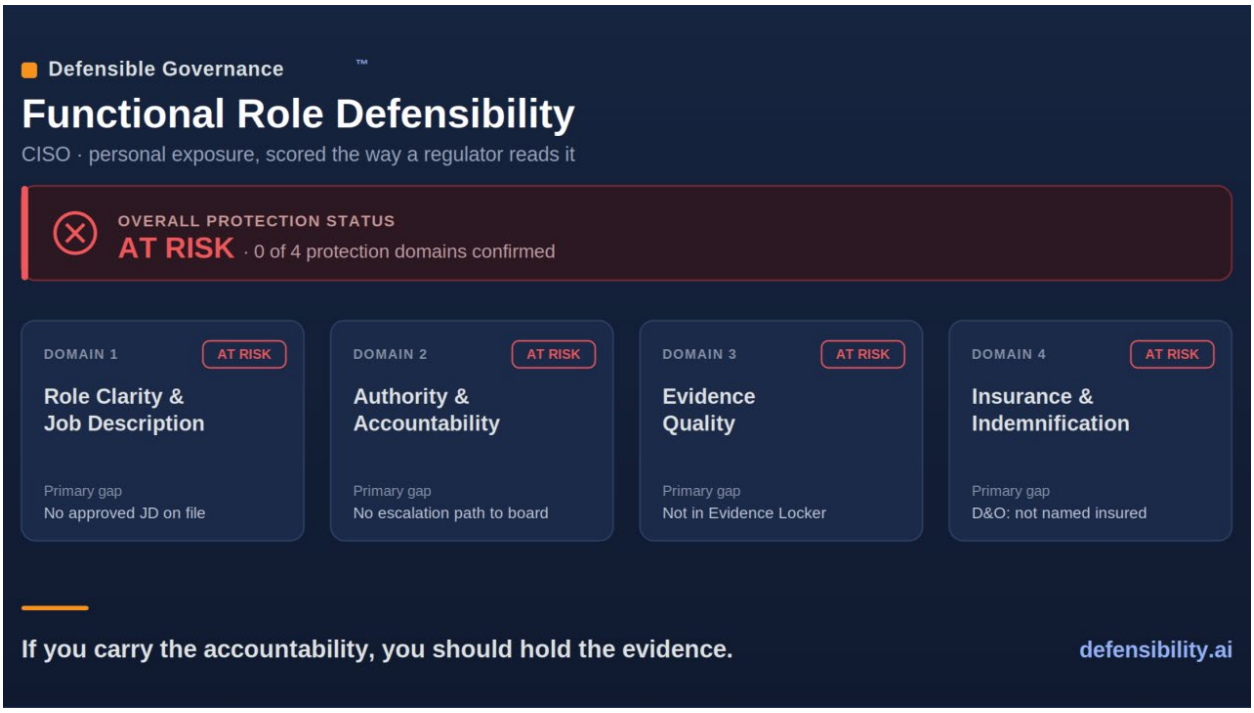


Judged Like an Executive, Equipped Like a Technician

The **CISO is now personally accountable** for cyber outcomes — often **without the authority**, **legal protection**, or **defensible decision record** to **survive** the **scrutiny** that follows. The **gap** is fixable, but only before the incident.

