



# The Red Pill of Resilience

Kelly Shortridge (@swagitda\_)

Rochester Security Summit 2017

A gray tabby kitten is standing in a field of autumn leaves. The leaves are mostly red and brown, with some yellow. The kitten is looking towards the right. A wire fence is visible in the background.

Hi, I'm Kelly

Resilience begets deterrence





“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 dark, moody photograph of a man's face, looking directly at the camera. Two circular insets are overlaid on the image. The left inset shows the man's hand holding a red pill. The right inset shows the man's hand holding a blue pill. The background is dark and textured.

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



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, likely a green tree python, showing its vibrant green and red scales. The snake's head is positioned in the center, with its mouth slightly open, revealing a red interior. The background is dark and out of focus, emphasizing the snake's head. The text is overlaid on the left side of the image.

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





# 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



Resilience is about the journey, not the destination

Accept the risk will exist

Reduce potential damage & restructure  
around the risk

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 red inflatable flood barrier, composed of several cylindrical segments, is positioned horizontally. A large, dynamic splash of water is breaking over the left side of the barrier, creating a misty spray. The foreground is filled with dark, turbulent water. The background is dark and indistinct, suggesting an outdoor setting at night or in low light.

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

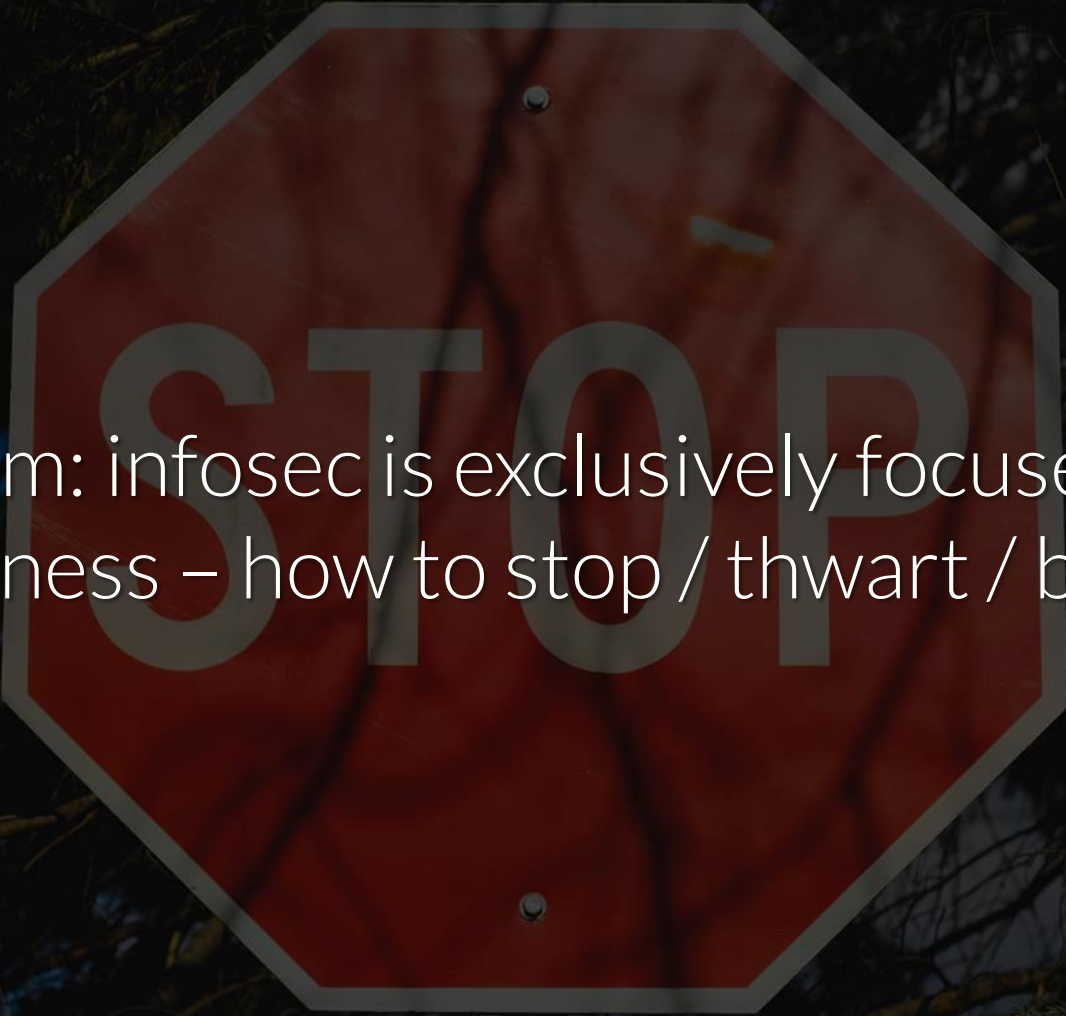


Artificially creating a stable environment  
makes the system less adaptive to disruption

An underwater photograph showing a rocky seabed covered with dark green seaweed and patches of coral. The water is dark and slightly murky, with some light reflecting off the rocks and coral. The overall tone is somber and naturalistic.

