RETAIL SECTOR EDITION

netskope

Report +

The Retail CISO: Bringing Balance

Ready for anything

Table of Contents

Executive Summary

Organizations 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 research of 1,031 CISOs worldwide, Netskope has found this is no longer an accurate depiction of the role in the retail sector. While 65% of CISOs across all industries reported the role was changing rapidly, this number grew to 84% of respondents in the retail and consumer industries sectors.

Within retail, an overwhelming majority (98%) of CISOs now consider themselves to be business enablers (well above the cross-sector average of 59%), and more than four-fifths (87%) want to play a more active role as a business enabler going forward (compared to an average of 67%). 81% say their appetite for risk has grown in recent years (much higher than the average of 57%).

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

However, the majority of research participants report a lag in the understanding of their potential among their C-suite peers. 84% of retail CISOs believe other members of the C-suite fail to see that their role makes innovation possible, and 100% of retail CISOs surveyed said conflicting risk appetites is an issue within their C-suite.

Netskope's researchers set out to gather CISO perspectives on both strategic and tactical considerations. Looking tactically, CISOs believe the emerging industry trend toward zero trust principles will help them to bring balance to their organization—if they can get it right. More than two-thirds of retail CISOs (72%) believe a zero trust approach will enable them to balance conflicting priorities better (higher than cross-sector averages of 55%), and that it will enable their organization to achieve key goals like moving faster (77%) and encouraging innovation (71%).

These are optimistic viewpoints, and 71% of CISOs from retail organizations report operating with zero trust principles today, but almost the same number (70%) also admit they do not know exactly where to start on their full zero trust journey.

The paradox at the heart of the zero trust model might be one reason why understanding 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.

76% of retail sector CISOs report 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 elevate their standing among their C-suite peers, CISOs will need to ensure they are not tempted into conversations about technology. Communication must avoid discussion of tools, instead focusing on business enablement and business risk.

81% **of retail CISOs say their appetite for risk has increased in recent years**

98% **classify themselves as business enablers**

100% **are experiencing difficulty with conflicting risk appetites in the C-suite**

Today's Progressive CISO

With a remit for keeping their organizations safe, 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 this image is outdated. In a survey of 1,031 CISOs across five countries, covering sectors from industrial to retail, finance and healthcare, 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. In the retail and consumer industries sector, this number was significantly higher (84%).

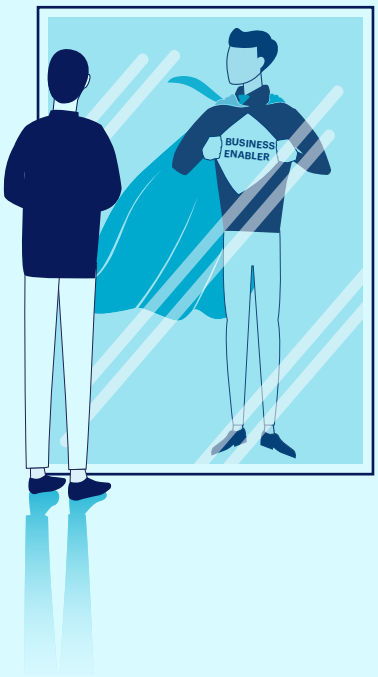
More specifically, CISOs have moved beyond the old-fashioned clichés that used to surround their jobs. They no longer view their main responsibility as trying to minimize risk by blocking innovation or turning their organizations into impenetrable fortresses. Indeed, within the retail sector, more than 83% of CISOs 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.

> *83% of retail 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 different ways across different sectors. All research participants were asked to describe their current role, choosing between Protector (defending the business), Catalyst (enabling business decisions), Designer (creating structures and workforce culture), and Navigator (driving future direction). Across all sectors, CISOs described their current role as a Protector, but these answers spread more broadly among the categories when participants were asked to forecast two years ahead.

Retail was the exception: 69% of CISOs currently see themselves as playing a "Protector" role and this proportion looks set to grow. 84% of retail CISOs felt that the most important role they could play was the Protector role, and 71% saw themselves best described in that way in two years' time. This may be a reflection of the way organizations with extensive customer and payment data see themselves on the frontlines of cybersecurity.

The retail CISO is very clear on the ways protection is shifting from a purely defensive to a more proactive enablement role.

