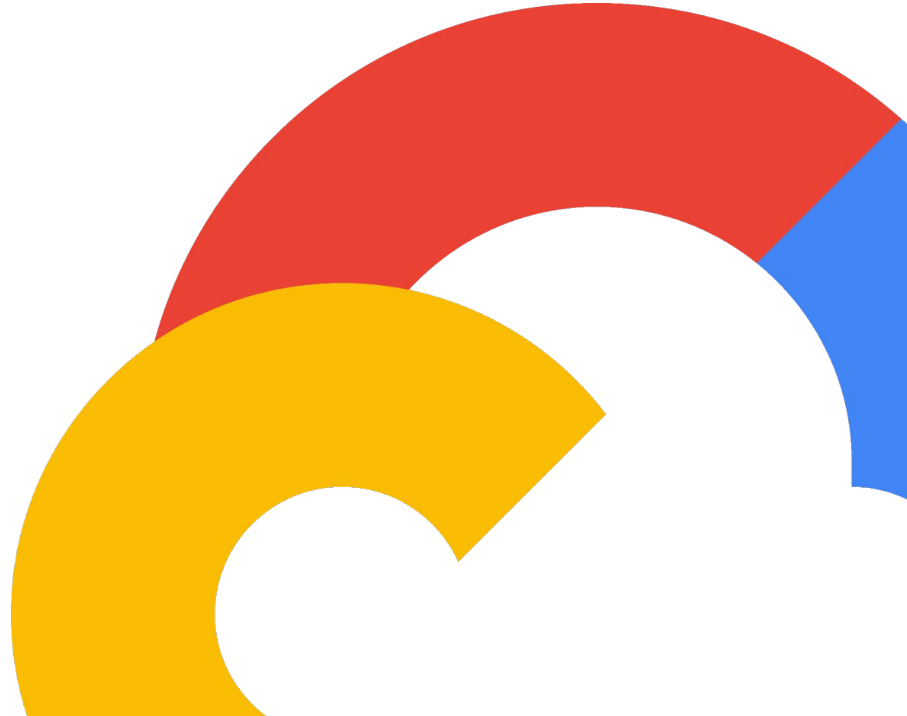


Security *enables* velocity



Michele Chubirka
Security Advocate
Google Cloud
<https://linktr.ee/chubirka>



When did security
and compliance turn
into this?

HIGH COTTON gifts

This perfectly fine, if not certainly adequate
doormat

is **MADE IN THE USA** from 100% Olefin® Indoor/Outdoor carpet and printed with color-fast inks. Wash with hose and brush. Dry flat. Do not machine wash. To best preserve your mat, use in sheltered areas and avoid prolonged exposure to sunlight and water.

**Important things you should know
about your new doormat**

Warning: Do not use mat as a projectile. Sudden acceleration to dangerous speeds may cause injury. When using mat, follow directions: Put your right foot in, put your right foot out, put your right foot in and shake it all about. This mat is not designed to sustain gross weight exceeding 12,000 lbs. If mat begins to smoke, immediately seek shelter and cover head. Caution: If coffee spills on mat, assume that it is very hot. This mat is not intended to be used as a place mat. Small food particles trapped in fibers may attract rodents and other vermin. Do not glue mat to porous surfaces, such as pregnant women, pets and heavy machinery. When not in use, mat should be kept out of reach of children diagnosed with CFED (Compulsive Fiber Eating Disorder). Do not taunt mat.

HIGH COTTON, INC.
9 SW Pack Square, Ste 300
Asheville, NC 28801
www.highcotton.com

