netskope

Report +

The Modern CISO:
Bringing Balance

Ready for anything

Table of Contents

Executive Summary

Businesses manage a series of balancing acts every day—between innovation and reliability, for instance, investment or profit, speed or security. Each leader contributes to how decisions are weighed and made, and traditionally Chief Information Security Officers (CISOs) have been expected to operate at one end of that scale, being the chief protector of the business.

But in new research of 1,031 CISOs worldwide, Netskope has found that this is no longer an accurate depiction of the role. According to 65% of respondents, the CISO role is changing rapidly. CISOs are becoming more proactive in their organization, with 59% classing themselves as business enablers, 57% saying their appetite for risk has increased in recent years, and 67% stating that they want to play an even more active role as a business enabler going forward.

Over the past decade, CISOs have transformed themselves, and their confidence in their ability to transform their organization is marked.

However, the majority report that there is a lag in the understanding of their potential among their C-suite peers. Two in three CISOs (65%) believe that other members of the C-suite fail to see that the CISO role makes innovation possible, and 92% said that conflicting risk appetites is an issue in their C-suite.

Netskope's researchers set out to gather CISO perspectives on both strategic and tactical considerations. Looking tactically, CISOs believe that the emerging industry trend toward zero trust principles will help them to bring balance to their organization—if they can get it right. A majority of CISOs (55%) believe a zero trust approach will enable them to balance conflicting priorities better, and that it will enable their organization to achieve key goals like moving faster (59%) and encouraging innovation (58%).

These are optimistic viewpoints, but only 44% of organizations operate with zero trust principles today, and 48% say they do not know where to start on their zero trust journey.

The paradox at the heart of the zero trust model might be one reason why understanding and adoption of it remains relatively low. Because they introduce more controls, it can seem counterintuitive that zero trust principles increase an organization's flexibility and speed.

58% of CISOs report that their executive teams and boards are asking about zero trust, but understanding does not match interest levels. To harness the benefits of zero trust and further elevate their standing among their C-suite peers, CISOs will need to drive discussion around business enablement and business risk, not fall back to typical exploration of tool investment before the right business discussions are had.

57% **of CISOs say their appetite for risk has increased in recent years**

59% **classify themselves as business enablers**

92% **are experiencing difficulty with conflicting risk appetites in the C-suite**

Today's Progressive CISO

With a remit for keeping their organizations safe, Chief Information Security Officers (CISOs) have typically been perceived as cautious and defensively minded. Such was their aversion to risk that sometimes in the past they have even been caricatured by colleagues as "the Department of No." But new research from Netskope has found that this image is outdated. In a survey of 1,031 CISOs across five countries (U.S., U.K., France, Germany, Japan), covering sectors from industrial to retail, we found a very different story—one that should help prompt reassessment from CISOs' boardroom colleagues.

Put simply, the CISO role is changing rapidly. That was the verdict of close to two-thirds of CISOs (65%) in a Netskope survey, confirmed by their responses to questions on topics from their risk appetite to their relationships with colleagues.

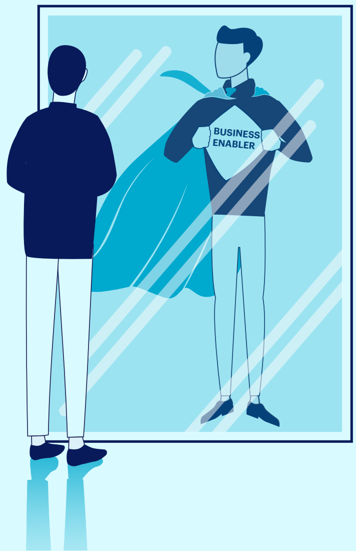
More specifically, CISOs have moved beyond the old-fashioned clichés that used to surround their jobs. They no longer view their main responsibility as trying to minimize risk by blocking innovation or turning their organizations into impenetrable fortresses. Indeed, 62% say they no longer want to be pigeonholed as the "bringer of bad news" in their companies.

Instead, CISOs increasingly relish the central role that digital technologies give them in modern enterprises. They embrace the new possibilities these create for driving innovation and generating business impact. In short, there's a new kind of progressive CISO at work today, forging new paths ahead, and working to ensure balance for their organizations.