In our survey, 86% of retail sector CISOs stated they increasingly see their role as improving business resilience—not just managing cyber risk—and they want to play a more proactive role in their organization. In fact, 88% of retail sector CISOs wish they could say "yes" to the business more often (compared to 66% average across all sectors).

This is what CISOs mean when they say they want to become "business enablers." A majority of CISOs (59%) already see themselves this way—but this number is significantly higher in the retail sector where 97% already see themselves as business enablers. Despite that head start, 87% of retail CISOs want to play an even more active role as a business enabler moving forward (higher than the cross-sector average of 67%).

> *86% of retail 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.

> *87% of retail 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.

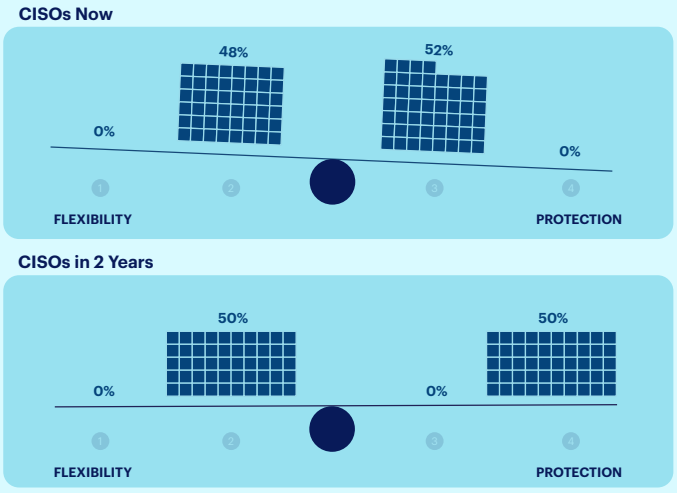
The data shows CISOs currently tend to sit in the middle of that scale, but they became more definitive in their choices when they looked two years ahead. That pattern was consistent across all four decision-making realms.

When looking specifically at the way they intended to support business agility (defined as the responsiveness of the business and its ability to make key decisions and remain competitive), retail CISOs saw themselves increasingly drawn to "measured, centralized decision-making with high levels of governance." This is notable because it runs completely in contrast to CISOs

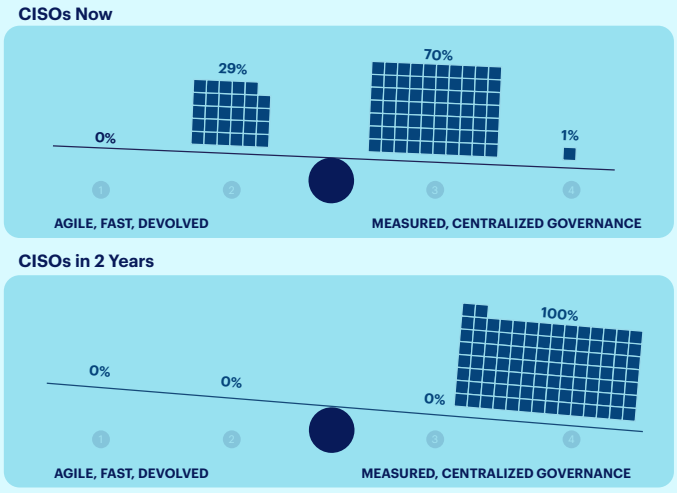
Q On a scale between 1 and 4, where do you fall when making decisions for the business as CISO?

percentage of respondents

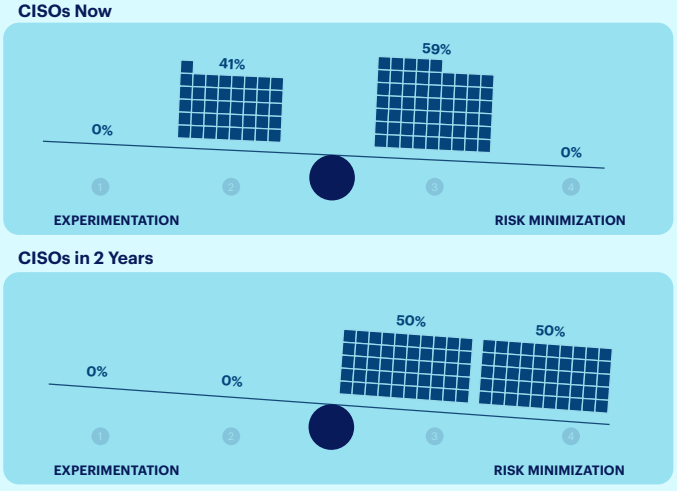
Workforce Productivity:
The requirement to enable your people to work securely yet effectively from wherever they are



