

A monarch caterpillar with yellow, black, and white stripes is crawling on a green, needle-like plant stem. The background is a soft-focus green.

# THE VERY HUNGRY DEFENDER: METAMORPHOSING SECURITY DECISION-MAKING BY INCORPORATING OPPORTUNITY COST

Kelly Shortridge @swagitda\_ | shortridge@hachyderm.io

USENIX Enigma 2023

A monarch caterpillar is shown hanging upside down from a green stem. The caterpillar has a black and white striped pattern with yellow spots. It has two long, thin black antennae. The background is a soft, out-of-focus green.

Infosec involves decisions about balancing costs that influence defensive outcomes

A close-up photograph of a monarch butterfly pupa (chrysalis) hanging from the underside of a green leaf. The pupa is translucent, showing the developing adult butterfly inside. The background is a solid, light blue color.

In cybersecurity decision making today, we often ignore what might have been

A close-up photograph of a bumblebee on a purple flower. The bee is positioned in the lower right quadrant of the frame, facing left. The flower is a dense cluster of small purple blossoms with a prominent, fuzzy, yellowish-green central structure. The background is a soft, out-of-focus green, suggesting foliage. Overlaid on the image is white text that reads: "When we expend resources on X, we inherently cannot expend them on Y".

When we expend resources on X, we inherently cannot expend them on Y

A dark, textured branch of a tree or shrub is the central focus, extending from the top left towards the bottom right. A small cluster of pink and white flowers, some in full bloom and some as buds, is attached to the branch. Several green leaves are also visible near the flowers. The background is a dark, gradient blue-grey.

We are very hungry defenders; alas, the world only offers finite, scarce resources

A monarch caterpillar with yellow, black, and white stripes is crawling on a large green leaf. The background is a soft-focus green, suggesting a natural outdoor setting.

Opportunity cost: the loss of potential gain from other alternatives when one is chosen

A monarch butterfly with vibrant orange wings and black veins is perched on a cluster of small purple flowers. The background is a solid, dark green color. The text is overlaid on the butterfly's wings.

How can we apply opportunity cost to metamorphize our defensive strategy?

I. On Opportunity Cost

II. The Spectrum of Costs

III. Case Study: AppSec



# I. On Opportunity Cost



OC: The loss of potential gain from other alternatives when one alternative is chosen

A close-up photograph of a monarch caterpillar chrysalis (pupa) hanging from a green leaf. The chrysalis is yellow with black and white markings. The background is a blurred green leaf.

Time pressure, tunnel vision, and info bias  
derail critical thinking during crisis

Opportunity cost applies across problem domains – let's extract their lessons learned

Opportunity cost should be considered in *every* cybersecurity decision...

A photograph of two birds, likely weavers, building a nest. The nest is a complex, woven structure of green grass, hanging from a branch. One bird is perched on the upper part of the nest, while the other is on the lower part, with its wings spread as if working on the structure. The background is a soft-focus green, suggesting foliage.

Buy a commercial solution to intrusion detection or spend time building our own?

Do we need expensive software at all or should that money be spent on chaos engineering and automated recovery?

A close-up photograph of a green caterpillar with yellow spots and black dots on its back, crawling on a green leaf. The caterpillar is positioned horizontally across the middle of the frame. The leaf is vibrant green and has a prominent vein structure. The background is dark and out of focus.

Should we create new procedures or ensure existing ones are standardized and documented so teams can self-serve?



If we spend resources on supply chain attacks but social eng pwns us, we suffer

A butterfly with dark wings and orange spots is perched on a pink flower. The background is a solid green color. The text "Incorporating OC helps us minimize attack impact and maximize company productivity" is overlaid on the image in white font.

Incorporating OC helps us minimize attack impact and maximize company productivity

A close-up photograph of a colorful caterpillar, likely a monarch caterpillar, resting on a green plant stem. The caterpillar has a pattern of black, green, and orange stripes and spots. The background is a blurred green, suggesting a natural outdoor setting.

## II. The Spectrum of Costs



What is the value of reading a book for 2 hours vs. practicing the violin for 2 hours?

We can answer these questions, even if we don't have precise, absolute dollar values

Prompts to think about alternatives at all is a key improvement in our decision-making



# Costs & Effects in Infosec

How do we elucidate the bigger picture of a decision?