> *62% of CISOs say they no longer want to be pigeonholed as the "bringer of bad news" in their companies*

Country Spotlight

CISOs in Germany are feeling this shift the least, with 52% agreeing their role is changing rapidly. In contrast, it is being felt most acutely in Japan, where 89% of CISOs say their role is changing rapidly.



A New Self-image

These changes are evident in the shifting ways that CISOs think about their professional persona. While 36% currently see themselves as playing a "protector" role, defending the business, this proportion looks set to shrink. Simultaneously, the proportions of CISOs who expect to be a "designer," shaping their workforce culture, or even a "navigator," driving the future direction of their organization, are forecast to increase over the next two years.

This highlights an ongoing shift from a more defensive to a more proactive enablement role.

In some ways, this evolution in how the sector views itself shouldn't come as a surprise. For a while now we've seen industry bodies and consultancies adopt new language that reflects reframed perceptions of the role infosec professionals play. Few industry events and conferences these days, for example, are complete without a session on "resilience" rather than "cybersecurity" per se. Likewise, risk is increasingly framed by these industry groups as a business-wide, rather than purely technical, issue. In our survey, 65% of CISOs agreed that they increasingly see their role as improving business resilience, not just managing cyber risk.

So what marks out today's progressively minded CISO in practice? Most of all, they want to play a more proactive role in their organization. In fact, 66% of CISOs wish they could say "yes" to the business more often.

This is what CISOs mean when they say they want to become "business enablers." A majority of CISOs (59%) already see themselves this way, and 67% want to play an even more active role as a business enabler moving forward. Just one in four (26%) say they do not see themselves as business enablers yet, but would like to be.

> *65% of CISOs increasingly see their role as improving business resilience, not just managing cyber risk*

Country Spotlight

43% of CISOs in the U.K. do not consider themselves business enablers yet but would like to be (vs. a global average of 26%) — reflecting the fact that the U.K. had the lowest number of CISOs who think they already are enablers in their organization.

> *67% of global CISOs want to play an even more active role as a business enabler moving forward*

+
Growing in Confidence

As they develop in self-belief, CISOs also expect to mature in their decision-making in the coming years. That can be observed in their answers to a series of questions the researchers posed around typical professional dilemmas.

In four core areas where business decisions frequently focus—productivity, innovation, process, and agility—CISOs were asked whether they are guided by the creation of a more open and flexible organization or a more closed and secure one. This scale was specifically chosen to ensure that neither extreme was obviously and universally preferable.

The data shows that CISOs currently tend to sit in the middle of that scale, but they became more definitive in their choices when they looked two years ahead. That pattern was consistent across all four decision-making realms.

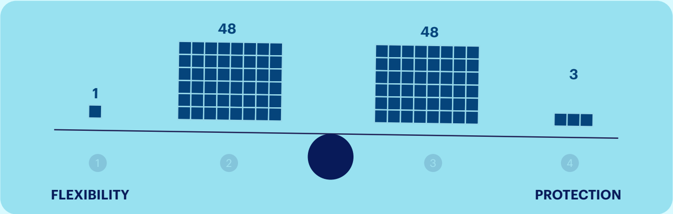
This finding raises some intriguing possibilities. It may be that CISOs are waiting for the business to make certain decisions, or ride out current market conditions, before they feel able to focus on one end of the scale over another. Or it may be that they are currently evolving their technology infrastructure and security posture in a manner that they believe will soon lessen the pressure they feel to provide that balance.

Q On a scale between 1 and 4, where do you fall when making decisions for the business as CISO?

