defensive strategy around reality

# Stages of Grief in InfoSec

## Etymology of Resilience

### The Resilience Triad:

- Robustness
- Adaptability
- Transformability

# Stages of Grief

A bouquet of red roses is the central focus of the image. The roses are covered in small, glistening water droplets, suggesting they are fresh or have been recently watered. The lighting is dramatic, highlighting the texture of the petals and the sheen of the water. The background is a deep, dark color, possibly black or very dark green, which makes the vibrant red of the roses stand out. The overall mood is somber and contemplative, fitting the theme of grief.

InfoSec is grieving that companies will never be invulnerable to attack



Denial – clinging to a false reality

“We aren’t really at risk”

Anger – frustration that denial can't go on

“It's your fault that I need security”

Bargaining – hope that the cause is avoidable

“Maybe we can stop attacks from happening”

Depression – despair over the reality

“We’re going to be hacked, why bother?”

Acceptance – embracing inevitability

“Attacks will happen, but I can be prepared”

A close-up photograph of a snake's head, showing its scales in shades of green and red. The snake's head is positioned in the center of the frame, with its mouth slightly open. The background is dark, making the snake's scales stand out.

Lack of acceptance feeds solution  
fragmentation, FUD, and snake oil

Security nihilism isn't the answer.

Resilience is.



# Etymology of Resilience



1858: Engineering – strength & ductility

20th Century: Psychology, ecology, social sciences, climate change, disaster recovery

The background of the slide is a deep space image. It features a dense field of stars of various colors, including white, yellow, and red. A prominent feature is a large, glowing red nebula located in the lower-left quadrant, with some blue and white highlights within its structure. The overall color palette is dominated by dark blues, blacks, and reds, with scattered points of light from distant stars.

# Resilience in Complex Systems

Non-linear activity in the aggregate

Intertwined components, unpredictability

Infosec is a complex system.

Defenders, attackers, users, governments,  
software vendors, service providers, ...



Ecological resilience

Continually adapt; high degree of instability



Chestnut trees in eastern North America's forests were wiped out by chestnut blight  
Oak and hickory trees grew in their stead

Evolutionary resilience assumes socio-ecological systems are co-evolutionary



Communities can diversify agricultural  
landscapes and production systems



Three central characteristics of resilience:  
Robustness, Adaptability, Transformability



Hurricane Harvey – primary damage was flooding from ongoing rain, not storm surges

A photograph of a long, narrow path lined with red torii gates, illuminated by a lantern. The path is paved with stone tiles and leads into the distance. A single lantern hangs from the top of one of the gates. The scene is dimly lit, with the red of the gates being the primary color.

Resilience is about the journey, not the destination

Accept **the risk will exist**

Reduce potential damage & restructure  
around the risk



“A building doesn’t care if an earthquake or shaking was predicted or not; it will withstand the shaking, or it won’t.”

– Susan Elizabeth Hough

Survival rests on embracing the unknown  
and accepting that **change is inevitable**



Robustness

**Robustness:** withstanding and resisting  
a.k.a. “engineering resilience”



Safe development paradox: stability allows risk to accumulate, compromising resilience

Focus on just engineering resilience leads to  
a maladaptive feedback loop



Suppressing fires in fire-adapted forests  
leads to a build up of fuel over time

Patching & retroactive hardening of vuln-prone systems **accumulates risk**

A photograph showing a row of red sandbags used as a levee. The sandbags are stacked in two rows, with water splashing over the top. The water is dark and turbulent, contrasting with the bright red of the sandbags. The background is dark and indistinct.

Levees support further human development  
in at-risk floodplains

“Don't treat the symptoms of bad planning  
with structures”

Technical controls shouldn't allow exemption from cyber insurance requirements

Artificially creating a stable environment  
makes the system **less adaptive to disruption**



An underwater photograph showing a rocky seabed covered with coral and seaweed. The coral appears somewhat bleached or stressed, with a mix of dark and light colors. The seaweed is dark and dense. The water is dark and slightly hazy. The text is overlaid in the center of the image.

Coral in marine preserves are less resilient to climate disturbance than “stressed” coral

Design & test internal systems with the same threat model as externally-exposed ones



Problem: infosec is exclusively focused on robustness – how to stop / thwart / block

Infosec's current goal is to return to  
“business as usual” post-breach.


