How can SRE help Security Governance ?

How to unstuck GRC with SRE

@madplatt

whoami

Director of Governance, Risk Management and Compliance for Security and Privacy @ LastPass

20+ years in tech, 18+ in Security. Penetration tester, Ops and Engineering, GRC and Leadership (Head of and CISO roles) and former consultant (vCISO/Interim CISO, Fractional CISO)
Project leader for “ASVS User Stories” open source project
Course instructor for “DevSecOps for Leaders” course on practical-devsecops.com
Speaker and enthusiast on Wardley Mapping, Cynefin framework, Safety Science, Resilience Engineering all applied to Security

the compliance guy?

really ?

What is GRC ?

“the integrated collection of capabilities that enable an organization to reliably achieve objectives, address uncertainty and act with integrity” from Wikipedia

Governance – aligning processes and actions with organisation’s business goals
Risk Management – identifying and addressing organisation’s risks
Compliance – ensuring activities meet legal, contractual and regulatory requirements

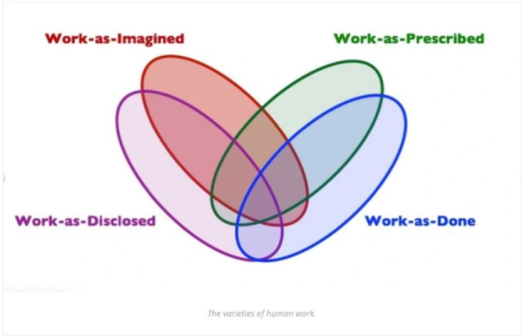
—

But… we’re a bit stuck… we are

The G & the C are stuck

- Stuck in command and control and centralised governance models
- Framing of the security “problem” as one of awareness, and not goal conflicts and trade-offs (that we’re often unqualified to appreciate)
- Detached from operational realities (hierarchical information filters)
- Actually fabricating business liabilities in the name of “best practice following”. Policies largely impractical

Stuck cat is stuck



Shorrock, Steven. “The varieties of human work” https://humanisticsystems.com/2016/12/05/the-varieties-of-human-work/