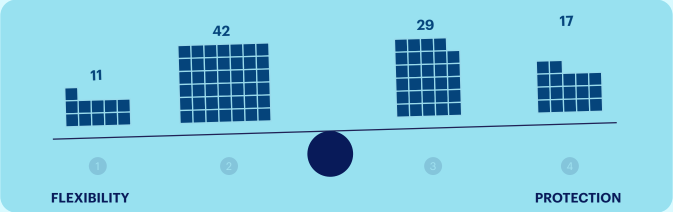
■ number of respondents

Workforce Productivity:
The requirement to enable your people to work securely yet effectively from wherever they are

CISOs Now

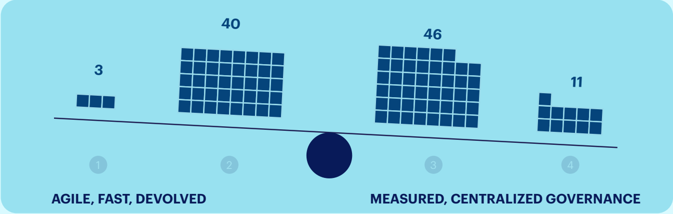


CISOs in 2 Years

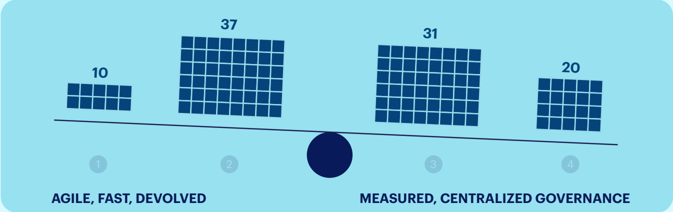


Business Agility:
The responsiveness of the business. Its ability to make key decisions and remain competitive

CISOs Now

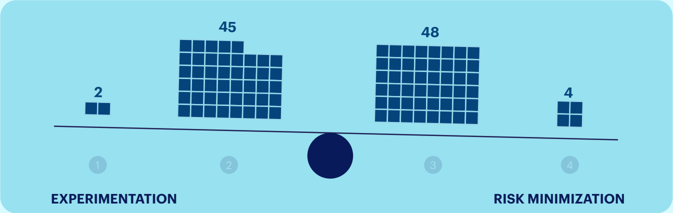


CISOs in 2 Years

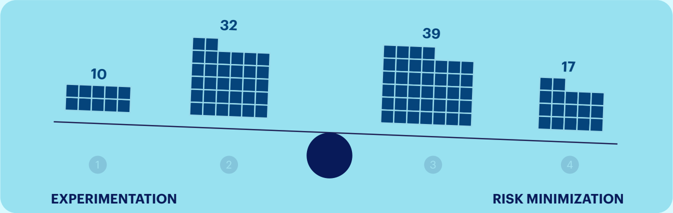


Business Innovation:
The requirement for a business to continuously evolve and grow

CISOs Now

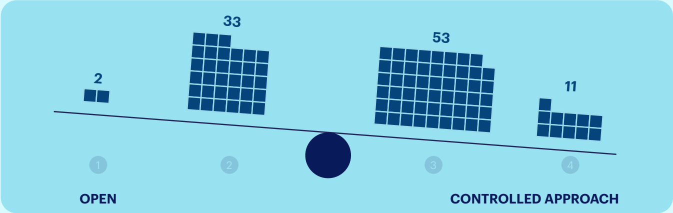


CISOs in 2 Years

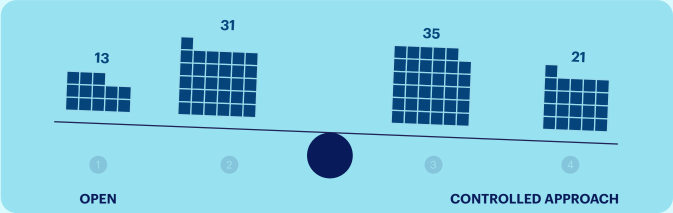


Business Process & Efficiency:
Providing the right people with access to the information, data, and tools they need

CISOs Now



CISOs in 2 Years



Reasons CISOs give for their increased risk appetite

1. Better access to data and analytics
2. Experiencing a cyber incident
3. Zero trust
4. Increased confidence in role
5. Shared accountability
6. Advances in security technology
7. Pressure to innovate
8. Desire for bigger role
9. New mandate

Whatever the underlying reason, CISOs anticipate becoming more decisive over the next couple of years—another indication of how their role is changing.

Strikingly—given the acknowledgement of the growing cyber threats faced by organizations—CISOs' appetite for risk, far from being a professional constant, has actually increased over the past five years. A majority (57%) said so, with one in seven (13%) saying it has significantly increased.