Map the potential costs & effects of security investments – including *not* pursuing them

## - COSTS

### Tangible Costs

#### Organizations:

- Wages of security personnel
- Capital costs (software or hardware investment)
- Overhead costs (tuning, maintenance, configuration)
- Service / outsourcing costs

### Intangible Costs

#### Employees:

- Time investment in security intervention
- Burnout (lack of meaning or perceived lack of impact)
- Cognitive overload (task switching)
- Lack of perceived "flow" (wait time, number of interruptions)
- Cynicism, exhaustion
- Workplace conflicts / friction

#### Organizations:

- Productivity loss from implementing intervention
- Time to plan and execute intervention
- Delayed time to market
- Increased attrition
- Curtailed innovation

#### Society:

- Consumer workload & anxiety
- Efficiency loss of public funds
- False sense of security
- National security risk from 3rd parties (defense industry)
- Research costs

## + EFFECTS

### Productivity Effects

#### Employees:

- Satisfaction (perception of work)
- Efficacy (availability of resources needed to get their work done)
- Less burnout and stress
- Collaboration, reduced conflicts
- Efficiency and perceived flow
- Standardized, less manual work (fewer mistakes, less toil)
- Faster, empowering onboarding

#### Organizations:

- Product quality gains (reliability, service health, number of bugs)
- Faster time to market
- Incident reduction (impact / severity, volume, duration)
- Speed of change integration
- Turnover and attrition reduction
- Learning culture (innovation, knowledge discoverability)
- Activity volume (PRs, deploys, infrastructure utilization)

#### Society:

- More dependable digital services
- Macroeconomic effects
- Reduced identity theft and fraud

### Tangible Benefits

#### Organizations:

- Revenue growth
- Customer satisfaction (renewals, expansion, feature adoption)
- Output gains (more software releases, more product lines)
- Profitability (doing more with less)
- Uptime (service availability)

### Intangible Benefits

#### Users:

- Enhanced user experience
- Reduced anxiety / worry about safety and privacy

#### Employees:

- More dedication, less cynicism
- Feeling that their work is meaningful and has impact
- Energized vs. drained

#### Organizations:

- Brand perception and corporate image
- Competitive advantage
- Compliance adherence
- Intellectual property
- Talent attraction and retention

### Tangible Savings

#### Organizations:

- Reduced headcount required
- Technology cost savings
- Compliance fines
- Incident response / crisis management retainer
- Insurance premiums

#### Society:

- Credit monitoring
- National security
- Consumer confidence given economic / political stability

# Tangible costs





# Intangible costs



# Productivity effects

# Tangible benefits




# Intangible benefits

# Tangible savings





The null baseline: what do you gain by *not* implementing the security measure?

A close-up photograph of two hummingbirds hovering near a cluster of pink, bell-shaped flowers. The birds have iridescent green and blue feathers. The flowers are covered in water droplets. The background is a soft, out-of-focus green.

Would developers be more productive?  
Would employees be less stressed?

Staying honest about what is *lost* when security is implemented opens our options

A close-up photograph of a large green leaf with several caterpillars of various colors (yellow, white, and black) feeding on it. The leaf has several holes eaten into it. The background is dark and out of focus, with some purple and orange colors visible. The text "Negative Externalities" is overlaid in white serif font in the center of the image.

# Negative Externalities

Externalities: the costs and benefits imposed on other entities by the choice



Classic example: pollution. The cost borne by the firm is much less than societal cost.

Appsec may impose negative externalities on SWE teams, the org, and customers



We should always consider how security adds burnout, conflict, disruption, etc.



The “shadow price”: a price that considers negative externalities and opportunity cost

A monarch butterfly with orange and black wings is perched on a cluster of small pink flowers. To the right, a honeybee is flying, carrying a small amount of pollen on its legs. The background is a soft, out-of-focus green.

In infosec, remember that a benefit for one stakeholder may beget a cost for another

What is the “shadow price” of each security mitigation in your organization?



Beyond Money

Monetary value matters, but “cost” is more than just money...

# Time



A detailed close-up photograph of a mechanical watch movement, showing several interlocking brass gears of various sizes. The gears are highly polished and feature fine teeth. The background is dark and out of focus, highlighting the intricate details of the watch mechanism. The lighting creates highlights on the metallic surfaces, emphasizing their texture and the precision of the craftsmanship.