The reckoning is here

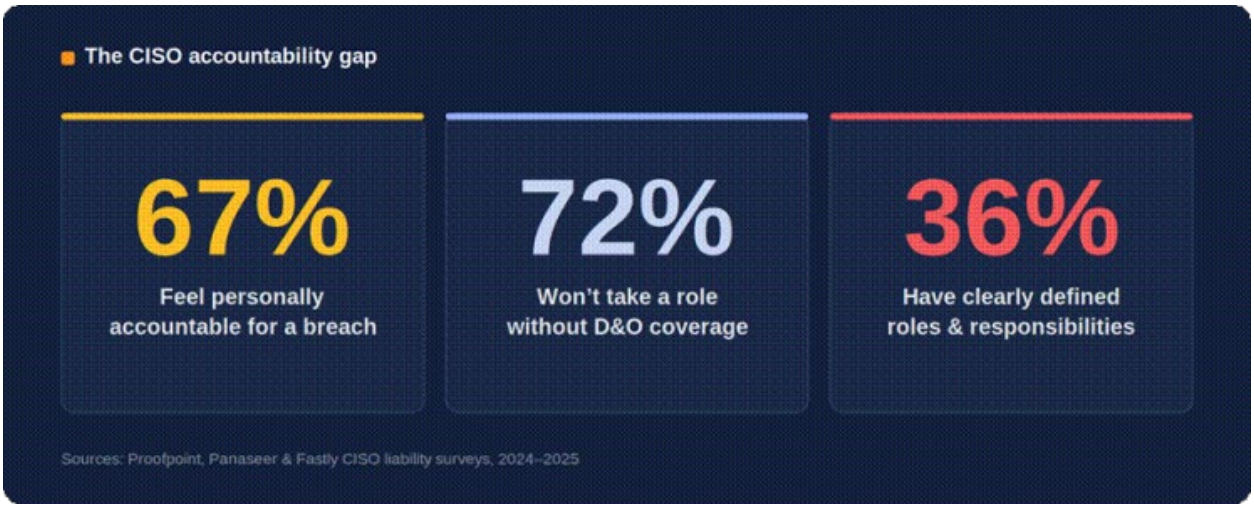
A few numbers capture where the role now sits. In recent surveys, **67%** of **CISOs say** they feel **personally accountable** when **a cyber incident occurs**, and **66% say** the **expectations** placed on them are **excessive** — yet **only 65% say** their **organization** has taken any step **to protect** them from **personal liability**. **Seventy-two percent** say they would **not take a job** at a company that lacks D&O insurance (Proofpoint). **Sixty-five percent** of security leaders **expect to be blamed personally for a major breach**, and **75% say** their **personal liability** is higher than it was two years ago (Panaseer). **Ninety-eight percent are worried** about the pace of regulatory change, and **79% say keeping up** with it is **no longer sustainable (Trellix). Sixty-nine percent** are **open to leaving their role within the year** (IANS / Artico).

Strip away the survey noise and one sentence remains: **CISOs are treated like technical operators *before* a breach**, and **held accountable like executives *after* one.**

Minimize image

Edit image

Delete image



The asymmetry no one designed

Before an **incident**, the **CISO** is asked to **run controls**, **manage tools**, and **report metrics**. **After** an **incident**, a **regulator** or **court treats** them as the **accountable officer** for a **decision** they may **never** have been formally **empowered to make**. The **organizational wiring** makes it **worse**: **46%** of **companies** are **unclear** about **who** ultimately **owns responsibility** for a cyber incident, and **only 36%** have **clearly defined roles** and **responsibilities** (Fastly). When ownership is ambiguous, it does not disappear — it lands on whoever is named when the enforcement action arrives.

That is why 93% of organizations changed policy in the past year to address CISO liability. But most of those changes — more board access, better insurance — manage the symptom. They do not produce the one thing that actually protects an executive under scrutiny: a contemporaneous, defensible record of what was decided, by whom, and why it was reasonable.

The question has changed

For most of the last decade, the governing question was *did you comply?* **Today** it is ***did your leadership exercise reasonable care — reasonable judgment****, in plain terms?* That is not a rhetorical difference. **Compliance is activity** — controls, certifications, audits. **Defensibility is accountability** — proportionate, documented reasoning that holds up when a court applies the negligence standard it actually uses:

- **Was the harm foreseeable**?
- **Did leadership weigh the benefit against the harm to others**?
- **Were alternative safeguards considered** — and would they have imposed an undue burden?
- **Was the decision documented, approved, and retained as evidence of reasonable care**?

These **questions appear** in **GDPR Article 35**, **FTC Section 5**, the **SEC cyber rules**, and **tort law worldwide** — and they are applied retroactively to decisions you are making right now. A certification answers none of them.

Why GRC doesn't save you

The **SolarWinds** case **made the gap concrete**. Regulators reviewed roughly 11,000 internal emails. A handful identified a risk. None explained why leadership accepted it. That **missing rationale — not the breach itself — became the liability narrative**. The evidence was **not absent because the company was careless**; it was **absent because no system existed to produce it**. GRC tools record that an activity happened. They **do not produce contemporaneous proof** that a threshold decision was made, by a named executive, for a reason a court would call reasonable.