There is no such thing.

Other domains tried defying nature – it doesn't work

Your systems must survive even if users click on phishing links and download `pdf.zip.exe's`



Robustness is effective when you have  
diverse and layered controls

A photograph of the New York City skyline at sunset. The sky is a deep, dark orange-red, and the buildings are silhouetted against it. The Freedom Tower is the most prominent building in the center. The water in the foreground is dark, with a few small white sails visible.

NYC's excess heat guidelines: backup hybrid-power generators, heat-tolerant systems, window shades, high-performance glazing



Diversity helps provide **redundancy** in  
uncertain conditions



APT BlinkyBox™ doesn't help when legit  
creds are used to access a cloud service

EMERSON  
Network Power

HEMULEX



Schneider



EMC

EMERSON  
Network Power

HEMULEX

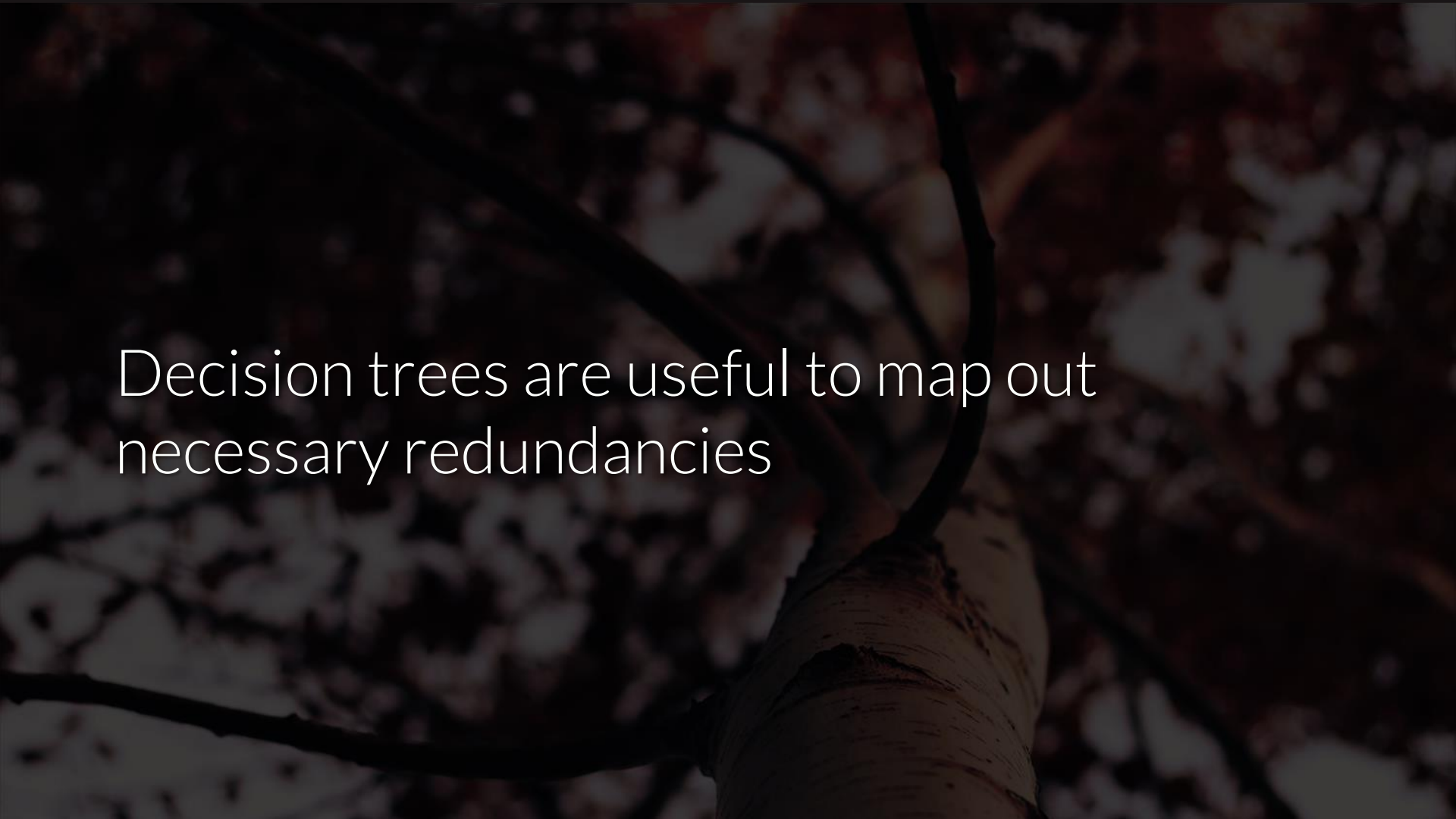


Don't ignore correlated risk.