# Cognition



Emotion



In infosec, stress from time pressure makes humans more likely to bypass security

A monarch butterfly pupa (chrysalis) is shown hanging from a thin, brown twig. The pupa is dark, almost black, with a translucent section in the middle that reveals orange and black patterns, likely the developing wings. The background is a warm, reddish-brown wood grain. The text "Example: what are the costs of moving to a disconnected development environment?" is overlaid in white on the left side of the image.

Example: what are the costs of moving to a disconnected development environment?

New hardware and increased IT support  
pale in cost vs. productivity and satisfaction

A close-up photograph of a butterfly with vibrant blue and orange wings, perched on a green stem. The background is filled with out-of-focus, colorful flowers in shades of purple, yellow, and red. The text is overlaid in the center of the image.

If devs can't query the internet (or copy + paste), new time investments emerge

Consider how else costs could be used & which option maximizes the org's outcomes

The image features four monarch butterflies in various stages of flight against a solid black background. The butterflies are positioned around the central text, with one in the top left, one in the top center, one in the bottom left, and one in the bottom right. Their wings are a vibrant orange with black veins and borders. The text 'The Thermodynamics of Cost' is written in a white, serif font, centered horizontally and partially overlaid by the butterflies' wings.

# The Thermodynamics of Cost

Energy within a system cannot be created or destroyed – but it is interchangeable

A close-up photograph of a hummingbird hovering near a cluster of purple flowers. The bird is in the foreground, facing right, with its wings blurred from motion. The flowers are in the background, also slightly blurred, creating a shallow depth of field. The overall scene is brightly lit, suggesting a sunny day.

Security programs can expend energy or absorb it within the organizational system.



Requiring users to be vigilant to phishing  
expends energy, which security absorbs



The energy expended by SWEs to triage bugs is absorbed by the security team

Think about where energy is expended and absorbed, and by whom, to spot OCs

A monarch caterpillar with bright green, black, and red markings is crawling on a brown stem. A spider web is visible in the upper left corner. The background is a soft-focus green field.

# III. Case Study: AppSec



An opportunity cost framing exposes overly prescriptive problem definition

“What SAST tool is best?” begets a narrow focal point and only prescribes SAST tools

Better: “How can we minimize the number of security bugs devs introduce into code?”

Best: “How do we minimize the impact of security bugs in code running in prod?”



A wooden bowl filled with water, containing a pink flower, a yellow leaf, and a white flower. The text "This allows us to allocate a finite pool of resources to a variety of alternatives." is overlaid on the image.

This allows us to allocate a finite pool of resources to a variety of alternatives.

Ephemeral infra, standardized libraries or patterns, isolation, chaos experiments...



The focal point is about the “true” outcome  
we seek in our decision problem

Our default tendency as humans is to remain “zoomed in” on a problem

A serene pond scene featuring several vibrant pink lotus flowers in various stages of bloom. The flowers are surrounded by large, dark green lily pads that float on the water's surface. The background is a soft-focus landscape of lush green trees and foliage, creating a peaceful and natural atmosphere. The water reflects the flowers and leaves, adding depth to the scene.

Which resort is best for a vacay? vs. what's the best option to reduce my stress?

Most organizations have a defined purpose to fulfill – and that mission *isn't* security

Work that doesn't directly support the org's purpose bears the OC of time, budget, and effort away from more purposeful work

A retail business lacks the internal skillsets of DBs, ad placement, and content delivery



A hummingbird with iridescent green and pink feathers is perched on a pink flower. To the left, a red liquid dispenser is partially visible. The background is dark green.

Instead: they can outsource to a platform service provider, adtech firm, and CDN

Their time & effort is better spent on retail business logic delivering value to end users

# IV. Conclusion



Opportunity cost must be considered in *every* cybersecurity decision



A close-up photograph of several butterflies with orange and black wings feeding on a cluster of small purple flowers. The background is a soft-focus blue sky. The text is overlaid in the center of the image.

We want to balance organizations' multi-faceted goals to nurture resilient operations

A hummingbird with iridescent green and brown feathers is shown in flight, hovering over a cluster of small, tubular yellow and orange flowers. The bird's wings are blurred, indicating rapid movement. The background is a soft, out-of-focus green.