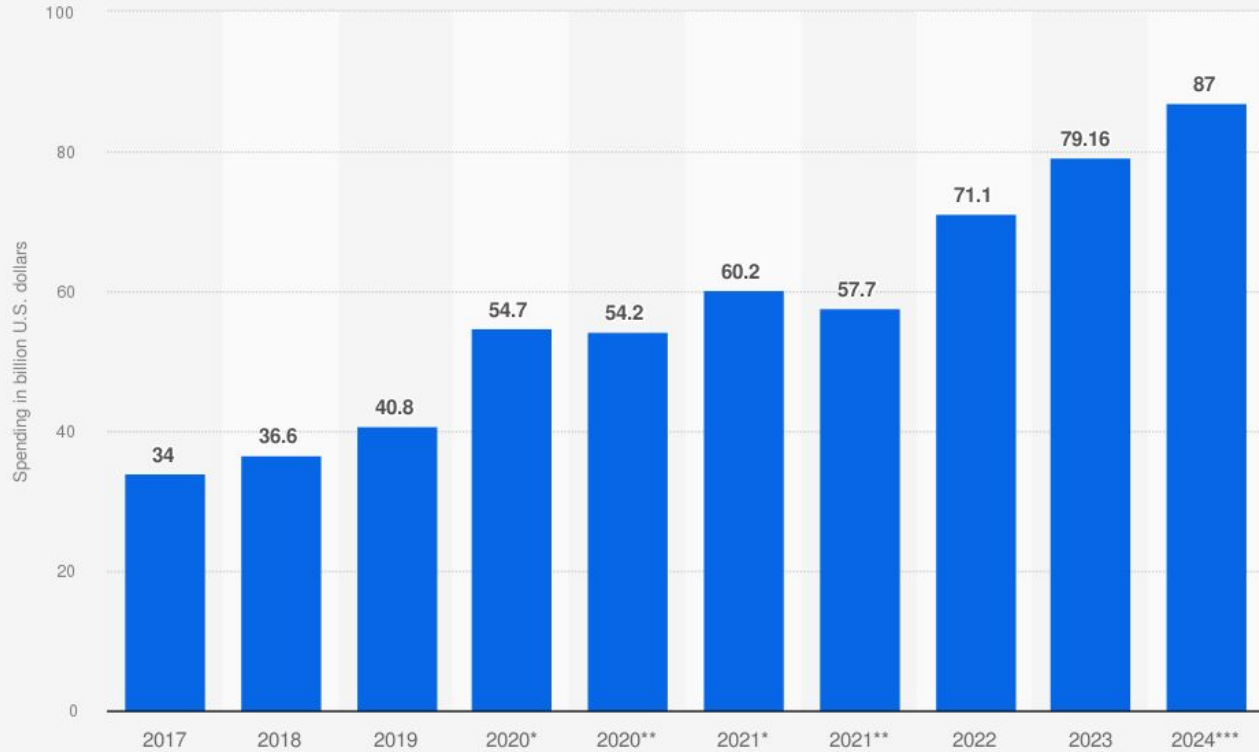


Made in the U.S.A.



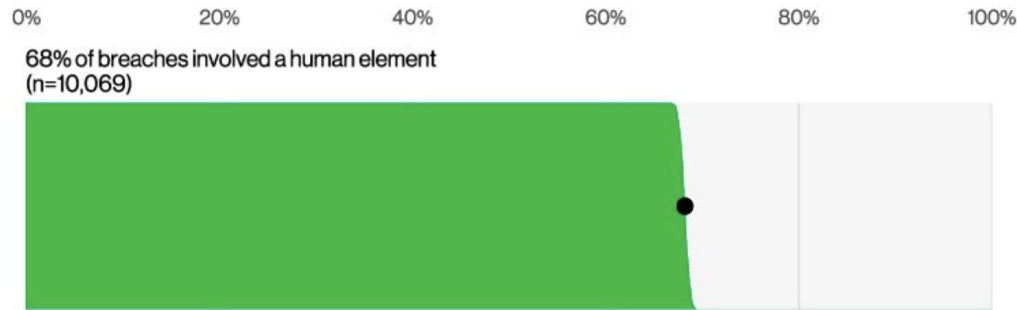
Current state

Spending on cybersecurity worldwide from 2017 to 2024 (in billion U.S. dollars)