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 with scattered clouds. The city's skyscrapers are silhouetted against the bright horizon, with some windows glowing with light. The Freedom Tower is the most prominent building in the center. In the foreground, the dark water of the harbor is visible, with a few small boats and a sailboat on the left.

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

Diversity helps provide redundancy in uncertain conditions



A person wearing a red hoodie and glasses is sitting in a dark room, looking at a laptop. The background is dark with a grid overlay. The text "APT BlinkyBox™ doesn't help when legit creds are used to access a cloud service" is displayed in white. At the bottom, there is a dark bar with various logos including Emerson, Memulex, HP, Intel, and others.

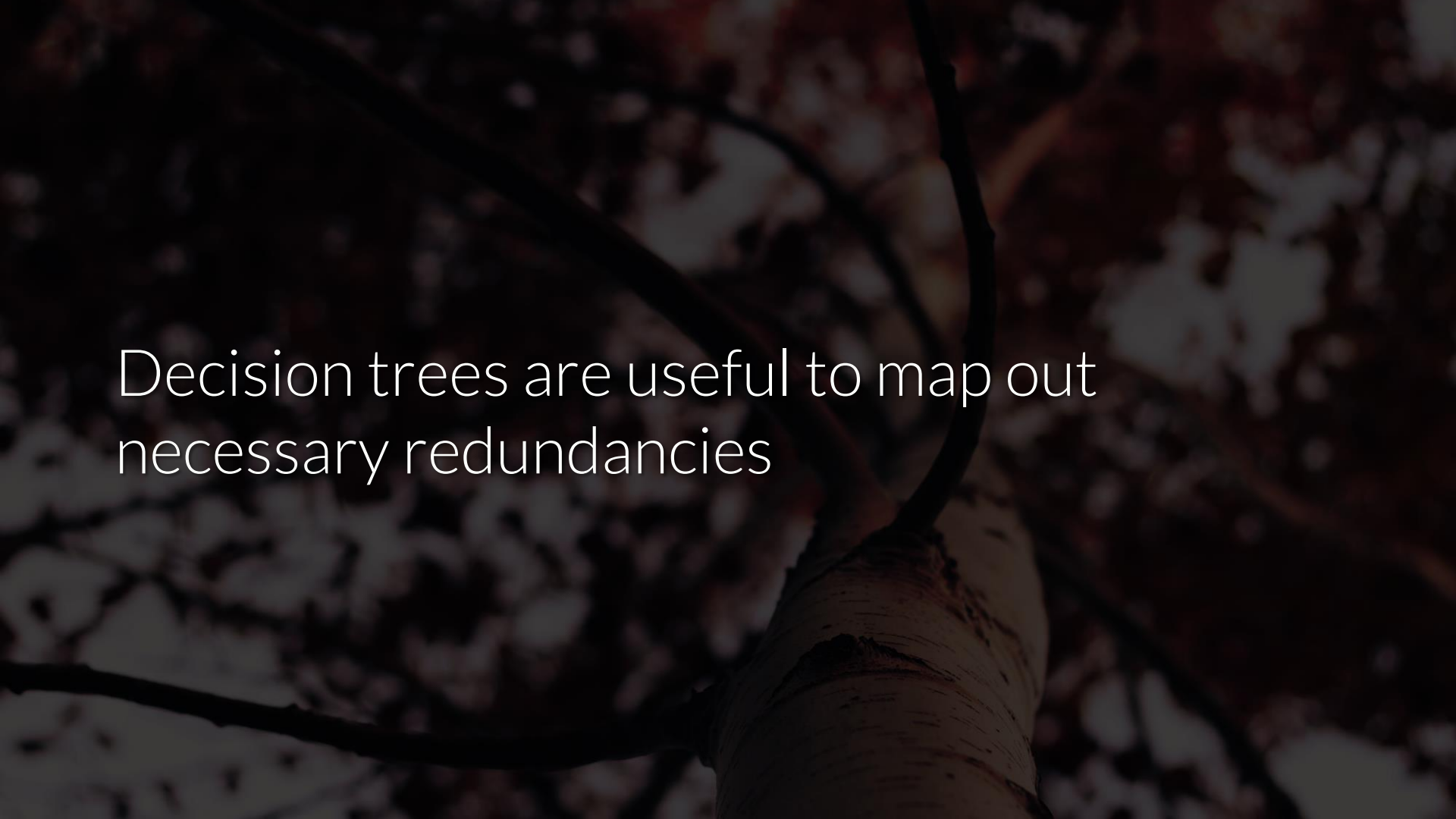
APT BlinkyBox™ doesn't help when legit  
creds are used to access a cloud service

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?