The R…. is also a bit stuck

Risk-management-as-Done

Org chart fence

Work as Imagined

Operation A
Team 1

Risk and
Compliance
Managers

Risk analysis
process

Controls Top Hat

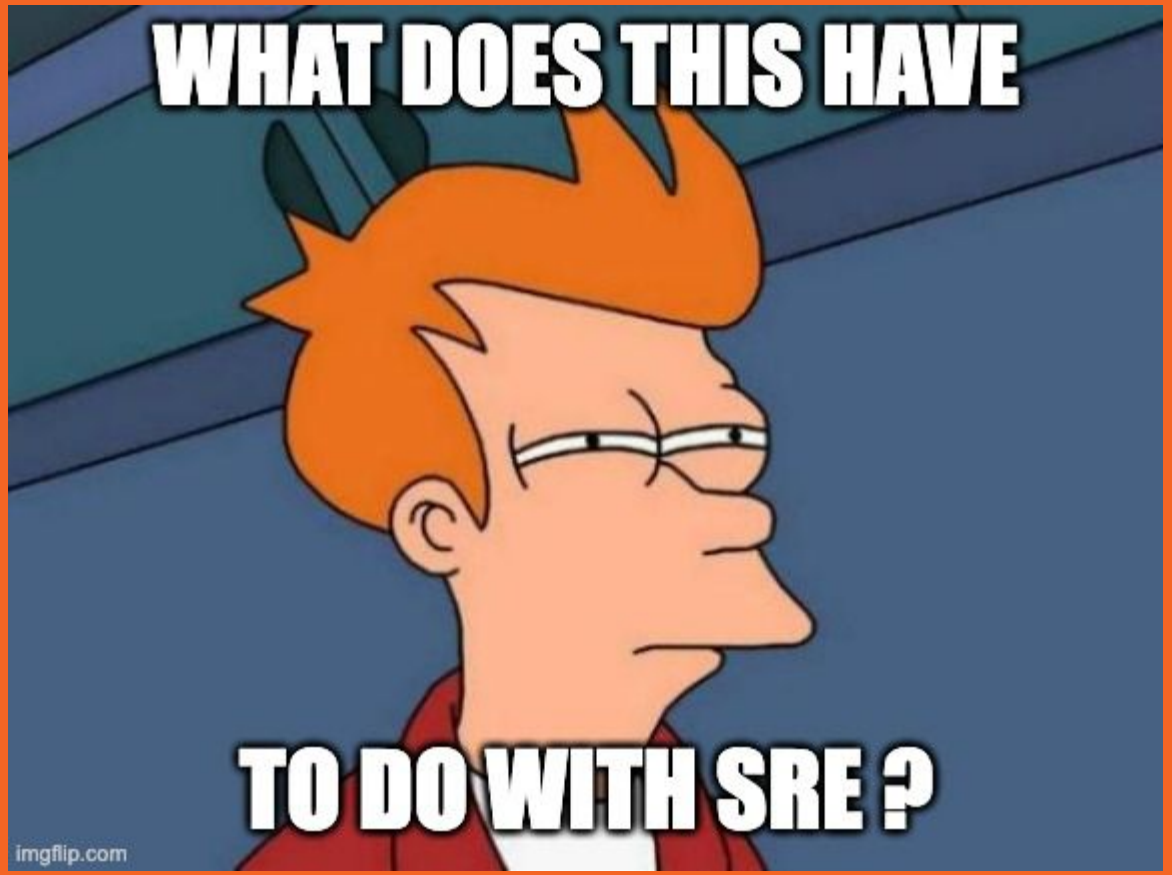
Operation B
Team 2

Training and
ingrained patterns
(bias)

Accepted Industry
best practices

"We see what we expect to see"

Stuck between what “oughta be” and “what actually is” and not knowing how to reconcile the difference constructively


WHAT DOES THIS HAVE
TO DO WITH SRE ?
imgflip.com

My soap-box schpiel:

The practices and structures to allow governance of technology, management of operational risk (including reliability) and enforce operational standards that SRE embeds... can be leveraged to manage security objectives, meeting and evidencing GRC goals

The G and the C often have broken team dynamics with Engineering

Control… blah blah ….. control…. Blah…. Governance… blah… Risks…. Blah… Compliance….blah blah Boogey man at the door

Control testing
Testing procedures
Evidence review
Checklists and spreadsheets
Compliance to
Risk analysis and uncertainty

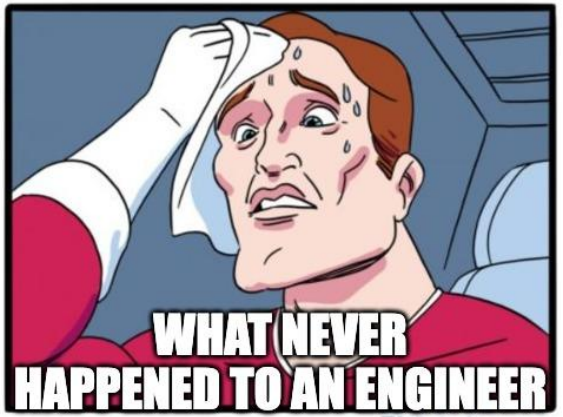
Wall of Confusion and Despair

Features… bah blah… that looks cool…. Blah blah… Speed…. Argh can't get that function to work blah blah They won't get out of the way…

Code
Tools
Processes and procedures
Delivery artefacts
Specifications
Sprints and Stories

@madplatt

Artefacts matter… they set the scene for collaboration (or lack thereof)



Having to ask the compliance team for feedback

Getting compliance feedback from CI/CD

@madplatt

SRE can help the G and the C

What's already there to leverage ?

- Answering "how much" through error budgets ,SLIs and SLOs
- Engineering and Ops know-how to understand constraints and trade-offs
- Levelled the playing field on Reliability concerns
- Readiness reviews and standards enforcement
- Managing toil
- Codification of policies in process

Between the C and the R - automated governance

Stage 1: Source Code Repository

Figure 4 shows a generalized overview of what an automated governance model might look like during the source code repository stage.

