panaseer

ControlWatch

and the Continuous Controls Battle

2025 Security Leaders Peer Report

Introducing

The Cyber Investigator: Special Operations squad

Aurelia Auditore
Expert in all things audit.

Conrad P. Lance
Compliance is the name of the game.

"Risky" Rick Roberts
Seeking out hidden risk.

Act 1
Enter the CI:SOs

Welcome to our fifth annual **Security Leaders Peer Report, 2025**. We've asked 400 security leaders from larger organizations (1000+ employees) across the US and UK about their opinion on the state of the cybersecurity industry.

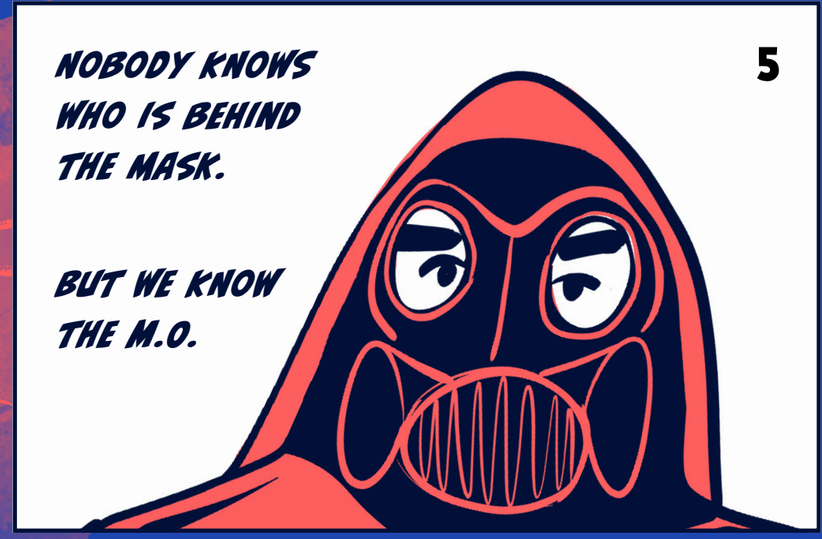
To the surprise of nobody, the landscape is one of increasing pressure from multiple sides.

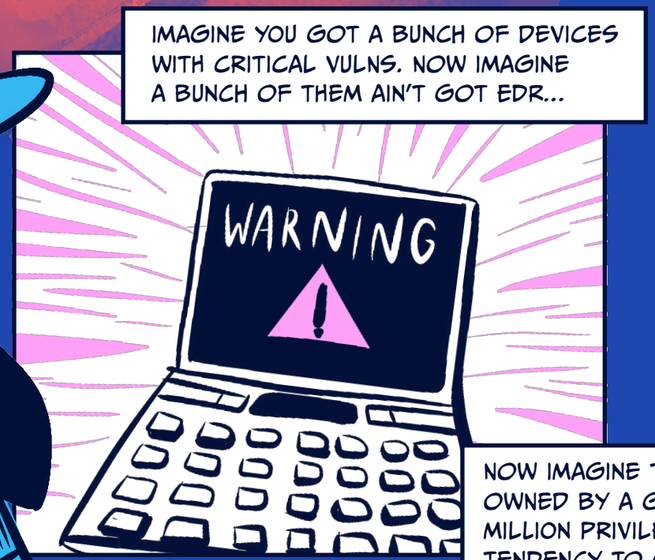
Perhaps the most impactful thing we found is that **61% of security leaders have suffered a breach because of failed or misconfigured controls** in the last 12 months. Which is a lot.

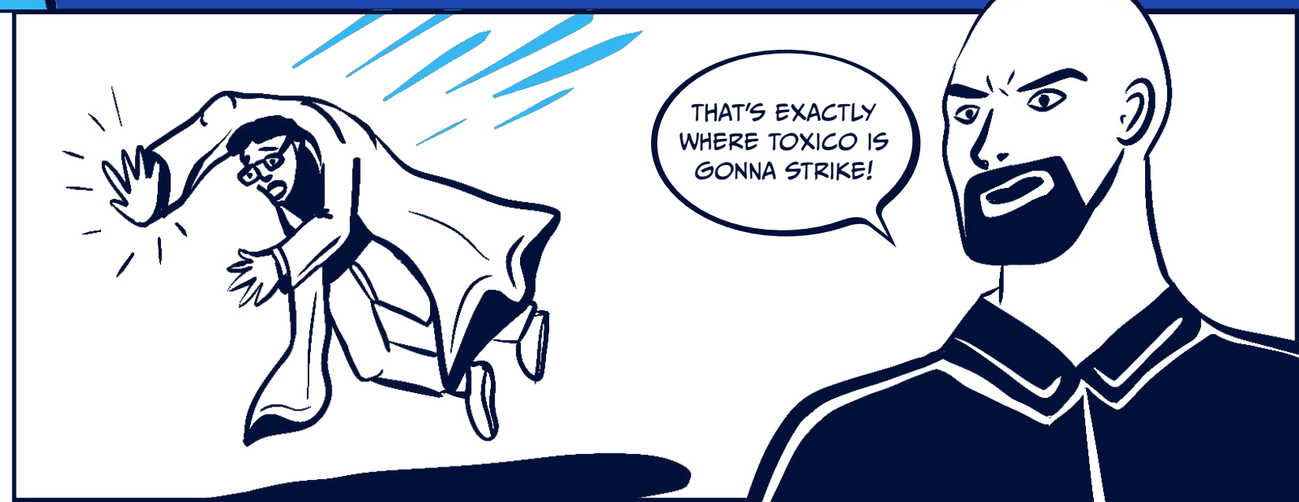
But it gets worse. Two thirds (65%) of which cost organizations more than $1million. And 12% over $10m.

