

Applied Emotions

Where Human Values Meet the Age of Intelligent Machines

SECURITY DESIGN

USER ALIGNMENT

RISK

GOVERNANCE

CRITICAL THINKING

The Human in the loop is miscast, not weak.

The security system is the weak link and value-based role design is how you change it.

The bottom line: Let's stop treating people as the problem to be fixed. The failure is in the system that surrounds them: the process, roles, incentives and conditions of oversight. The single most powerful lever is putting the right people with the right values in the right seats.

What do we mean by 'values'?

Human values are a structured, measurable system that transcends culture, geography and generation. While surface behaviours vary widely, the underlying value structures that drive them follow consistent, mappable patterns across worldwide populations.

The diagnosis: The system is set up to fail.

Humans are involved in ~60% of breaches (Verizon DBIR 2025): concede that.

However, 'involved in' is not 'to blame for'. Safety science settled this decades ago in aviation, healthcare and nuclear: errors **recur in predictable patterns set by the conditions, not the person**. If the same seat produces the same failure regardless of who sits in it, the individual is not the weak link, the system is. And the standard fix is more training that barely moves behaviour: a 69-study meta-analysis¹ found users are strong on knowledge but weak on lasting behaviour and DBIR data shows phishing click rates essentially unmoved by it.

The lever: Right people, right roles, right seats.

If the system is the problem, redesigning the system is the remedy and the sharpest lever within a CISO's control is *who* sits in each oversight role, matched by what fundamentally motivates them. Value based matching maps three orientations to the functions that fit them:

- **Security orientated:** (safety, process, certainty): Reliable in bounded, rules-based sign-off; stability focus, a potential liability where independent challenge is required.
- **Growth orientated:** (status, speed, metrics): Strong on adoption and monitoring with guardrails; will let impact and throughput beat scrutiny in a quality gate.
- **Change orientated:** (ethics, autonomy, systems-thinking): The profile that will challenge a confident-but-wrong output and escalate under pressure. The right fit for AI Governor, ethics and exception-escalation roles which most systems inadvertently select against.

Put people with misaligned Values in a seat and you get failure **by design**, not by incompetence. Put the right people with the right Values in it and oversight becomes a genuine control instead of a rubber stamp that launders liability onto the security function.

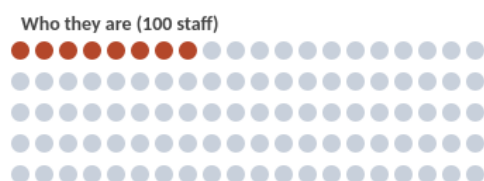
¹Prümmer, J., van Steen, T. & van den Berg, B. (2024). "Assessing the effect of cybersecurity training on end-users: A meta-analysis." *Computers & Security*, Vol. 150, art.

Where to point the effort: Risk is concentrated.

Changing the system does not mean boiling the ocean. Risk is not evenly spread so effort should not be either.

Risk Is Concentrated, Not Uniform

Verizon DBIR 2025: just 8% of employees account for 80% of security incidents



- 8 high-risk users
- 92 lower-risk users

Where the incidents land



Implication:

Blanket training spreads effort evenly across a problem that isn't evenly distributed. Values-and-role matching concentrates it where risk actually is.

Note that just 8% of employees account for 80% of security incidents (Verizon DBIR 2025). Matching users values to the roles where risk concentrates changes the system where it counts at a fraction of the cost of blanket training.

What changing the system delivers:

1. **Sharper detection** on the rare, high-cost anomaly others might wave through.
2. **Real resilience** and shorter dwell time from teams wired to escalate.
3. **Lower cost** and a defensible budget story.
4. **Reduced liability** that holds up where 'we trained everyone' does not.



Who should act now?

- CISO's with AI in their security strategy and humans in their security decision-support stack.
- Cyber & security risk, governance operational model design specialists.
- Leadership teams navigating AI-driven human restructuring programs.
- Risk and compliance functions managing AI governance.
- CHRO's and People Leaders in collaboration with CISO/Security Leadership.

If you don't have the right users with the right Values in the right roles, you're creating a greater security risk profile with a potential for unseen and unmanaged breaches which could cost you irrevocable trust, reputational, and commercial damage.

Right people, right roles, right seats.

Your security alignment journey starts here.

VALUES DRIVEN ALIGNMENT INDEX

Overall Alignment

Excellent Alignment

People	Brand	AI Agents
97%	99%	98%



Request a Diagnostic

Visit our Website