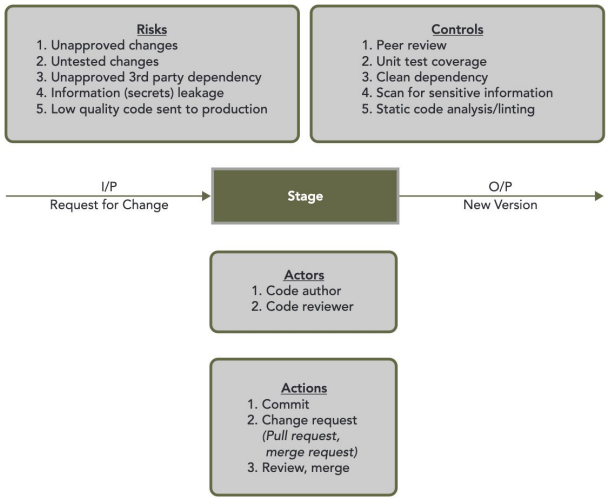
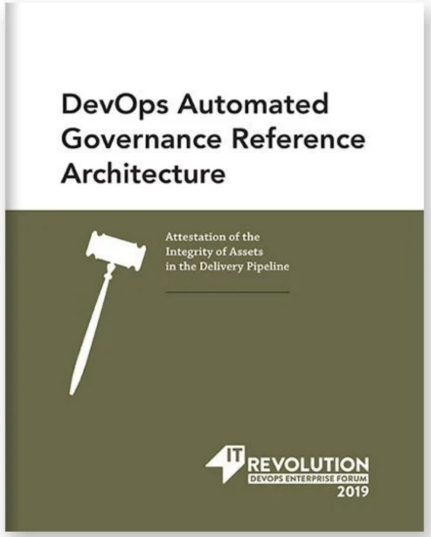