Source
Canalys
© Statista 2024

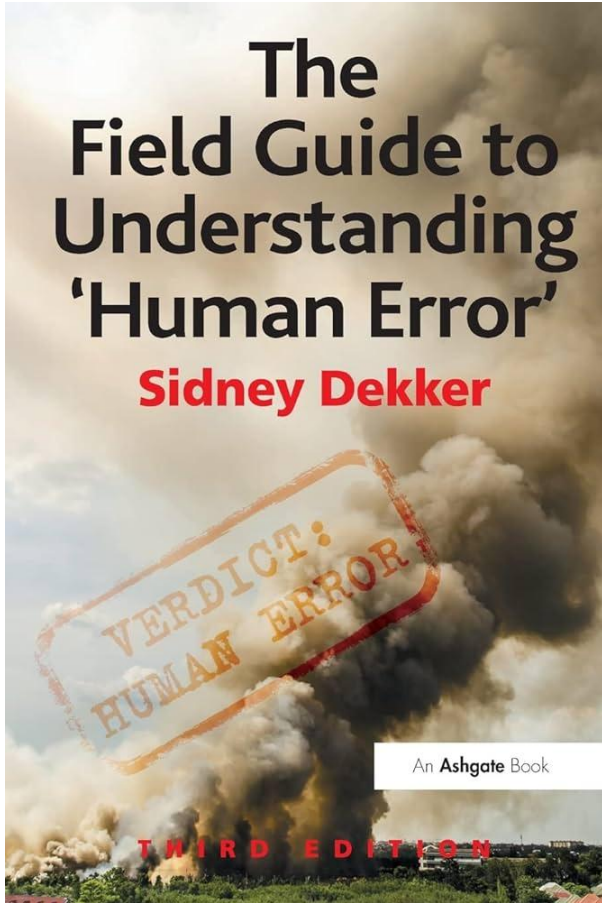
Additional Information:
Worldwide; 2017 to 2024



According to the Verizon 2024 Data Breach Investigations Report, “the human element was a component of 68% of breaches, roughly the same as the previous period described in the 2023 DBIR.”



Causes



'human error' is not a cause of trouble. It is the consequence, the effect, the symptom of trouble deeper inside your organization.... You and your organization may well have helped create those conditions. Leave those conditions in place, and the same bad outcome may happen again.

Dekker, S. (2017). *The field guide to understanding 'human error.'* CRC Press.

Behavioral issues

An aerial photograph of a busy city street, showing a large number of pedestrians walking across a crosswalk. The street is paved with light-colored asphalt, and the crosswalk is marked with white diagonal lines. The pedestrians are scattered across the crosswalk, some walking alone, some in small groups, and some in larger groups. Their shadows are cast long and dark on the pavement, indicating that the sun is low in the sky. The overall scene is one of a busy, active urban environment.

- Bystander effect – People in groups feel less responsible.
- Bounded Rationality - Humans tend to satisfice vs maximize for cognitive economy.
- Cognitive load theory – Limits to working memory and decision fatigue caused by fear or too many choices.
- Protection motivation theory (aka fear appeals) doesn't work well in an organizational context.
- Criminal justice theories - Moral disengagement and neutralization theory.

Culture matters for security

- Renaud, et al. identify that **stigmatizing shame is a counterproductive tactic** with the workforce after a security incident.
- Ogbanufe, et al. find that formal controls and policies **do not correlate to** voluntary security behaviors. Sanctions and fear appeals **correlate to reduced voluntary security behaviors, apathy, and resistance.**
- These and other researchers identify that employees who feel **supported by an organization are more likely to act responsibly** in protecting information resources. They act as stewards.