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



Preserving habitats is unnatural &  
counterproductive.

Wildlife naturally “tracks” ideal conditions.

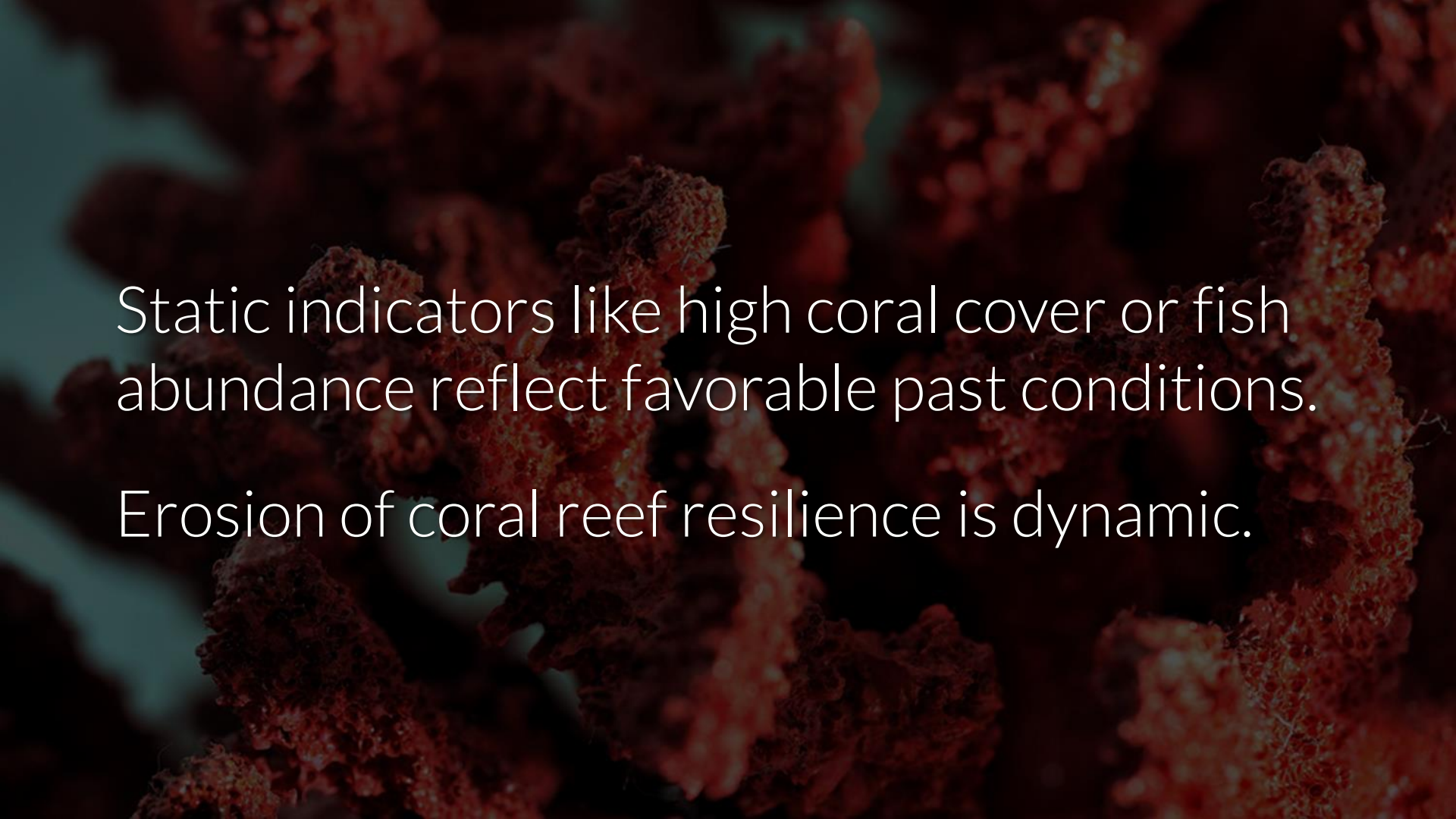
Legacy systems are like preserved habitats.

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



Example: patching inline PHP code

Instead: single class for DB queries

A close-up photograph of a coral reef, showing the intricate, porous structure of the coral. The image is dark and moody, with a reddish-brown hue. The text is overlaid on the image, providing information about coral reef indicators and resilience.