Fragmentation can inject a healthy level of instability to foster resilience.

Pitfall of efficiency: more limited space in which your operations can survive

Up for debate: **manageability** via uniformity  
vs. **minimized impact** via diversity?

A dark, low-key photograph of a tree trunk and branches, serving as a background for the text. The tree trunk is the central focus, with several branches extending outwards. The lighting is dramatic, highlighting the texture of the bark and the silhouettes of the branches against a dark, blurred background.

Decision trees are useful to map out  
necessary redundancies

Raising attacker cost is the bridge from  
robustness to adaptability



“Attackers will take the **least cost path** through an attack graph from their start node to their goal node.”

– Dino Dai Zovi



Adaptability



*Adaptability*: reduce costs and damage incurred, while keeping your options open

Intergov't Panel on Climate Change (IPCC):

Incremental change creates a false sense of security – goal is **managed transformation**

A large herd of wildebeest is captured in the middle of crossing a river. The animals are densely packed, with some in the water and others on the muddy bank. The scene is set in a natural, open landscape under a hazy sky. The overall color palette is a warm, monochromatic brown, which serves as a background for the white text.

Preserving habitats is unnatural &  
counterproductive.

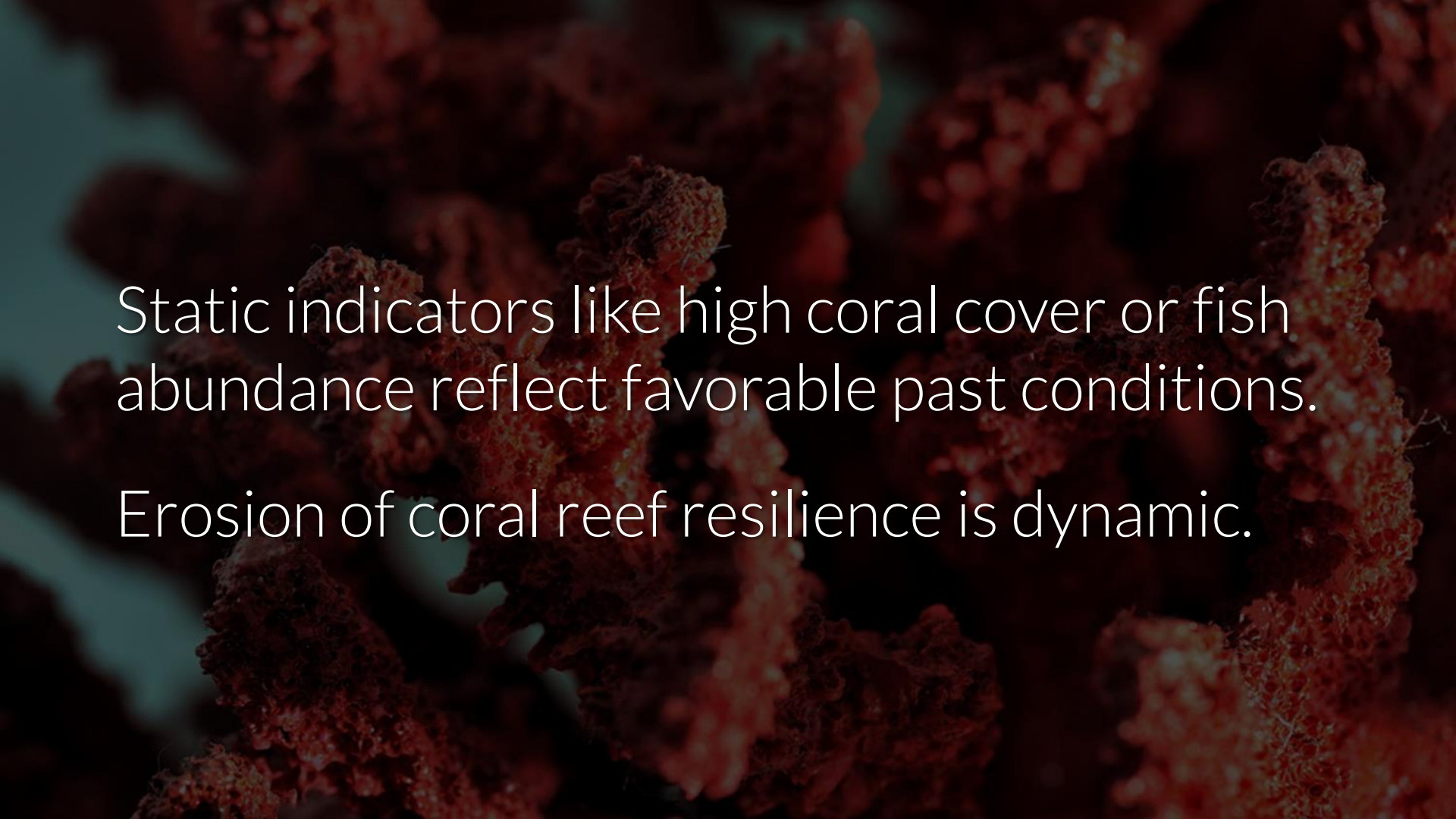
Wildlife naturally “tracks” ideal conditions.