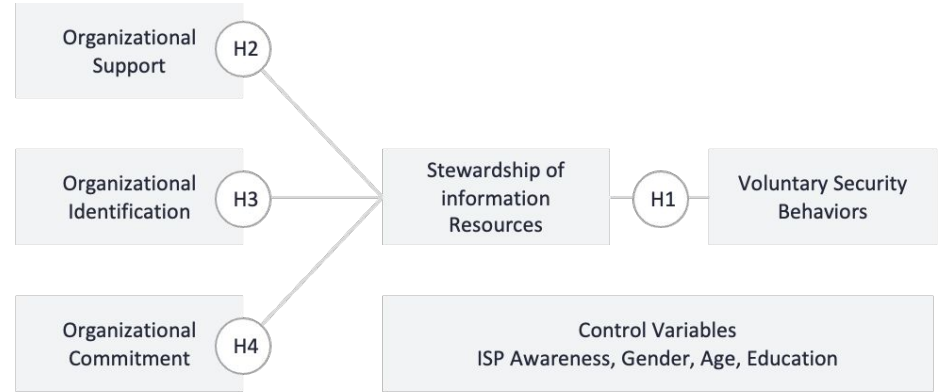
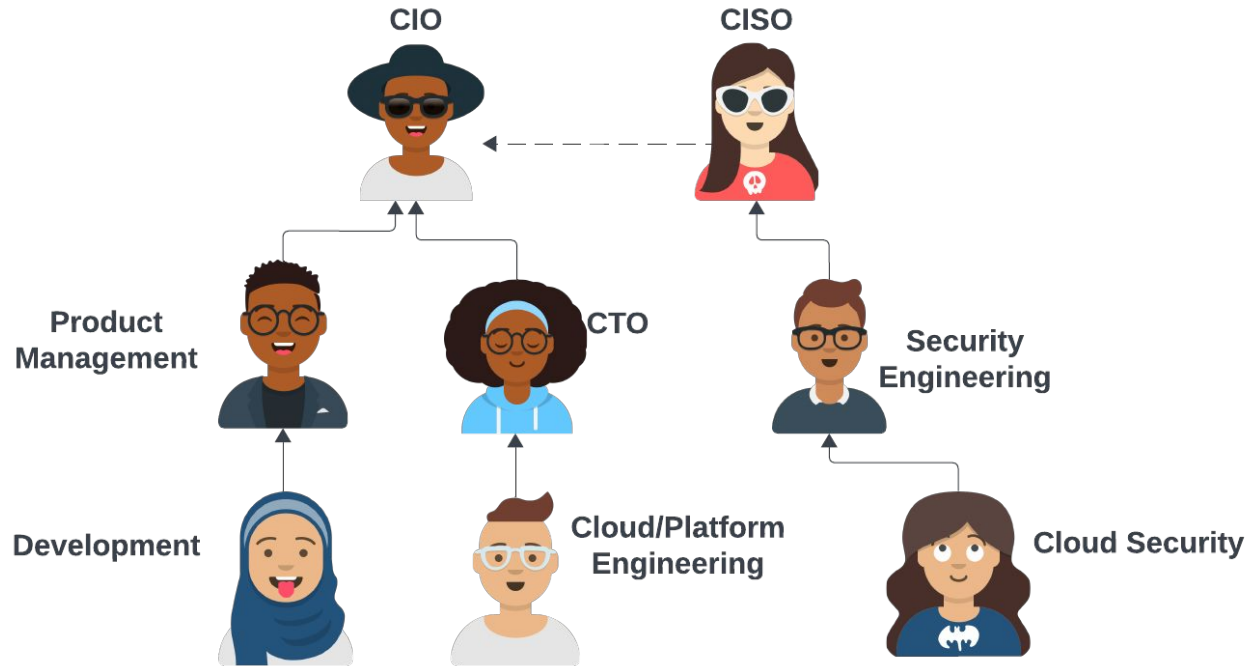


Fig. 1 – Research model.

Conway's Security Law: Program effectiveness will mirror your org chart





A different approach

If something is breached...

When something is breached...



Security failures lead to
scapegoating



Not *my* fault!



Security failures lead to
scapegoating



Not *my* fault!



Security failures
demand justice



Someone must be punished!



Security failures lead to scapegoating



Not *my* fault!



Security failures demand justice



Someone must be punished!



Security failures lead to inquiry



We must diagnose the system!