Figure 4: Governance during the Source Code Repository Stage

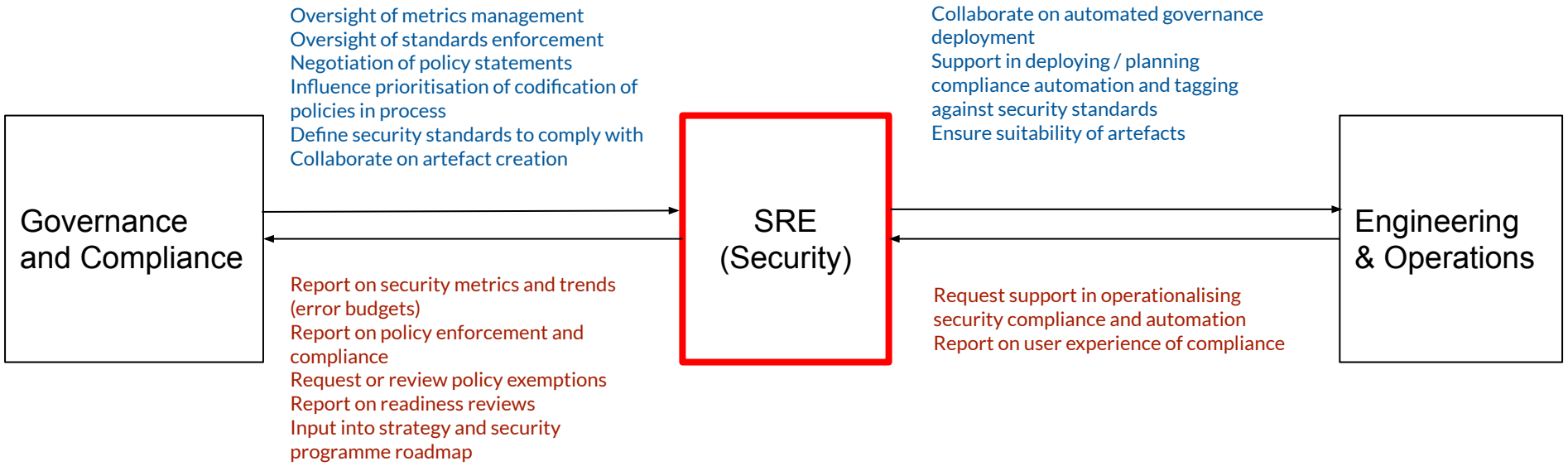


DevOps Automated Governance Reference Architecture

John Willis - https://jfrog.com/user-conference/devops-automated-governance/

