The First Rule of GRC is We Don't Talk About GRC

October 11, 2025

anecdotes

Consultant...	CISO...	Advisor/vCISO...
IBM	SingleStore	crocs™
KPMG	whistic	Maui Jim
nccgroup	anecdotes	plotly

anecdotes

Any questions?

anecdotes

What is GRC?

Why is GRC hard?

anecdotes.

How do we change culture through GRC?

anecdotes

Life in GRC used to be boring – spread sheets, policy writing, evidence collection…
I want to give you a different truth how in the age of AI & Data GRC is now an engineering discipline

- Like Fight Club, GRC is misunderstood.
- It's seen as boring, bureaucratic, and lesser than "real security."
- But just like Tyler Durden's underground revolution, GRC is the force actually driving transformation.

This is the problem…you look like these guys!

- Not hackers in hoodies

- Just red tape & a lot of paperwork

Reality Check: The best security leaders embed GRC principles **without calling it GRC**—because forcing compliance never works – they build a revolution

This is how you want people to think of you (minus the criminality).

Quote: "The first rule of Fight Club is you DO NOT talk about Fight Club."

The Whispering Revolution without ever "talking about it":

- The best GRC leaders don't "sell" GRC—they embed it into security culture.
- **They operate through influence, not enforcement.**
- The power is in making security second nature, not a compliance burden.

Analogy: *Tyler Durden didn't ask for permission to disrupt the system; he changed the rules of the game.*

Similarly when you make it an engineering discipline, a revolution, something cool then you write the rules & people follow.
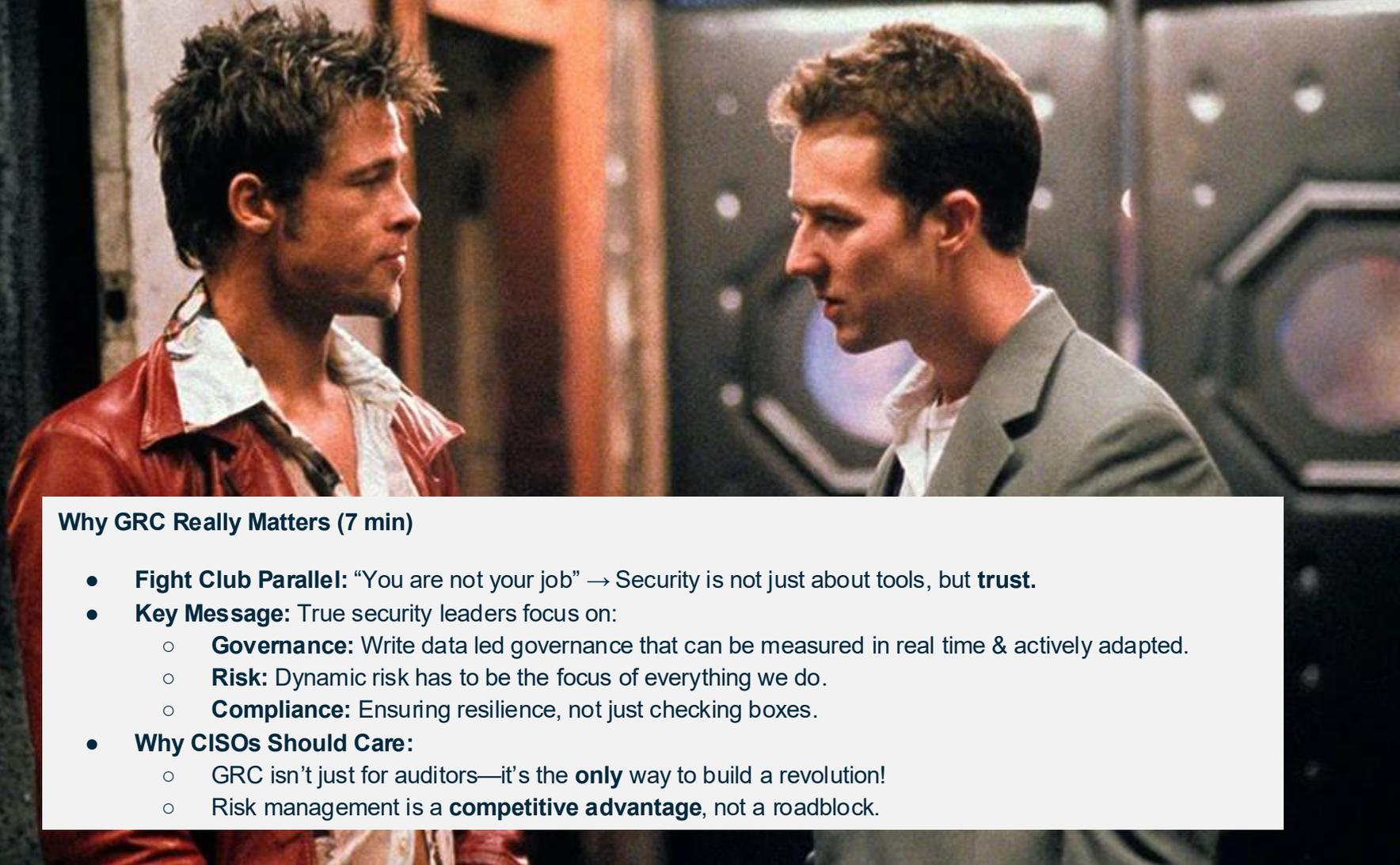
Why GRC Really Matters (7 min)