THIS↑

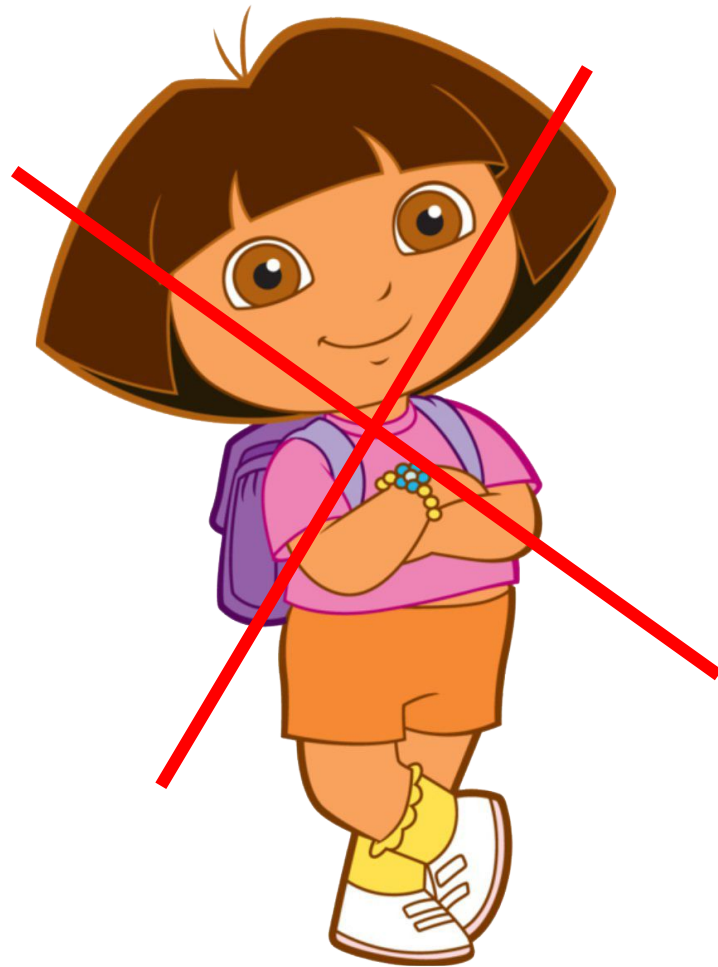


Enter DORA

Enter DORA

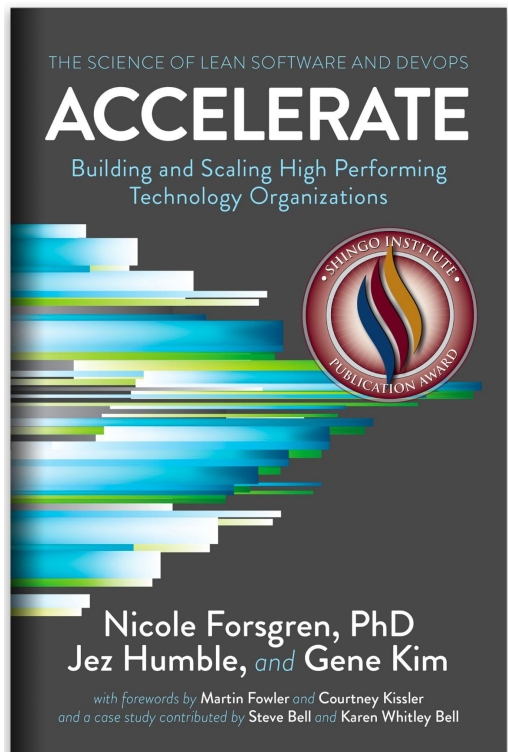


Enter DORA









*“Having security teams work alongside developers, **collaborating** on policy-as-code, **increases trust** between the teams and **confidence** in the changes being deployed.”*

Presented by
DDORA
GOVERNANCE, RISK & COMPLIANCE

Google Cloud

Accelerate
**State of
DevOps
Report
2023**

Premiere Sponsors

LINEAR B digital.ai OPSERA BROADCOM SOFTWARE SLEUTH Deloitte Qarix

dora.dev/report


*“...teams with **low levels** of security practices have **1.4x greater odds of having high levels of burnout** than teams with high levels of security.”*