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

A close-up photograph of a branch from a cold-hardy plant, possibly a holly, covered in a thick layer of white frost. Several bright red berries are visible, partially obscured by the frost. The background is blurred, showing more frost-covered branches.

Survival strategy: combine 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 shows a brick building and a street lamp.

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 Chaos Monkey, a species of macaque known for its bright red face and chest. The monkey's face is the central focus, with its eyes partially closed and its mouth slightly open. The surrounding fur is dark and textured. The text "Chaos Monkey" is overlaid in the center in a white, sans-serif font.

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.





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

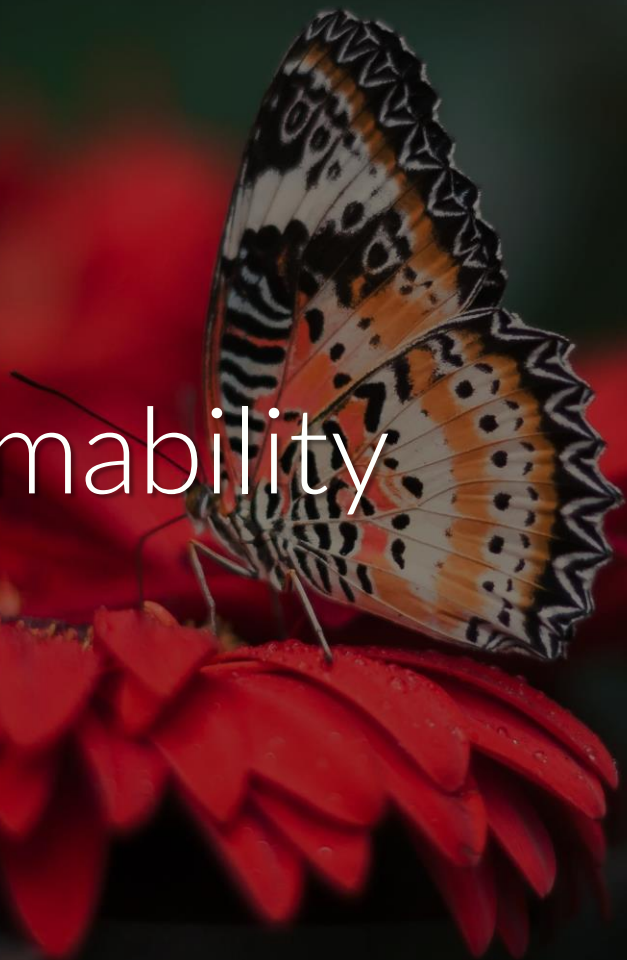
Easier to kill the infection & stop spread



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

A close-up photograph of four circular red emergency lights mounted on a metal surface. The lights are arranged in a 2x2 grid. The top-left light is partially obscured by a dark, irregular shape. The metal surface is light-colored and shows signs of wear, including scratches and small holes. The text is overlaid in the center of the image.

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

2011: 6.3mms earthquake hit Christchurch

Cost to rebuild of \$40bn+

A photograph of a 'DANGER' sign with a large exclamation mark inside a red triangle, mounted on a chain-link fence. The sign is white with a red border and the word 'DANGER' in bold red letters. The background is a blurred chain-link fence.

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”

A group of Maasai people, including men, women, and children, are walking in a dusty, open landscape. They are wearing traditional red and blue patterned shuka robes. Many are holding long wooden staffs. The scene is captured in a cinematic style with a slightly desaturated, warm tone. The text "Continually consider how you can prepare in advance for migration" is overlaid in white, sans-serif font across the middle of the image.

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 dark skin and long braids, wearing a white shirt and large hoop earrings. The woman on the right has light skin and long dark hair, wearing a red top. They are both smiling and looking at the laptop screen. The background is a blurred office or meeting space with 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 close-up photograph of several hands reaching towards the center, with red paint smeared on the palms, creating a circular pattern. The background is dark, and the lighting highlights the texture of the skin and the vibrant red of the paint.

“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 close-up photograph of a cat's head, wearing a red fire chief's hat. The hat has a white shield-shaped patch on the front with the words "FIRE" and "CHIEF" in black. The cat has dark fur around its eyes and ears, and white fur on its face. It is sitting next to a red fire truck, which is partially visible in the background. A yellow mouse toy is also visible on the right side of the frame. The text "The blue pill relegates us to the role of a firefighting cat who's drunk on snake oil" is overlaid on the image in white.

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

A close-up photograph of a single red rose. The rose is in full bloom, with its petals tightly curled in the center and gradually unfurling outwards. The petals have a rich, deep red color with some darker, almost black, shadows in the folds, giving it a three-dimensional appearance. The background is a solid, dark black, which makes the red of the rose stand out prominently. The lighting is soft, highlighting the texture of the petals.

“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