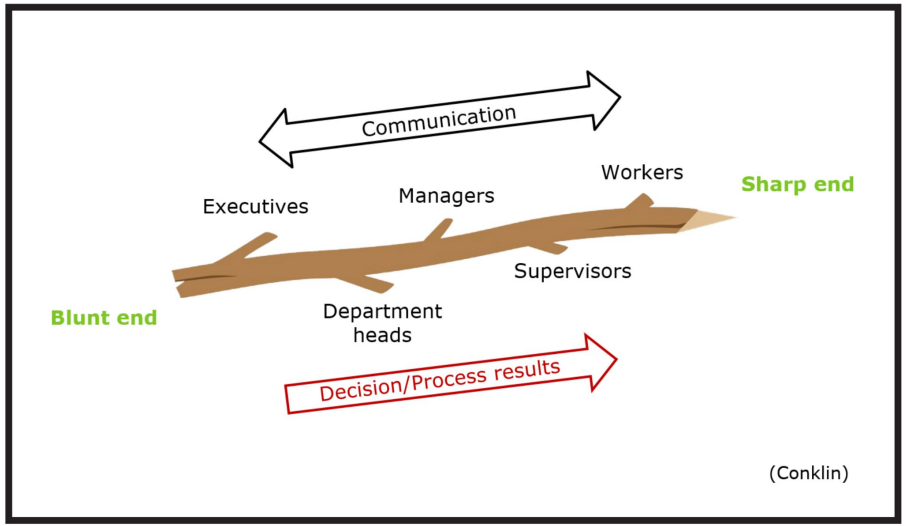
@madplatt

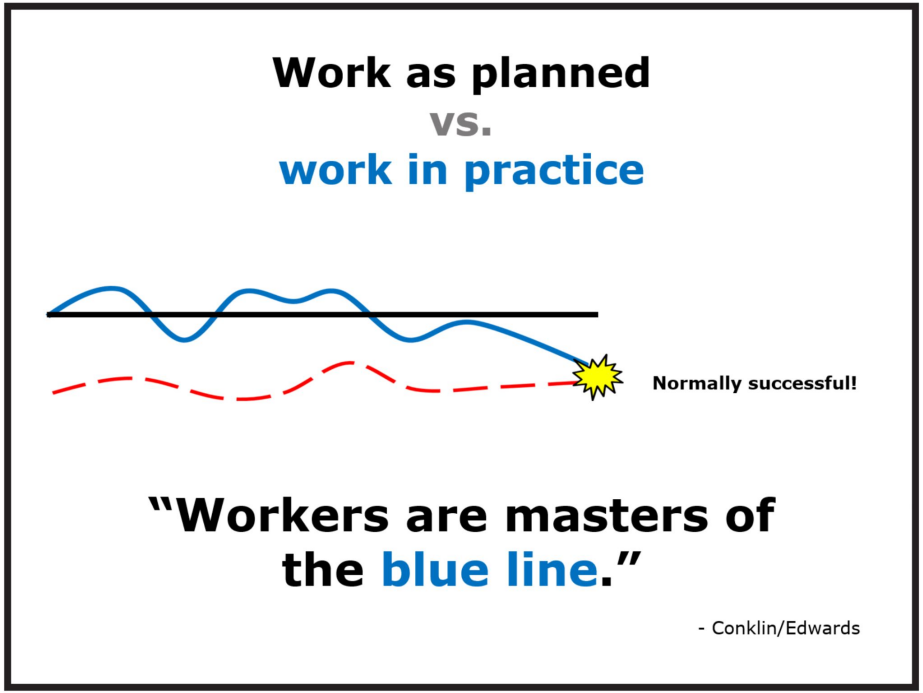
Helping connect multiple timespans…



Observability of actions (feedback loops)