That threshold is what we call the CDAR — the Calculated Definition of Acceptable Risk. It rests on a **proportionality principle courts** have **used** for **nearly** a **century**: a safeguard is expected when its burden is less than the probability times the magnitude of the harm it prevents. **Burden < Probability × Harm.** CDAR **forces leadership** to **set** that **threshold in advance** and document the reasoning behind it. When a **risk rises above the line**, it escalates to a Duty-of-Care Cost–Benefit Analysis — **a structured review** of whether deferring, modifying, or implementing a safeguard can still be justified over a three-year horizon. **Together they produce** the **thing regulators invoke** but **rarely define**: a **documented reasonableness posture**.

It only counts if it predates the harm

Here is the **part most governance programs miss**. **Evidence created after** an incident is reconstruction, and reconstruction **carries little legal weight**. The **protection exists** only if the **record was sealed** — timestamped, attributed, immutable — **before anything went wrong**. A decision rationale written the week the subpoena arrives is not a defense. A decision rationale sealed the quarter the feature shipped is.

This is also **why the CISO** the **SEC named personally** in the SolarWinds action, **Tim Brown**, sits on our **advisory board. The platform is modeled on exactly the gap his case exposed.**

Proof that the record changes outcomes

The pattern is visible in the outcomes. Marriott reduced a proposed £99 million fine by roughly 81% — about £80 million — by showing board-level oversight and documented assessments. UPMC faced a negligence claim after a major breach and had it dismissed, on a finding that it had met its duty of care. Contrast that with Uber, where the security chief was criminally convicted for concealment, and Drizly, where the FTC bound the chief executive personally for twenty years. The companies that could show their reasoning kept their money and their people. The ones that could not did not.

Analysis of the largest breach, **privacy**, and **AI settlements** since 2021 — more than $21 billion in total — **found that** essentially all of them turned on a **finding of presumed negligence**, that **almost all** had **active GRC programs** at the time, and that none could answer the questions a judge actually asks. **Compliance** was present. **Defensibility** was **not**.

What this means for you, personally

If you are a **CISO, GC**, or **board member**, the **exposure is no longer the company's alone**. It is yours. The **protection is not perfection** — it is the **ability to show you exercised reasonable judgment** given what you knew at the time. That is the **difference between a nine-figure fine and an executive who walks out with their credibility intact.**

The **fastest way** to **see your exposure** is to **run the assessment on yourself**. It produces a **snapshot** of where **you stand** — and **where** the rest of the **C-suite** and the **company stand** — scored the **way a regulator would read it**. That gives you several things at once: **credibility** with leadership, **because you walk into the room holding their exposure** and not just your own; the **ability to discuss risk in business terms** rather than technical ones, which is the language the board and CFO actually evaluate; and a documented, defensible **answer when the board asks what the organization's top three risks are**. And it **shows** you **exactly where** your **personal gaps sit** — the **missing job description**, the absent **escalation path**, the **D&O policy** that doesn't name you — with a clear path to close them before they matter.

All of that is what we built Defensible Governance to do — and it is the basis of the Personal Defensibility Plan we offer executives, in addition to the corporate Defensibility.

- Personal liability review

- D&O and indemnification gap analysis
- HR-aligned job-description modifications — what you are, and aren't, accountable for, in writing
- Quarterly Defensibility Gap Assessment
- Executive dashboards with accept / reject decision logs
- Board-level risk-exposure reports

Think of it as career insurance you put in place before the regulatory event, not after.

We're **offering 25 CISOs a no-charge Functional Defensibility Assessment** — normally a $12,500 engagement — in **exchange** for working with us as design partners, **providing feedback**. You keep the output regardless: your gap assessment, your C-suite exposure report, and a **signed accountability record documenting what your role does and does not own**. That record is the one Tim Brown didn't have.

If you carry the accountability, you should hold the evidence. Message me, or start at defensibility.ai.

Defensibility.ai *builds the legal-defensibility layer for executive leadership and boards. Its two commercially available applications — Defensible Governance and Minors Safety & Child Welfare — are the subjects of pending U.S. provisional patent applications. We do not guarantee a specific legal outcome and are not a replacement for legal advice from a licensed attorney.*