2022 ACCELERATE

State of DevOps Report



dora.dev/dora-report-2022

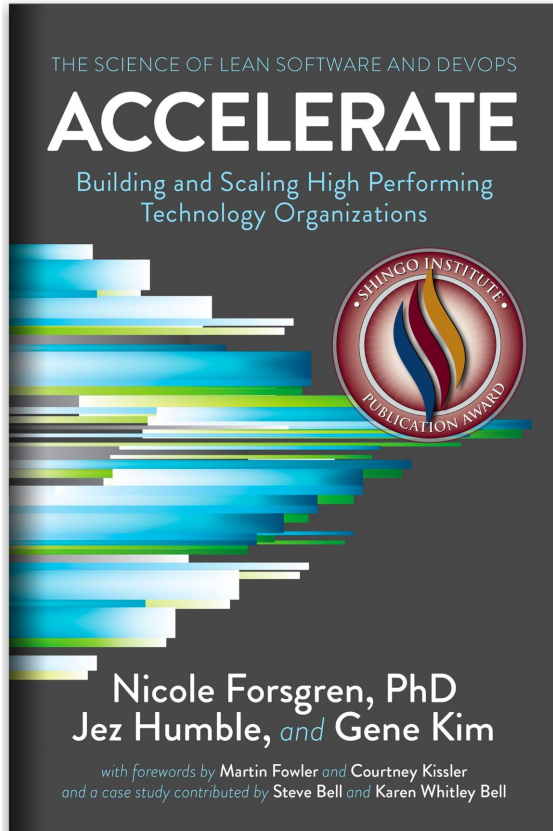


The highest performers who met or exceeded their reliability targets were **twice as likely** to have security integrated into their software development process.

Teams who integrate security practices throughout their development process are

1.6x

more likely to meet or exceed organizational goals.



Accelerate Delivery to improve security

“...**building** security into software development not only **improves delivery performance** but also **improves security quality**. Organizations with high delivery performance **spend significantly less time remediating security issues.**”

Forsgren, N., Humble, J., & Kim, G. (2018). *Accelerate: The science behind devops: Building and scaling high performing technology organizations*. IT Revolution.



Culture is defined as the organization's pattern of response to the problems and opportunities it encounters.

Westrum, R., A typology of organisational cultures. *BMJ Quality & Safety* 2004;13:ii22-ii27.

<http://bmj.co/1BRGh5q>

Westrum's organizational cultures

Power-oriented Pathological



Low cooperation

Messengers shot

Responsibilities shirked

Bridging discouraged

Failure leads to scapegoating

Novelty crushed

Leader's focus: personal needs

Rule-oriented Bureaucratic



Modest cooperation

Messengers neglected

Narrow responsibilities

Bridging tolerated

Failure leads to justice

Novelty leads to problems

Leader's focus: departmental turf

Performance-oriented Generative



High cooperation

Messengers trained

Risks are shared

Bridging encouraged

Failure leads to inquiry

Novelty implemented

Leader's focus: the mission

Culture drives performance

Teams with generative cultures have

30%

higher organizational performance than teams without.

dora.dev/dora-report



SLSA

<https://slsa.dev>

Supply-chain Levels for Software Artifacts

“...organizations closest to the ‘generative’ Westrum culture group were significantly more likely to say they had broadly established security practices, as defined by the SLSA framework.”