@madplatt





https://www.saif.com/documents/SafetyandHealth/Leadership/S1104_Human_and_Organizational_Performance_%28HOP%29-Another_way_to_think_about_safety.pdf

On managing (operational) risk

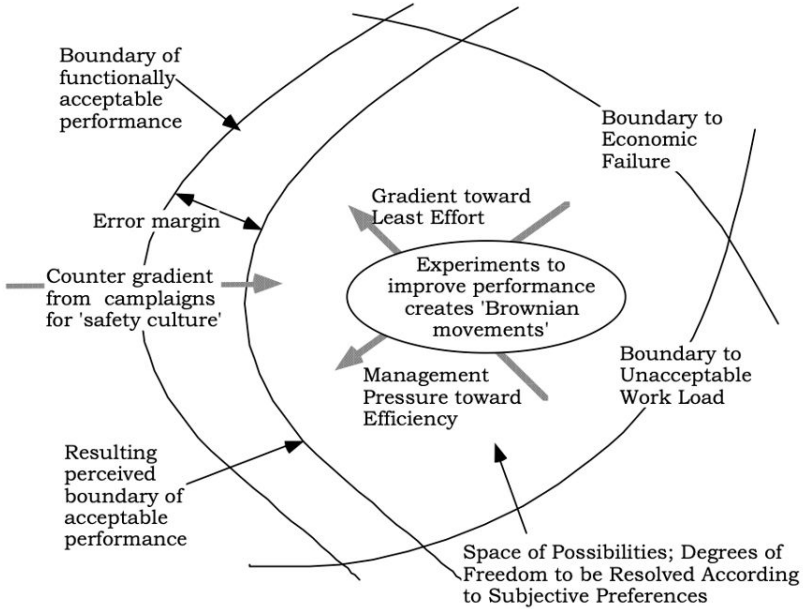
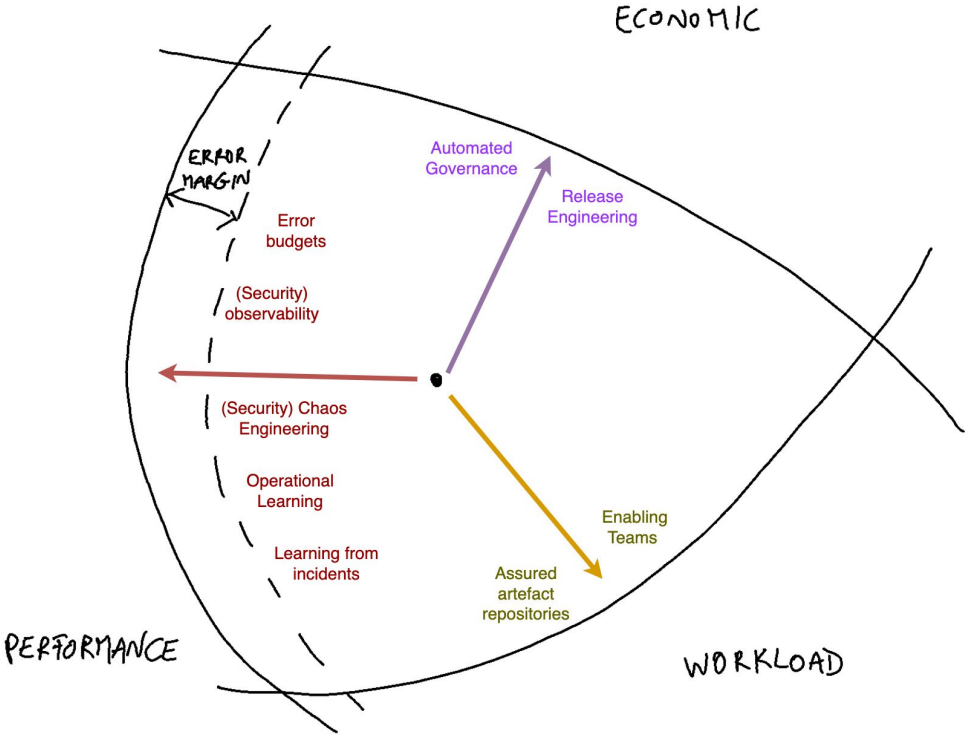


Figure 3. Under the presence of strong gradients behaviour will very likely migrate toward the boundary of acceptable performance.