67% went on to agree that they needed to trade off on risks because it was impossible to protect everything.

61%
HAVE SUFFERED A BREACH DUE TO CONTROL FAILURE







A major threat: Toxico

Your fellow cybersecurity leaders are also feeling the pain of “toxic combinations”.

The term “toxic combinations” alludes to pharmacology in the sense that if you put two drugs together, you can kill the patient.

In the context of cybersecurity, it means risks that are compounded by the presence of other significant risks in the same place. For example, a laptop with a critical vulnerability that doesn’t have endpoint protection.

A staggering **92% of security leaders agree that toxic combinations are a cause for real concern**.

ACT 2
HOW DO WE COMBAT HIDDEN RISK?

Communication and reporting are increasingly fundemental to cybersecurity. Delving into the data, we can see that leaders are striving to share the best information they can.

There is a clear need to communicate both the state of security controls (79% said they were doing so) and regulatory and audit compliance (84% currently delivering - or have plans to in the near future).

Clearly, cybersecurity leaders are working hard on reporting. So much so that **their teams spend 46% of their time on reporting**.*

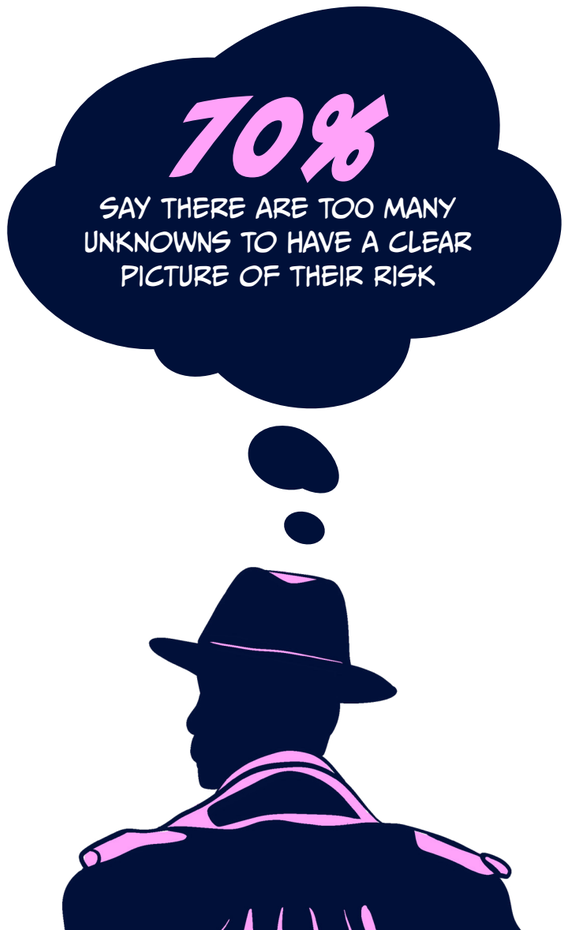
On the surface, everything seems fine. Aside from the large amount of time spent, perhaps. But, when you analyze data like in this report, the most interesting insight is often in the contradictions.

Despite the confidence in reporting, **70% say there are too many unknowns to get a clear picture of risk**. It's troubling to see that security leaders are stranded on a tightrope. On one side is a clear picture of risk. The other is meeting reporting and compliance demands. Internal requirements are putting real pressure on the accuracy of the information being shared

With contradiction, though, comes action.