DORA Accelerate State of DevOps
2022 dora.dev/dora-report-2022

Security as an enabling feature

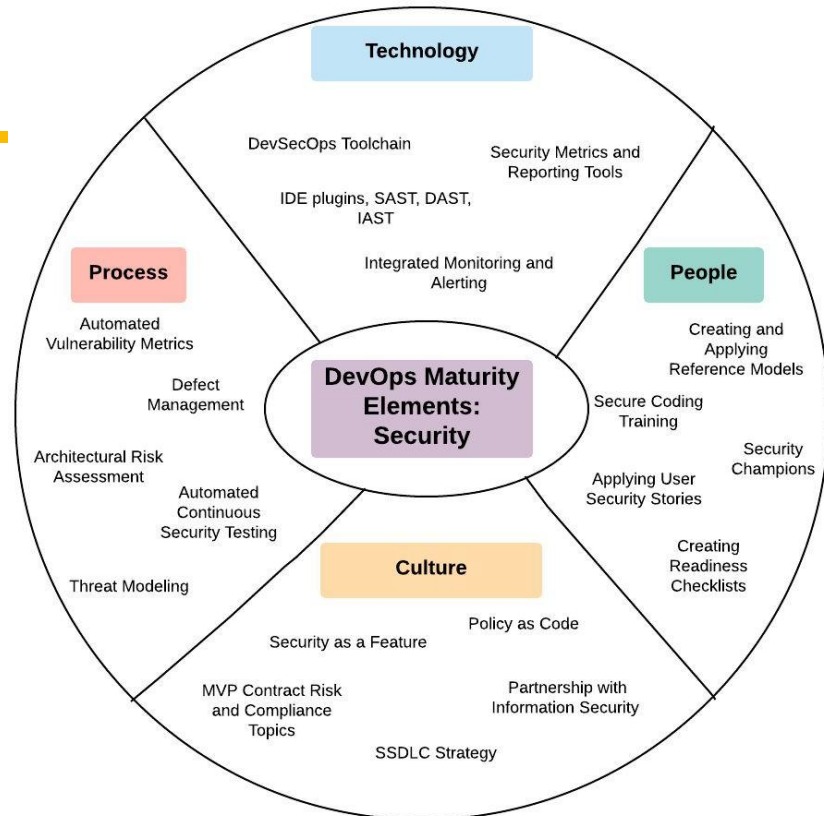


“...consider the brakes on a car...**having better brakes enables the car to be driven at much higher speeds, because the driver now has the confidence that ... braking will be fast and efficient.** It is a completely different way of viewing the same function – one way is about reducing overall speed, the other about increasing it.”

Sherwood, J., Clark, A., & Lynas, D. (2005). *Enterprise security architecture : a business-driven approach*. Cmp Books.

How can security collaborate with engineering?

- Include security criteria in tracking and evaluating DevOps and engineering maturity.
- Create partnerships and align security team metrics with engineering teams.



Takeaways

- Focus on security as an *enabler* of the business.
- Organizational culture will impact the effectiveness of your security program.
- Engineering platforms are run by **people**: collaboration is essential.
- A pervasive security approach requires alignment with the SDLC, which supports delivery velocity and organizational performance.

DORA

2024


Google Cloud

Accelerate State of DevOps

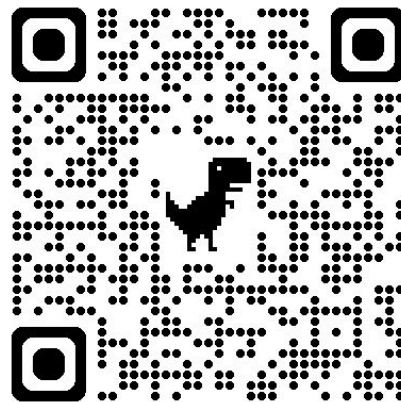
Gold Sponsors

 catchpoint  chronosphere  DATADOG

 Deloitte.  Exella  Gearset

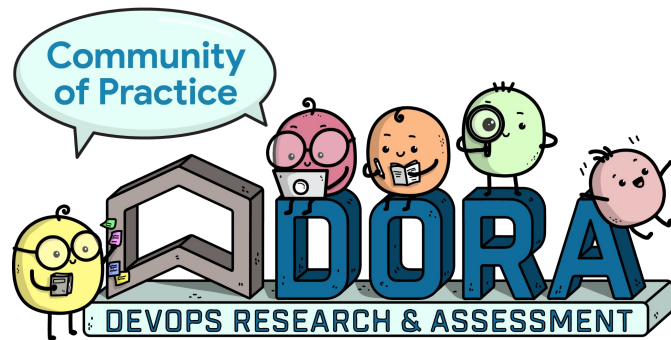
 liatrion  Middleware  OPSERA

10
A decade with DORA



Download the current report at
dora.dev/report

You cannot improve alone!



Join [DORA.community](https://dora.community)

Thank you

Google Cloud