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. Safety Science, 27(2-3), 183-213. https://doi.org/10.1016/S0925-7535(97)00052-0

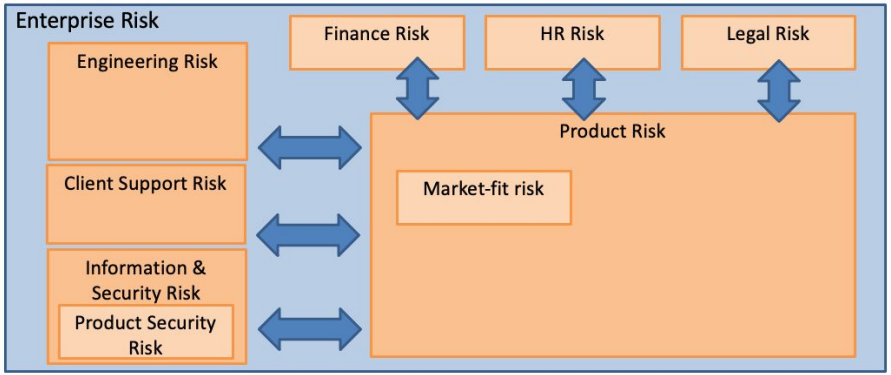
On managing (operational) risk



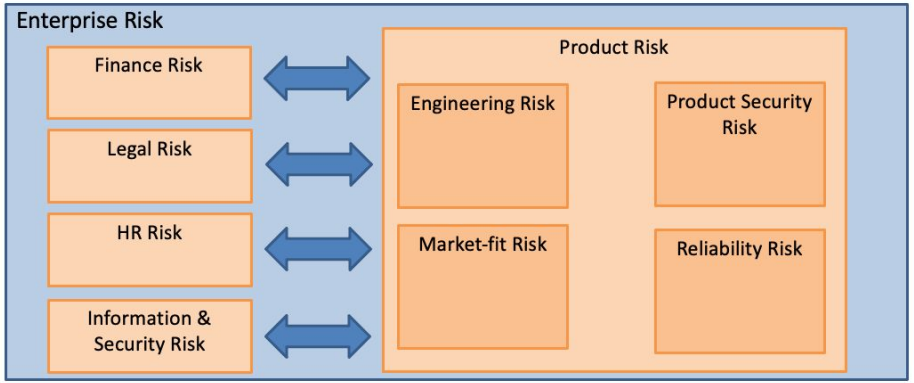
Adapted from Jens Rasmussen

On modelling product risk

Hierarchically-aligned model



Product-oriented model



Managing risk requires multiple strategies

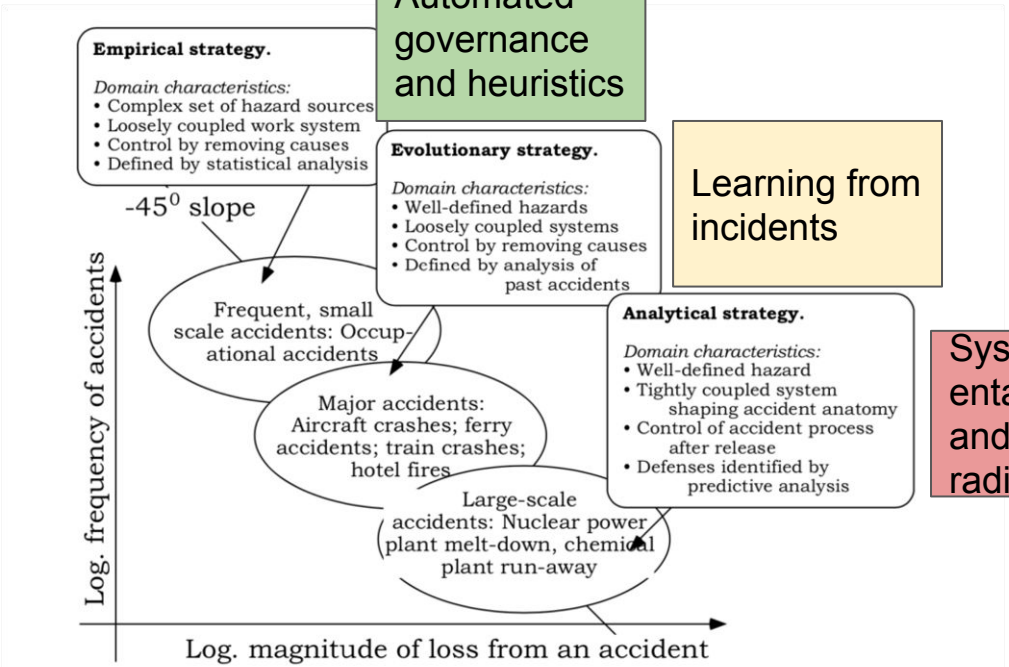


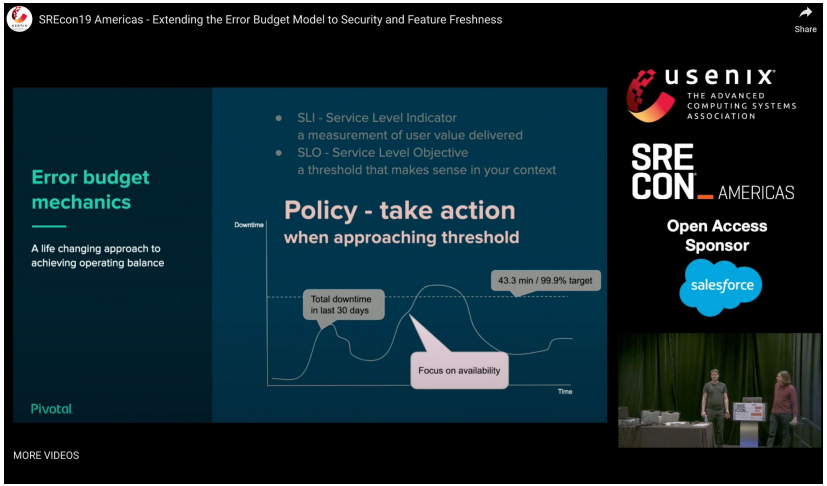
Figure 7. Hazard source characteristics and risk management strategies.