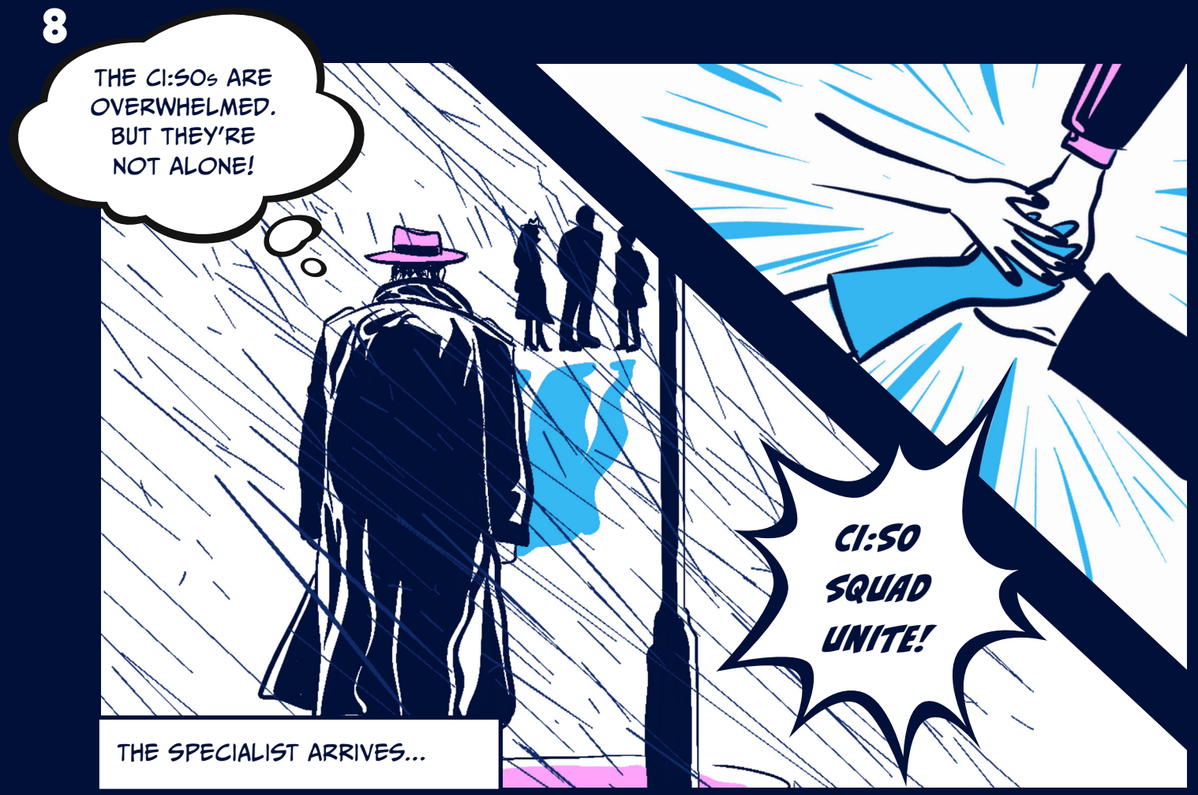
We see cyber professionals battling to meet the demands on them, knowing where the shortcomings are and taking steps to spend more in the right places (assurance and control governance). In fact, **95% have seen an increase in budget for controls governance**. And half say it has increased by 25% or more in less than two years.

They want to know what data to trust, what to report, and ultimately, how to make the right decisions.



*Panaseer Security Leaders Peer Report 2024

MEANWHILE...



ACT 3
CI:SOs UNITE

Rightly or wrongly, cybersecurity is under pressure. And leadership is feeling the brunt.

90% of CISOs are being asked to give more assurances on security controls than ever, communicate with more stakeholders than ever (**85%** agree) and face greater scrutiny than ever.

We're all for ownership, responsibility, and accountability in cybersecurity. But that isn't the same as blame. Increased legislative and regulatory scrutiny brings the apparent need to apportion blame. We've entered the age of CISO liability, where our leaders seem to be living under a corporate sword of Damocles.

75% of CISOs believe they face greater personal liability. And while **70%** feel it's fair, **72%** have personal indemnity in place, with another **20%** seeking to get it in the next year. **13%** are paying for it themselves.

But the current landscape doesn't set security leaders up for success. They're in an environment where **two thirds (67%) agree that specialized tools for cyber analytics aren't readily available**. Almost half (**46%**) have visibility gaps because data is only available where tools are deployed. And **72% believe they could stop more breaches if they spent less time reporting**.

85% OF SECURITY LEADERS FACE GREATER SCRUTINY THAN EVER!

Is it OK to hold someone liable for failure when you haven't given them the tools for success?

We as an industry need to take better care of the people leading security from the front.

ACT 4

THE CI:SOs LIVE TO FIGHT ANOTHER DAY

Security leaders are willing to take the increasing scrutiny (**85%** feel they answer to the board more) and are relishing an increased sense of influence across a wider subset of their businesses (**85%** communicate wider across their business than five years ago).

But the threat of liability has led to 47% of security leaders being more anxious**, and 15% have even considered leaving the industry**.

We have CISOs fighting the good fight, doing amazing things in headwinds that weren't there ten years ago. We need to provide support and celebrate the successes we don't see. There are no front-page headlines for the breaches that were stopped.

We can use automation and data science to support them. Address hidden risks, improve decision-making, demonstrate compliance and identify control failures. Continuously.

That's what Panaseer is doing, both with this report and our CCM solution.

Reduce control failures and manage risk. **Continuously.**