Legacy systems are like preserved habitats.

We need to be able to *migrate* to better conditions.

Example: patching inline PHP code

Instead: single class for DB queries



Static indicators like high coral cover or fish abundance reflect favorable past conditions.

Erosion of coral reef resilience is dynamic.

Ensure your threat models aren't based on favorable past conditions





Survival strategy: comingle warm-adapted species with cold-adapted cohorts

A row of red telephone booths on a city street at night. The booths are illuminated from within, and the word 'TELEPHONE' is visible on the top of each booth. The background is a dark, multi-story building.

Apps built with legacy systems and libs will not survive in an increasingly open API world

Uncertainty and surprise must be baked into  
your approach

Test adaptability to attacker methods with  
attack simulation or auto playbook testing

A close-up photograph of a monkey's face, focusing on the eye and ear area. The monkey has dark, coarse fur on its head and a prominent, bright red patch of skin around its eye and ear. The monkey's eye is partially closed. The text "Chaos Monkey" is overlaid in white, sans-serif font in the center of the image.

Chaos Monkey

Randomly kills instances to test their ability to withstand failure.

It also makes persistence really hard.

Design your security architecture for survival even if individual controls fail

Rethinking security architecture is hard.

The industry offers too much complexity.



APPROVED FOR TRANSPORT  
 UNDER CUSTOMS SEAL

USA 109-12763-01

TYPE (R410A) MANUFACTURED BY SA...  
 OF THE CONTAINER

DESIGNED AND MANUFACTURED BY  
 WITTENBERG CONTAINER SYSTEMS, DIVISION  
 OF FORT WORTH, TEXAS, U.S.A.  
 Not to be used in a capacity different  
 or for use in other than intended applications.

THIS CONTAINER SYSTEM  
 HAS BEEN APPROVED BY  
 THE U.S. CUSTOMS SERVICE  
 MANUFACTURED BY  
 WITTENBERG CONTAINER  
 SYSTEMS, DIVISION

CSC SAFETY APPROVAL  
 5-01/12/12-251

ACEP  
 JIS  
 1-28-1  
 07/08

TYPE MANUFACTURED BY  
 WITTENBERG CONTAINER SYSTEMS, DIVISION  
 OF FORT WORTH, TEXAS, U.S.A.

DESIGNED AND MANUFACTURED BY  
 WITTENBERG CONTAINER SYSTEMS, DIVISION  
 OF FORT WORTH, TEXAS, U.S.A.