While better access to data and analytics (76%) is believed to be an important driver of this increased risk appetite, first-hand experience of a specific cybersecurity issue (74%) was the second most cited reason for the increase.

> *Whatever the underlying reason, CISOs anticipate becoming more decisive over the next couple of years—another indication of how their role is changing*

+

Clashing Perspectives

The data is clear that CISOs are ready and willing to play a more active role in their organizations, with a more assured attitude to risk at its root. However, there is a catch. While these changes in mindset and ambition sound positive, and reflect a more confident community of practitioners, there is a perception among CISOs that they aren't yet fully accepted by their colleagues.

While 72% of CISOs who reported an increase in their risk appetite recognized a new mandate from business leadership as an important factor in the change, some CISOs report that their leadership peers still harbor old-fashioned views of what they do, and their potential contribution. For instance, while two-thirds of CISOs feel that they are perceived as business enablers by other business leaders, nearly one in three (30%) believe that they are still not.

23% of CISOs strongly agree that other members of the C-suite currently fail to see the ways in which the CISO role makes innovation possible. As one tangible example of this in practice, CISOs report that their interaction with the business today is still more often about risk management (58%) than opportunity (42%), despite their appetite to be more of a business enabler.

Despite this, CISOs feel strongly about the impact they can have within their organization. Almost two-thirds (65%) believe they can enable more business innovation than other members of the C-suite—reflecting the central role that digital technologies play in modern enterprises, powering the rise of AI, unlocking efficiencies, and securely enabling new partnership and supply chain models.

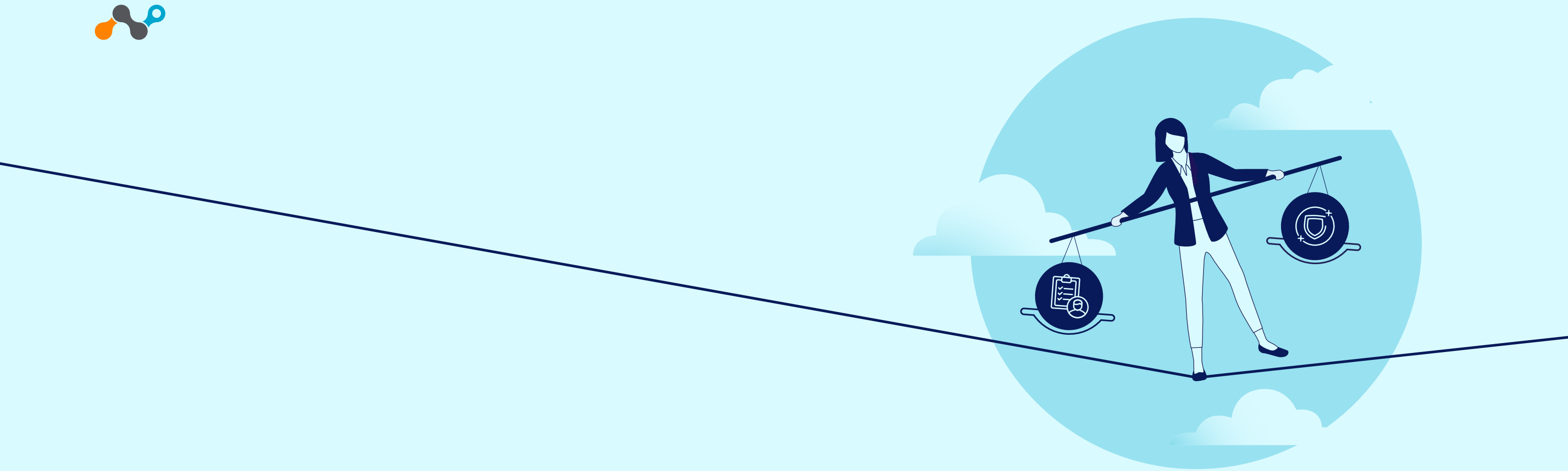
Q Do you feel that the CISO role is perceived as a business enabler by other business leaders?