- **Fight Club Parallel:** "You are not your job" → Security is not just about tools, but **trust.**
- **Key Message:** True security leaders focus on:
    - **Governance:** Write data led governance that can be measured in real time & actively adapted.
    - **Risk:** Dynamic risk has to be the focus of everything we do.
    - **Compliance:** Ensuring resilience, not just checking boxes.
- **Why CISOs Should Care:**
    - GRC isn't just for auditors—it's the **only** way to build a revolution!
    - Risk management is a **competitive advantage**, not a roadblock.

Tyler Durdon Playbook on GRC Transformation

"You are not special"
→ Drop the security ego.
- Security teams often overestimate their own visibility.
- People don't care about security—they care about **getting their job done.**

"Self-improvement is pointless. Self-destruction is the answer."
→ Burn down bad security models.
- Overly strategic, compliance-first approaches don't work.
- Security must embrace **real-world risk**, not theoretical frameworks.

"It's only after we've lost everything that we're free to do anything."
→ Use failure as a catalyst.
- Breaches force change more effectively than policies.
- GRC teams should use **near-misses** as teachable moments.

"We are the all-singing, all-dancing crap of the world."
**→ Mobilize the real people.**
- Security teams alone can't drive change.
- GRC should focus on empowering **frontline employees** as the first line of defense.