Automated governance and heuristics

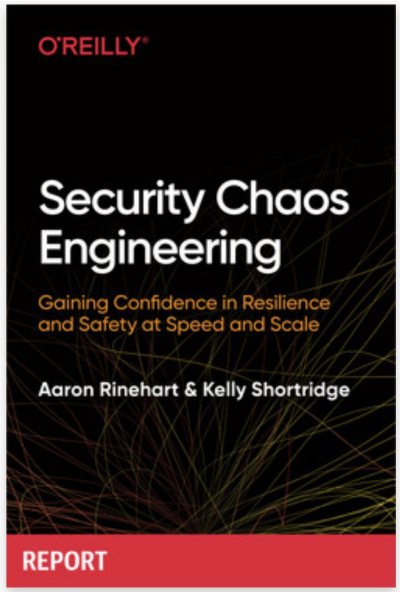
Learning from incidents

System entanglement and blast radius

(Vulnerability) Error budgets



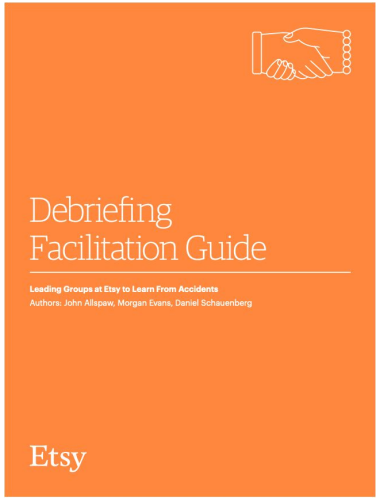
Security Chaos Engineering

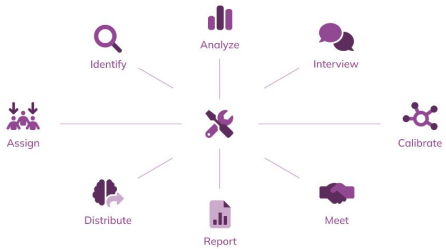


https://www.usenix.org/conference/srecon19americas/presentation/thomson

On Learning

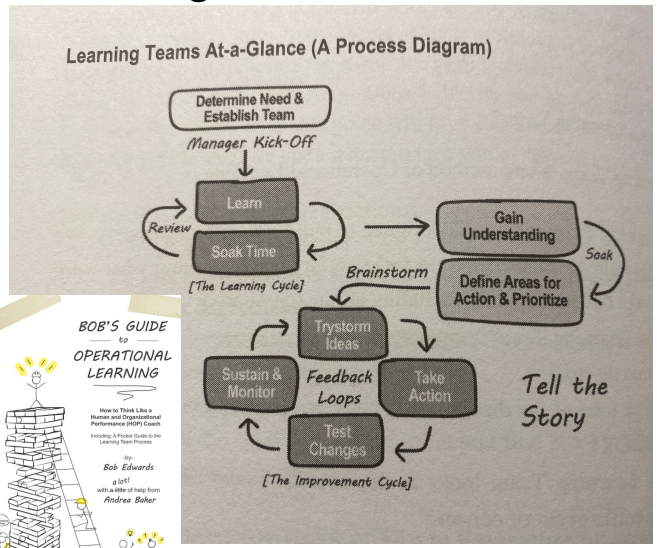
Learning from (security) incidents





Howie, https://www.jeli.io/howie/welcome
Etsy guide, https://extfiles.etsy.com/DebriefingFacilitationGuide.pdf

Learning from normal work

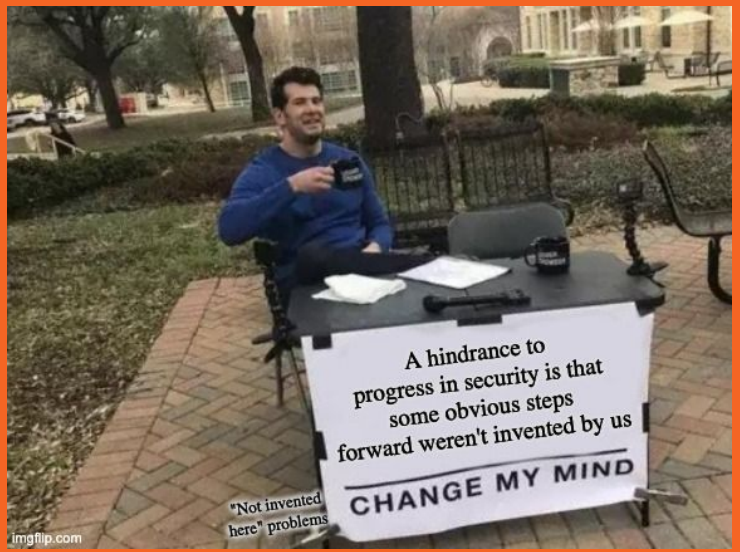


https://www.learningteamscommunity.com/

"Learning organisations become graduate studies in the skills they require to be successful" @littleidea

Key Take-aways

- Traditional GRC functions are stuck. We're largely **bringing spreadsheets to a declarative fight**
- Work as imagined by "gatekeepers" and work as done by practitioners isn't the same.
- SRE metrics embed good governance of competing goals. *Why not Security ?*
- SRE Readiness practices can be leveraged to ensure a pragmatic level of capability in the teams to manage their own product components. *Why not Security ?*
- SRE community is years ahead in (actual) learning from incidents. *Why not Security ?*
- SRE's conception (and therefore management) of risk is more aligned to the dynamic reality of operations and how surprises happen. *Why not Security ?*



Thanks.

Questions ?
Comments ?

Mario Platt

www.securitydifferently.com

mario@securitydifferently.com

Twitter **@madplatt**