	All	UK	NA	FR	DE	JP
Yes, I do	66%	50%	58%	79%	56%	91%
No, I do not	30%	48%	35%	19%	39%	8%
I do not know	4%	2%	7%	2%	6%	1%

65% of CISOs believe they can enable more business innovation than other members of the C-suite

30% think their peers don't see them as an enabler

65% think their peers don't think they make innovation possible



There are other clashes and contradictions too. Only 16% of CISOs classify their risk appetite as low, yet when asked about their perspective of their colleagues' risk appetite, twice as many of them (32%) would describe their CEO's risk appetite as low. When juxtaposed, these two figures suggest CISOs believe they have a higher risk appetite than their CEO—a reversal of a common assumption. Research participants report that these differing views can manifest as real problems in the boardroom.

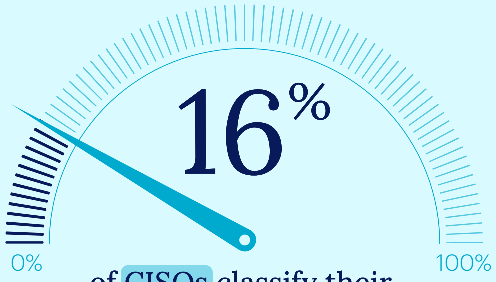
An overwhelming majority (92%) of CISOs confirmed that conflicting risk appetites is an issue in their C-suite, with 32% of them saying these differing perceptions cause conflict often.

Given these reported clashing perspectives and approaches, today's CISOs are working hard to strike the right balance in their organization. They need to find a happy medium between enabling their business and defending it, simultaneously embracing the new possibilities of their role to help achieve business goals, while still delivering their core remit and ensuring security priorities are met.

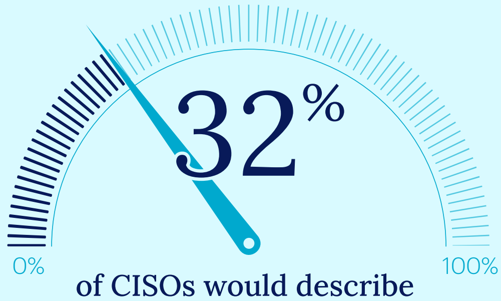
Not surprisingly, then, a large majority of CISOs (70%) see their role as "a balancing act." Two-thirds (66%) say they are "walking a tightrope" between what the business wants and what makes sense from a security perspective. Little wonder that 66% of CISOs see influencing and educating other members of the C-suite as an increasingly important aspect of their role.

Country Spotlight

This was felt particularly strongly in France and Japan, where 74% and 88% of respondents respectively said they felt other members of the C-suite currently fail to see that the CISO role makes innovation possible.



of CISOs classify their risk appetite as low



of CISOs would describe their CEO's risk appetite as low

Zero Trust Approach

> *The appeal of a zero trust approach is that while it sounds rigid in theory, paradoxically in practice, when done right (building upon extensive contextual signals), it actually helps organizations enhance their agility—a key priority for business leaders in today's fast-moving world*

So where are CISOs looking, in their search for solutions and strategies that will help them in this balancing act? The zero trust security model seems to be riding high in the hype cycle, with CISOs reporting a long list of expected benefits from the approach.