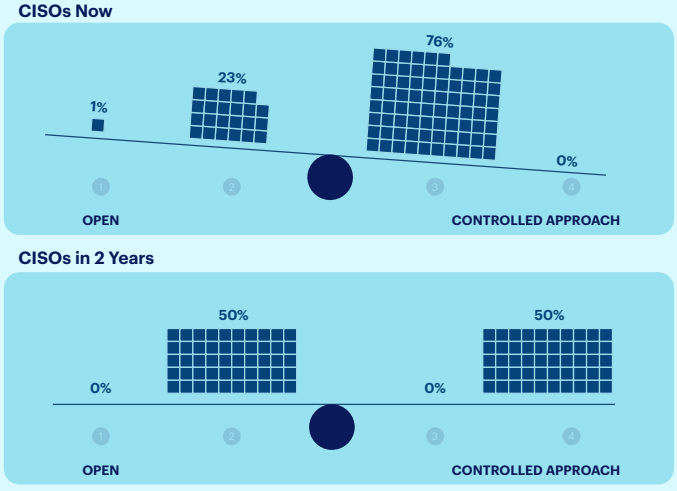
Business Agility:
The responsiveness of the business. Its ability to make key decisions and remain competitive



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



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



from other sectors (who saw themselves moving the other way—drawn to a model described as "agile, fast decision-making with devolved responsibility").

This same polarization was seen when retail CISOs considered workforce productivity. While none of the participating CISOs currently placed themselves at the far end of the scale, identified as "protection of workforce," the majority (52%) identified with that end of the scale over "flexibility of workforce." But looking ahead at two years from now, retail CISOs aren't expecting these priorities to shift. In fact, all but two retail CISOs surveyed didn't expect to change. These findings perhaps reflect the intention for security leaders to perhaps catch up with some of the business-led allowances that have been made in recent years, and perhaps they tie to the appetite for zero trust, which we will analyze in a later section.

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 of all CISOs (57%) said so—and an even higher percentage among the retail sector (74%).

Advances in security technology and solutions (88%) are believed to be an important driver of this increased risk appetite within the retail sector, but the primary reasons for the change for this sector's cohort were attributable to personal attitude. An increase in shared responsibility/accountability for risk across the C-suite came up top (90%), alongside pressure on the business to compete and innovate (90%).

Reasons CISOs give for their increased risk appetite

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

> *Within the retail sector, there was a clear trend toward the creation of more open and flexible organizations in two years*

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. It also seems that retail CISOs are working with their C-suite colleagues in new ways.

Cross-sector averages show a perception among a third of CISOs that they aren't yet fully accepted as business enablers by their colleagues. However, retail CISOs are more positive. 83% of retail CISOs who reported an increase in their risk appetite recognized a new mandate from business leadership as an important factor in the change (11% higher than industry averages). In fact, 98% of retail CISOs feel they are perceived as business enablers by other business leaders.

Averaged across all sectors, CISOs report 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. In retail, these numbers flip, with 47% of the Interactions being about risk and 53% about opportunity.

It is clear that CISOs feel strongly about the impact they can have within their organization. 87% of CISOs in the retail sector 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.

There are other clashes and contradictions too. Less than 2% of retail sector CISOs classify their risk appetite as low, yet when asked about their perspective of their colleagues' risk appetite, nearly a quarter (23%) 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 these differing views can manifest as real problems in the boardroom.

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%

87% **of CISOs in the retail sector believe they can enable more business innovation than other members of the C-suite**

2% **think their peers don't see them as an enabler**

85% **think their peers don't think they make innovation possible**

All retail CISOs surveyed (100%) confirmed that conflicting risk appetites have created challenges for their organization.