THIS CONTAINER SYSTEM  
 HAS BEEN APPROVED BY  
 THE U.S. CUSTOMS SERVICE  
 MANUFACTURED BY  
 WITTENBERG CONTAINER SYSTEMS, DIVISION



# Containers

Containers promote adaptability and support transformability

@jessfraz | [blog.jessfraz.com/post/talks](https://blog.jessfraz.com/post/talks)

Containers = “isolated, resource-controlled,  
and portable runtime environments”

Easier to determine root cause

Easier to transport to better infrastructure

Easier to kill the infection & stop spread



Ongoing stress like ocean warming or overfishing makes coral less resilient in the face of cyclones or coral bleaching events

Complexity will erode your resilience in the face of new vulns or data breaches

Transformability



Transformability = challenge existing assumptions & reorganize your system



Prior example: inline code makes it difficult to reorganize your system vs. a single class



In disaster recovery policy, ideal is to change location & remove urbanization

2011: 6.3mms earthquake hit Christchurch

Cost to rebuild of \$40bn+



NZ designated a “red zone” where land is too vulnerable & where rebuilding is uneconomic

Identify the red zones within your IT systems

Choose your own infosec redzone criteria:

Publicly exposed, legacy systems, critical data, privileged access, overly verbose, single point of failure, difficult to update, ...

Example: API consuming critical data should be in “red zone” whether it has vulns or not

Identify assets that fall under your red zone criteria & migrate them to a safer system




Example: Planned decommission of levees to assist migration

Prohibits becoming a permanent “fix”



Continually consider how you can prepare in advance for migration

A photograph of two women sitting at a table, looking at a laptop. The woman on the left has braided hair and is wearing a white shirt. The woman on the right has long dark hair and is wearing a red top. They are both smiling and appear to be in a collaborative work environment. The background is slightly blurred, showing office furniture like chairs and tables.

Complex systems require collaborative  
planning across stakeholders

Open sharing of protections in place, what risk remains, uncertainties in the approach

Partner with engineering – they benefit from flexibility and transformability as well



Your role is to manage state transitions.

Consider how a resilience approach fits into engineering workflows.

2FAC @ Facebook: integrated 2FA into dev workflows without creating friction

A top-down view of a group of people's hands, all holding red hearts. The hands are arranged in a circle, with the palms facing up. The hearts are a vibrant red color and are held in various positions, some fully visible and others partially obscured. The background is dark, making the hands and hearts stand out. The overall mood is one of unity and care.

“You can actually implement security controls that affect every single thing people are doing and still make them love it in the process”



Find someone with whom to collaborate &  
how security can fit into their workflows

Ensure your org is learning from prior experiences – foster a security culture

Conclusion



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

Robustness is optimized through diversity of controls

Adaptability minimizes the impact of an attack and keeps your options open

Transformability demands you challenge  
assumptions & reorganize around reality



“The history of evolution is that life escapes all barriers.

Life breaks free. Life expands to new territories. Painfully, perhaps even dangerously.

But life finds a way.”





Attacks will evolve. We can evolve, too.

Let's strive for acceptance of our grief, and  
architect *effective* and *realistic* defense

A fluffy black and white cat is wearing a red fire chief hat with a white shield-shaped patch on the front that says "FIRE CHIEF" in black letters. The cat is sitting on a red surface, and a yellow stuffed mouse is visible to its right. The background is blurred, showing what appears to be a fire truck.

The blue pill relegates us to the role of a firefighting cat who's drunk on snake oil

Instead of accepting snake oil, take the red pill of **resilience** instead



“Good enough is good enough. Good enough  
always beats perfect.”

– Dan Geer



@swagitda\_



/in/kellyshortridge



kelly@greywire.net

# Suggested Reading

- Engineering resilience versus ecological resilience
- Resilience and disaster risk reduction: an etymological journey
- A strategy-based framework for assessing the flood resilience of cities – A Hamburg case study
- Vulnerability, Resilience, and the Collapse of Society
- Are some forms of resilience more sustainable than others?
- Flood Resilience: a Co-Evolutionary Approach
- The oak or the reed: how resilience theories are translated into disaster management policies
- Rethinking Ecosystem Resilience in the Face of Climate Change
- Building evolutionary resilience for conserving biodiversity under climate change
- Complexity and Planning: Systems, Assemblages and Simulations
- [“Windows Containers”](#) by Microsoft
- [“The Netflix Simian Army”](#) by Netflix