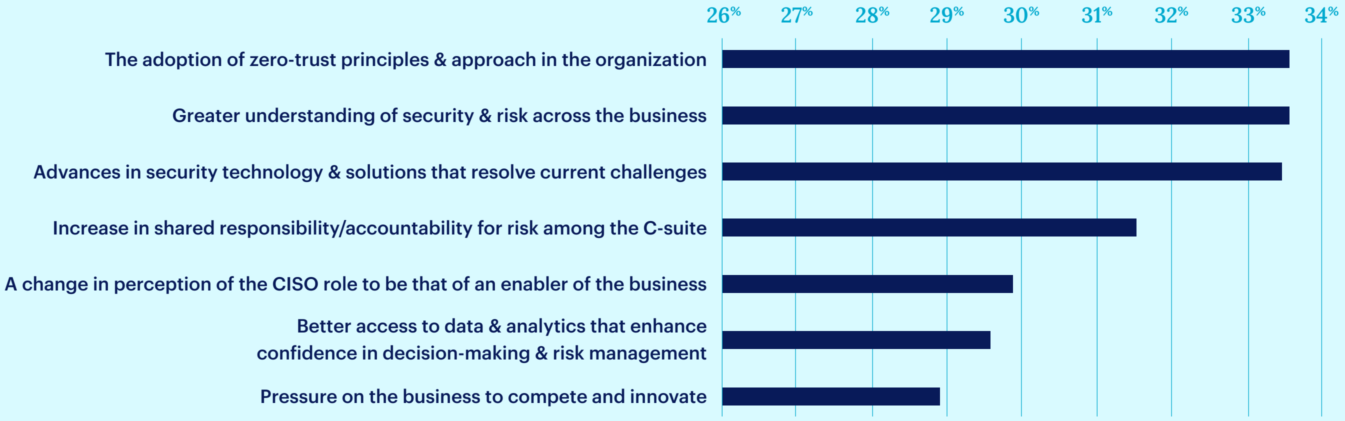
Originally coined in the 1990s, but only popularized from the late 2010s onwards, the zero trust security approach has been widely embraced by the industry as cloud-based services and remote working have challenged traditional ways of granting access to resources no matter where users are. The appeal of a zero trust approach is that while it sounds rigid in theory, paradoxically in practice, when done right (building upon extensive contextual signals), it actually helps organizations enhance their agility—a key priority for business leaders in today's fast-moving world —by giving the appropriate users access to the resources they need without any of the friction they've come to accept.

That helps explain why attitudes among CISOs toward zero trust principles are already very supportive. A majority agree that zero trust enables organizations to move faster (59%), encourage innovation (58%), increase flexibility (58%), and improve decision-making (55%). Similarly, 55% of CISOs believe a zero trust approach enables them to balance conflicting priorities better.

Looking ahead, CISOs go so far as to point to the adoption of a zero trust approach as the single most significant factor in organizations becoming more open and flexible over the next two years. No security model is a silver bullet on its own, but it's clear that CISO expectations of zero trust are consistently positive—and they have high hopes for its continuing impact.

There are some signs that the zero trust model has already helped organizations and information security functions gain confidence. 73% of CISOs say that the adoption of a zero trust approach in the business helped increase their risk appetite in recent years (30% go further, saying it has played a very important part in these risk appetite changes).

Q **If your organization were to shift from a more closed/protected environment to a more open/flexible one over the next two years, which of the following, if any, would you expect to be the most significant factors in driving that?**



Ultimately, zero trust is about making sure the right people have the right access to the right things within an organization's network. That's about enablement as much as it is about controls.

A Paradoxical Presentation

While the CISOs the researchers spoke to tended to focus on the anticipation and promise of zero trust, the research turned up some warning signs too. For instance, it seems that excitement for the zero trust model can sometimes get ahead of what most security professionals, and their organizations, are doing in practice. Fewer than half of organizations globally (44%) operate with zero trust principles today—although a further 38% say they plan to adopt zero trust soon.

Also noteworthy is the fact that the zero trust philosophy does not appear to be well understood by the wider business leadership—despite their familiarity with the term. While 58% of CISOs report that their executive team is asking them to pursue a zero trust approach, 51% state that their executive team or board doesn't actually understand what that means.

It's intriguing to see the extent to which security leaders are being asked about zero trust by their C-suite peers, but if CISOs are to realize their objective of being recognized as business enablers and strategic partners, they will need to avoid getting down into the weeds of tools and technologies when communicating with their C-suite peers. Concepts of zero trust (and zero friction) are both important only in terms of what that enables—risk mitigation and business enablement.

> *The paradox of zero trust is that the ultimate closed environment creates the most open, agile, and innovative business*

The paradox at the heart of the zero trust model might be one reason why understanding and adoption of it remains relatively low.

Zero trust principles introduce more controls and reduce access to the corporate network and applications, which all sounds like it should add friction and slow down the enterprise. Yet, counterintuitively, it actually increases the flexibility and speed of the organization—because these granular controls enhance confidence in decision-making.