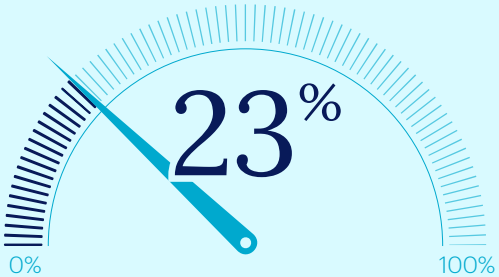
Given these reported clashing perspectives and approaches, today's retail sector CISOs are working hard to strike the right balance in their organization. They need to find a happy medium between enabling their business and defending it, simultaneously embracing the new possibilities of their role to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

Not surprisingly, then, a majority of retail CISOs (62%) see their role as "a balancing act." More than three-quarters (81%) say they are "walking a tightrope" between what the business wants and what makes sense from a security perspective. Little wonder that 85% of retail 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 retail CISOs classify their risk appetite as low



of retail 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 onward, 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.**

That helps explain why attitudes among retail CISOs toward zero trust principles are already very supportive. A large majority agree that zero trust enables organizations to move faster (77%), encourage innovation (71%), increase flexibility (71%), and improve decision-making (71%). Similarly, 72% of retail CISOs believe a zero trust approach enables them to balance conflicting priorities better.

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. 87% of retail CISOs say the adoption of a zero trust approach in the business helped increase their risk appetite in recent years (24% 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. Reported adoption of zero trust across all sectors was 44%, but the retail participants reported much higher rates (71% say their organization operates with zero trust principles today).

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 76% of retail CISOs report their executive team is asking them to pursue a zero trust approach, 67% state 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.

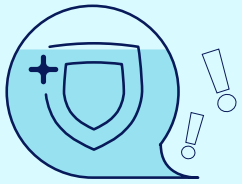
> *The paradox of zero trust is that the ultimate closed environment creates the most open, agile, and innovative business*

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.

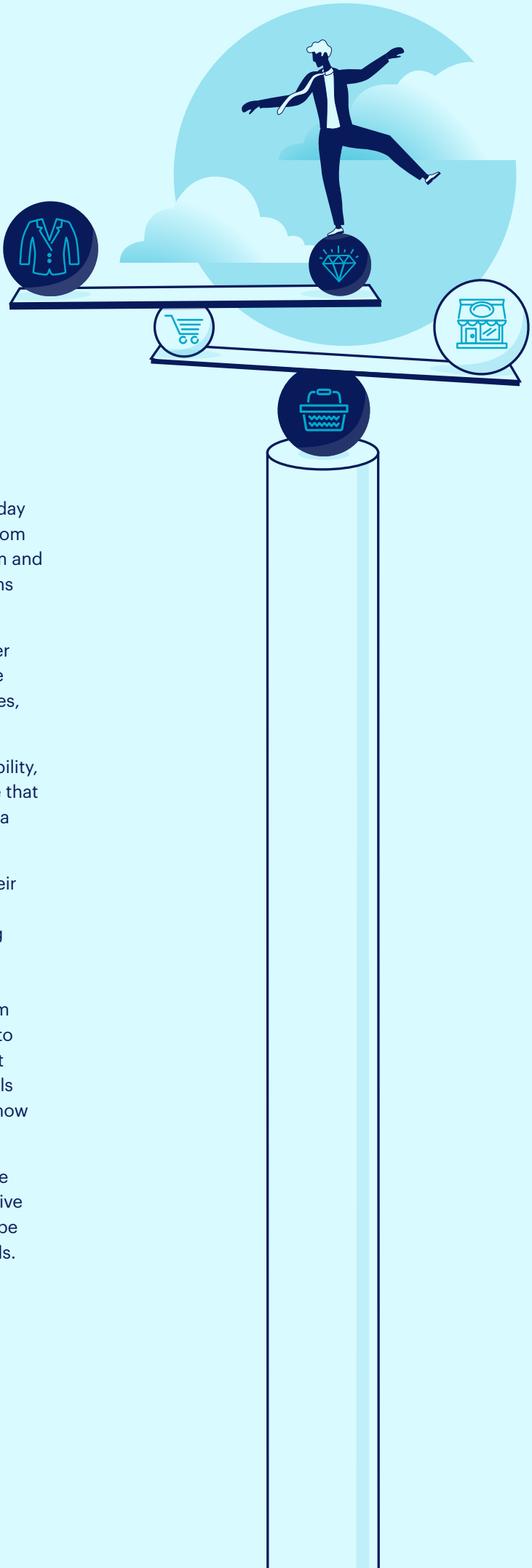
In other words, **the paradox of zero trust is that the ultimate closed environment creates the most open, agile, and innovative business.**

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



76%
My executive team or board is asking me about zero trust

67%
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 the modern CISO has found their way out from under the wing of other members of the executive team and is 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.