We must recognize the many types of cost  
in cybersecurity decisions, beyond money

A vibrant blue butterfly with black and white markings on its wings, resting on a green leaf. The butterfly is the central focus, with its wings spread wide. The background is a soft, out-of-focus green, suggesting a natural, leafy environment. The text is overlaid on the butterfly's wings in a clean, white, sans-serif font.

Remember the “null baseline” heuristic:  
consider the option of doing nothing instead

A monarch butterfly is shown in three stages of its life cycle, hanging from a dark branch. On the left is a bright green caterpillar. In the center is a dark, segmented pupa. On the right is the adult monarch butterfly, displaying its characteristic orange and black wings. The background is a blurred indoor setting.

Incorporating opportunity cost in decision-making can become natural & accessible



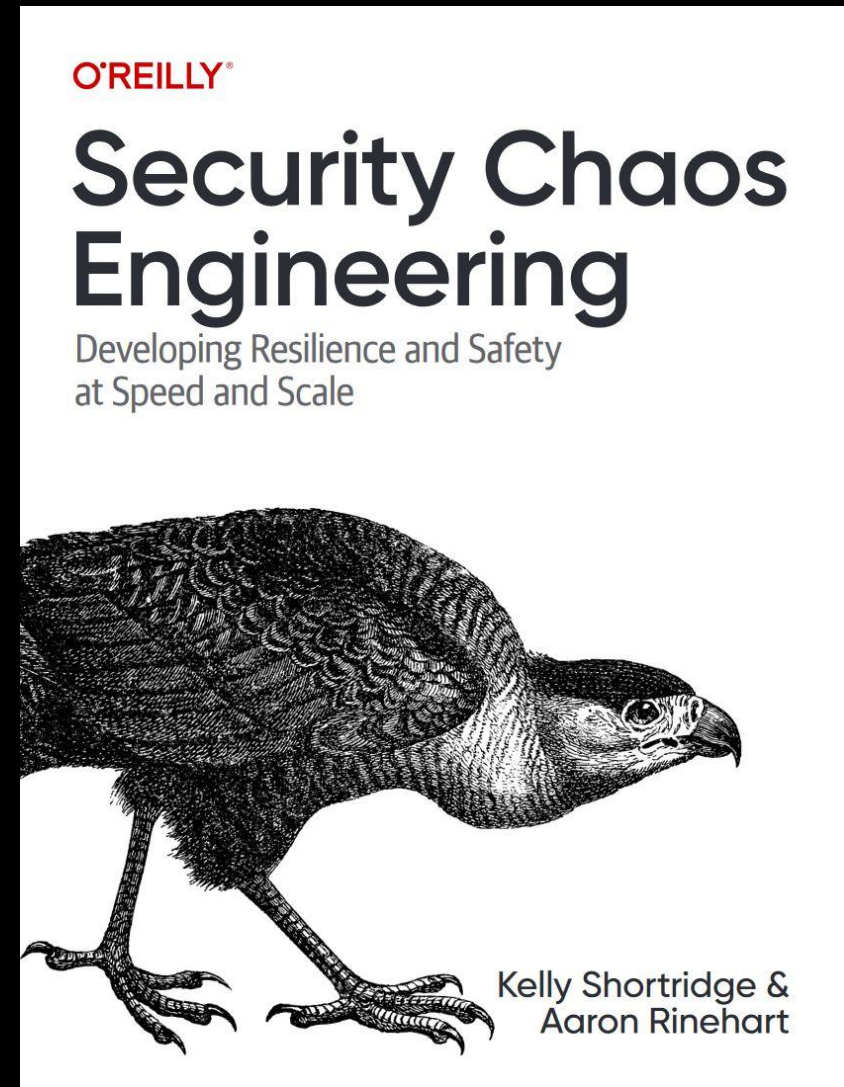
A close-up photograph of two butterflies with black and white patterned wings feeding on a cluster of small pink flowers. The background is a soft, out-of-focus green. The text is overlaid in white on the left side of the image.

How can we nurture the widespread inclusion of OC in research and practice?

Preorder the book &  
stay tuned for its  
release in Spring 2023:

[Bookshop](#)

[Amazon](#)





@swagitda\_



/in/kellyshortridge



shortridge@hachyderm.io



chat@shortridge.io