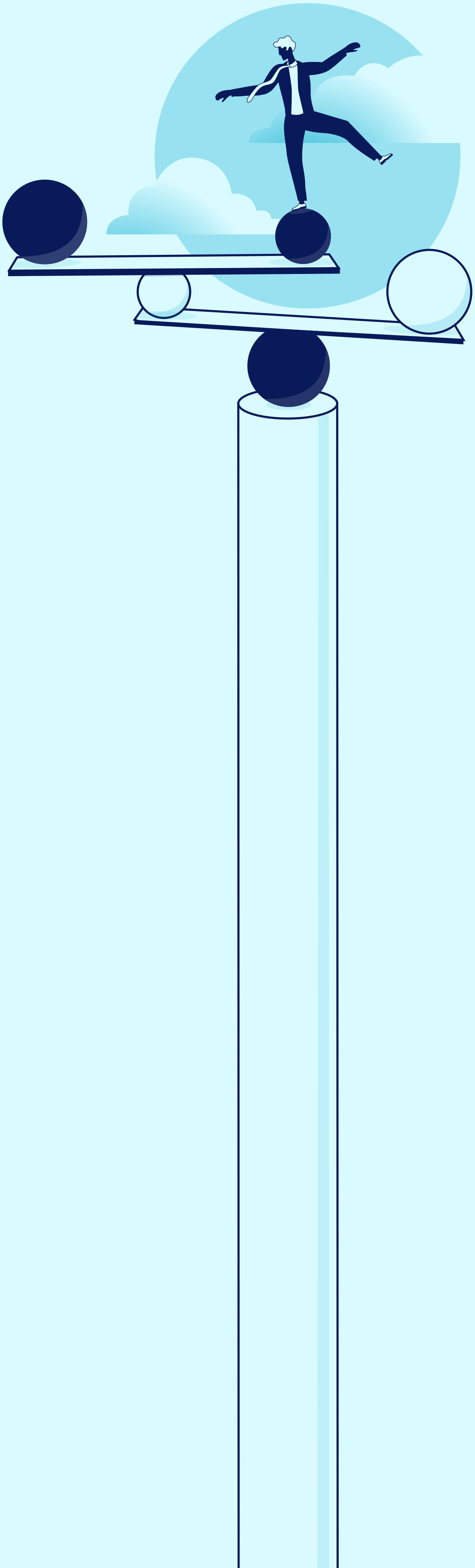
In other words, the paradox of zero trust is that the ultimate closed environment creates the most open, agile, and innovative business.

Q To what extent do you agree or disagree with the following statements?

58%
My executive team or board is asking me about zero trust

51%
My executive team or board doesn't really understand what zero trust is

Conclusion



A decade ago CISOs began to change, and the data today shows that modern CISOs have found their way out from under the wing of other members of the executive team and are ready to take their place in broad business discussions and decision-making.

The trend is truly global, with confident CISOs no longer being limited to back-office support functions. They are clear—they want to contribute to the business objectives, enabling growth and innovation.

But while the CISOs themselves understand their capability, there is still some significant work to be done to ensure that the role they perform is not seen simply as a backstop, a technical insurance, or the designated naysayer.

Technology evolution has helped the CISO to adjust their own views both of risk and their role, but technology alone cannot navigate the perception challenge among peers. Zero trust is the latest buzz phrase—and it's one that has gathered traction among non-technical senior stakeholders—but CISOs would do well to treat the term with caution. It is doubtless the right approach to take to build a security posture for frictionless enablement, but discussions with C-suite peers should focus less on tools and technology and more on answering questions of "how do we enable this business case?"

CISOs who are able to define the ways in which they are helping their C-suite peers to acquire new revenues, drive efficiencies, and navigate regulatory requirements will be recognized as valuable contributors at the highest levels.

About Netskope

Netskope, a global SASE leader, helps organizations apply zero trust principles and AI/ML innovations to protect data and defend against cyber threats. Fast and easy to use, the Netskope One platform and its patented Zero Trust Engine provide optimized access and real-time security for people, devices, and data anywhere they go. Thousands of customers trust Netskope and its powerful NewEdge network to reduce risk and gain unrivaled visibility into any cloud, web, and private application activity—providing security and accelerating performance without compromise. Learn more at netskope.com.