- **Key Actions for CISOs:**
  - Make risk management **visible**— make people squirm & hurt so you make better decisions!
  - Get frontline workers invested in **real security**, not just compliance – competitions, hack yourselves!
  - Speak in business terms, not security jargon – avoiding a breach in not ROI
  - Build **cross-functional alliances** (legal, finance, HR) to push change from within.
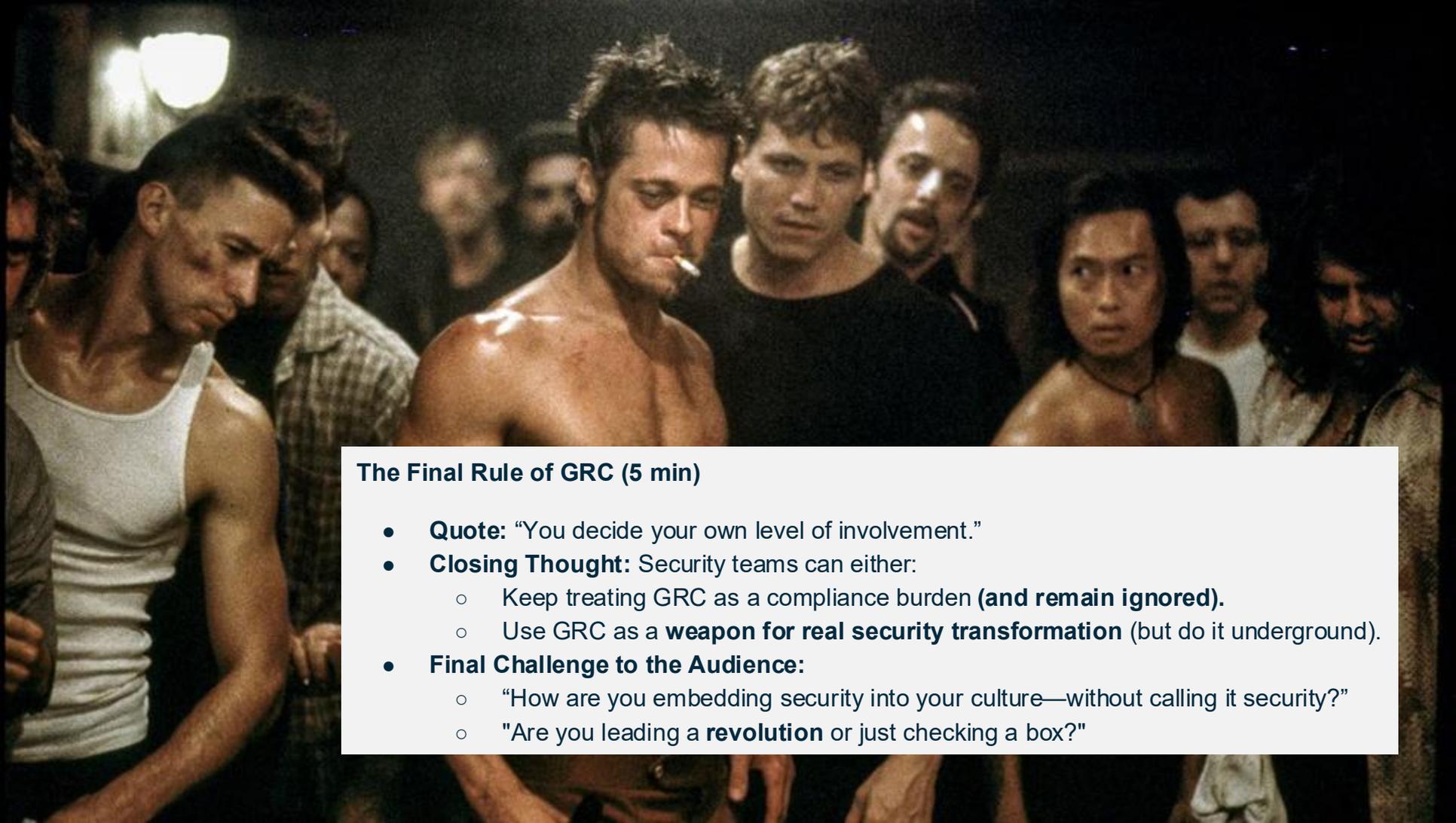
The Final Rule of GRC (5 min)

- **Quote:** "You decide your own level of involvement."
- **Closing Thought:** Security teams can either:
  - Keep treating GRC as a compliance burden **(and remain ignored).**
  - Use GRC as a **weapon for real security transformation** (but do it underground).
- **Final Challenge to the Audience:**
  - "How are you embedding security into your culture—without calling it security?"
  - "Are you leading a **revolution** or just checking a box?"

Thank You.

Jake Bernardes

jake.Bernardes@anecdotes.ai

www.linkedin.com/in/jakeleobernardes

anecdotes