

How to Work With a CISO Who Always Says **NO**

Practical strategies for navigating cybersecurity gatekeeping

For CEOs, COOs, CFOs, CIOs, & CLOs

Does your business or organization have these symptoms?

- There is constant **friction** with security.
- Every meeting with security is a **debate**.
- **Security says no** before they hear the full proposal.



It always feels like **security is working against us**.

Why doesn't security get it?
If we don't build & deploy anything, **they won't have anything to protect!**

If this feels familiar, you're not alone.

In fact, this behavior is often rewarded in early-stage cybersecurity leadership. But in today's environment, it's a liability for the business.

What You Need to Know | For some cybersecurity professionals, control is their identity

- **Some CISOs navigate their careers by saying no** *to protect the business*. That instinct once earned them respect - or fear.
- But now, AI, cloud, & business-led technology are shifting the model. **Without a new way to lead, their identity may be threatened.**

“If I’m not the gate, then **what am I?**”



What You Need to Know | Many CISOs have IT Infrastructure or GRC* backgrounds

Cybersecurity professionals are typically trained for

- **Rigor** rather than agility
- **Documenting & responding to risk**, not designing forward

And in cultures where they've been punished for past mistakes, that **caution can calcify into stubbornness.**



Innovation can feel like danger instead of opportunity.

“I was trained to prevent loss, not enable innovation.”

- Fortune 100 CISO, post-transformation interview

What You Need to Know | Some CISOs carry real scars

- Some CISOs have been **bypassed, undermined, or pressured to sign off on bad ideas** – so, they default to suspicion.
- They're not trying to block progress; **they're trying not to get burned *again*.**



I'm the **Chief Scapegoat**
...the last to know & **the first to be blamed.**

It's all about **trust...and trauma.**

You're not stuck with a "No CISO." But you might be reinforcing one.

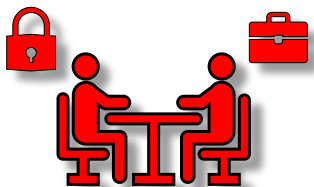
Some CISOs are wired to say *no* because of their professional training and because they've been burned when they said yes.

But **their behavior isn't fixed**. It's shaped by the system around them. And that means **every CXO (CEO, COO, CFO, CIO, CLO) has leverage**.

Here's how each CXO can **unlock a different response...**



Chief Executive Officer (CEO)



Typical tension

Security is **resisting** strategic change.

Why it matters

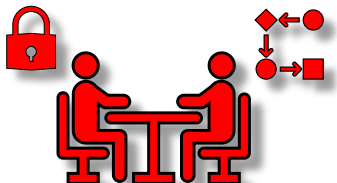
CISOs take their cues from the top.

If the CEO only shows up during a crisis, a CISO may lead from fear; however, **if the CEO signals partnership, the CISO can lead with purpose.**

Recommended CEO lens

- ✓ Reposition security as a **strategic lever** instead of a final checkpoint.
- ✓ Tell your CISO: “I’m not asking you to say yes to everything. **I’m asking you to help us say yes to the right things.**”

Chief Operating Officer (COO)



Typical tension

Security **adds friction** to operational workflows or **causes** implementation **delays**.

Why it matters

COOs depend on **speed, scale, & reliability**.

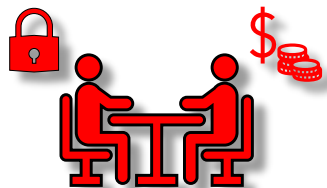
When controls are unclear or inconsistent, **operations stall & workarounds start to spread**.

Security should **stabilize execution**, not disrupt it.

Recommended COO lens

- ✓ Ask your CISO to **tie controls to operational flow** (not just policy & compliance).
- ✓ Push for **resilience that's built in** instead of bolted on.

Chief Financial Officer (CFO)



Typical tension

Security spend feels high, with **unclear ROI or business value**.

Why it matters

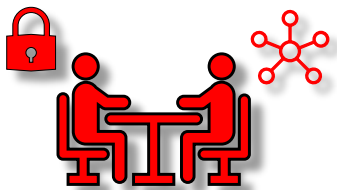
If cybersecurity is framed only as “protection,” it looks like **a sunk cost**.

Cybersecurity tied to risk reduction, fraud prevention, or business continuity, becomes a **strategic investment**.

Recommended CFO lens

- ✓ Ask your CISO to frame budgets in terms of **exposure avoided** instead of tools or personnel.
- ✓ Engage in **cost–risk tradeoff** discussions.

Chief Information Officer (CIO)



Typical tension

Security **slows delivery** or **limits system flexibility**.

Why it matters

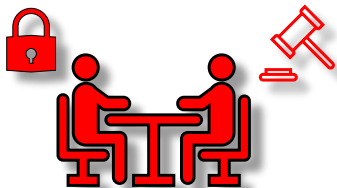
CIOs are accountable for both **uptime & innovation**.

If your CISO defaults to **caution instead of collaboration**, transformation efforts stall & IT becomes the battleground.

Recommended CIO lens

- ✓ Align risk appetite early, **before architecture or vendor decisions**.
- ✓ Co-create governance so security **scales with tech**, not against it.

Chief Legal Officer (CLO)



Typical tension

Legal **isn't looped in early** on **risk exposure** or **incident response** plans.

Why it matters

Security missteps can lead to **legal liability, contract breaches, & regulatory fines**.






When legal & security work in sync, **risk is shared & better managed**.

Recommended CLO lens

- ✓ Ask your CISO to **map controls to legal risk** (not just compliance).
- ✓ Partner on breach preparedness **before the subpoenas** arrive.

Every executive has a role in unlocking a better security partnership

When each role leans in, the CISO becomes a partner, not a gate.

-  **CEO:** Reposition **security as a strategic lever** instead of a final checkpoint. You're not asking for yes. You're asking your CISO for **insights that sharpen the business**.
-  **COO:** Ask your CISO for **frictionless controls**. The goal is **resilience that flows with operations** rather than clogging them.
-  **CFO:** Work with your CISO to **quantify risk in terms of loss prevention & cost avoidance**.
-  **CIO:** Create space for your CISO to shape **risk appetite**. Governance needs to evolve with delivery.
-  **CLO:** Ensure the CISO can **map security practices to legal risk**, not just policy & compliance checklists.

Ready to unlock a strategic partnership with your CISO?

Let's have a candid confidential conversation.

[ResilientTech Advisors](#)

jchatman@resilienttechadvisors.com

