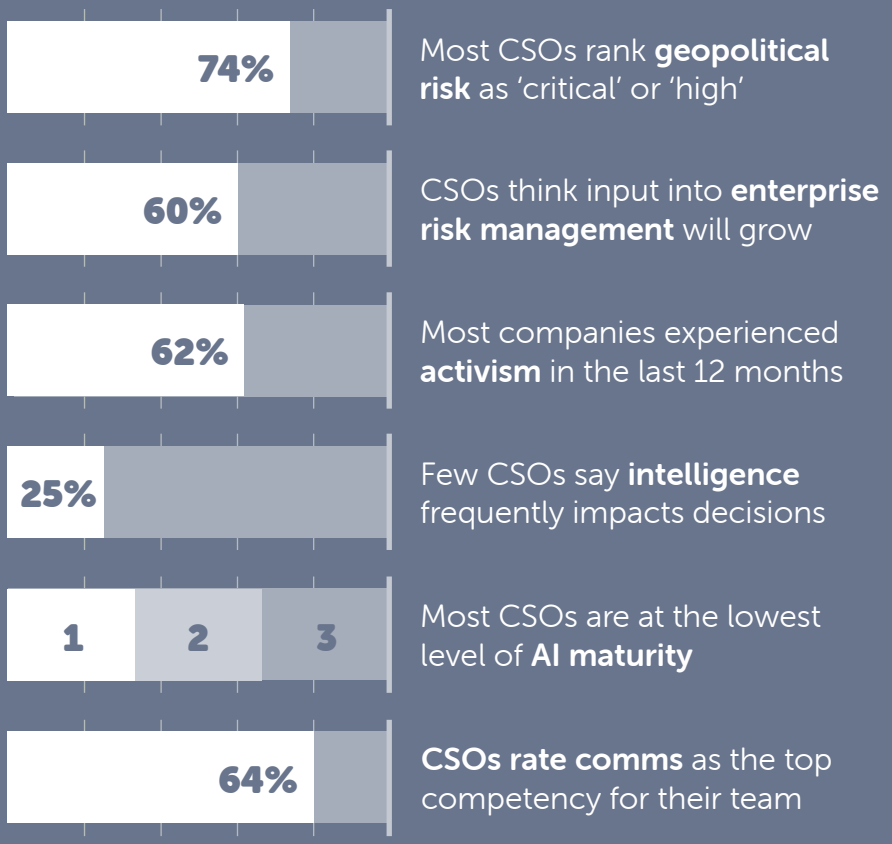
the clarity factory

Rachel Briggs OBE

Annual Chief Security Officer Survey 2026



the clarity factory

Platinum partner

ONTIC

Gold partners

ASIS INTERNATIONAL
Advancing Security Worldwide®

CSA
CORPORATE SECURITY ADVISORS

Silver partners

Factal

SEERIST®

Bronze partner

Dataminr®

Thanks to our sponsors: Ontic, ASIS International, Corporate Security Advisors (CSA), Factal, Seerist, and Dataminr. Views expressed do not necessarily reflect those of the sponsors.

Thanks to the 2026 CSO Survey Advisory Council: Ryan DeStefano, Andrew Gay, Alex Hawley, Wayne Hendricks, Charles Lacy, Joshua Levin-Soler, Duncan Manning, Kirsten Meskill, Jules Parke-Robinson, Hugh Parsons, Arlin Pedrick, Matt Sinden, and Keith White.

The survey was conducted March–April 2026. Of 176 respondents, 118 met our criteria – CSOs from international companies with over 3,000 staff – for inclusion in this report. We also interviewed CSOs and select sponsors.

The report uses 'Chief Security Officers (CSOs)' as shorthand for the most senior corporate security leader within an organisation. 'Corporate security' is known in some companies as physical or global security.

ISBN: 978-1-7384176-3-6

Contents

About the 2026 Annual CSO Survey

The Clarity Factory 2026 Annual CSO Survey contains a wealth of data to help CSOs understand industry trends, benchmark their programmes, and make resourcing and talent decisions. This year, our second, delivers trends data to show how the function has evolved in the past year, showing a clear direction of travel. We also highlight differences between US and UK CSOs, the two largest countries represented in the survey.

The data draws on 118 responses from CSOs from multinational corporations with more than 3,000 employees globally. The survey was anonymous and open to all, though only respondents that met our criteria were included. This creates a meaningful dataset for CSOs overseeing corporate security at large multinational corporations. The research also included interviews with CSOs and industry experts, and we benefited from the advice and wise counsel of our 2026 CSO Advisory Council.

The survey is kindly sponsored by our Platinum sponsor Ontic; Gold sponsors ASIS International and Corporate Security Advisors (CSA); Silver sponsors Factal and Seerist; and our Bronze sponsor Dataminr.

Clarity Up Front

"The role of my corporate security function is now less about managing incidents and more about enabling the business to navigate uncertainty with confidence."

– CSO

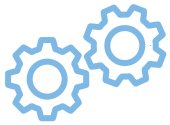
Corporate security is evolving from a protection function into an enterprise capability that creates value through insight, enterprise-wide coordination, technology-enabled decision support, and effective crisis management, alongside a consolidated security portfolio.

Five insights stand out in 2026

1. Corporate security is an enterprise integrator

- Our data suggests **companies are placing risk ownership with the most specialised function**: fewer CSOs now have primary accountability for business continuity, third party risk, and supply chain security, with their remits shifting from ownership of these areas to involvement alongside other business functions.
- This was accompanied by **higher levels of collaboration with operational risk partners**, such as the technology group, HR, and cyber security. Two-thirds of CSOs said they expected their team to contribute more to enterprise risk management over the next five years.
- The data shows **collaboration levels are up overall** in 2026, and CSOs more strongly agree that organisational silos and fragmented data limit their effectiveness.
- **Corporate security teams are consolidating around their core areas of responsibility**, such as global meetings and event security, incident management and response, and people protection (including workplace violence). The data shows the highest levels of uplift in primary accountability for CSOs in these areas.

- **Consolidation in core areas of responsibility reflects heightened risks linked to geopolitics** (ranked as a 'critical' risk by twice as many CSOs in 2026); **conflict** (rising to a top tier security risk and ranked as a top geopolitical risk by twice as many CSOs in 2026 than in 2025); and **reputation and external positioning.**
- **The message for corporate security teams in 2026 is less 'stay in your lane' and more 'specialise and connect'.**



2. Corporate security should prioritise formal integration

- In a risk environment characterised by interconnected risks, **governance forums are one of the primary mechanisms through which cross-functional decisions can be made**.
- The majority of **CSOs report in-person at least annually to their company's key leadership and risk committees, but only two-in-five report in this way to the board**. Boards and key committees are calling on corporate security to report on crisis management as well as security.
- Our data shows that **corporate security teams are collaborating in a less regular and more ad hoc way with governance partners** – including IT, finance/procurement, legal/compliance, and internal audit teams – and there was a **9% drop in regular collaboration with executive leadership**. This could be further evidence of the trend to consolidate approaches to operational risk management.

- Our data shows that **formal membership of enterprise-wide committees is a force multiplier for corporate security**. In companies with structures for managing geopolitical risk, corporate security teams are more likely to play a strategic role and are **twice as likely to be involved in scenario planning, red teaming, and exercises**. Similarly, when CSOs are members of formal taskforces for managing risks stemming from social and political polarisation, their team is typically involved in a higher number of associated risk management activities, and they are **three times more likely to brief the board or executive committee**. CSOs must advocate for formal inclusion because informal engagement tends to limit involvement to a tactical level.
- **Impactful KPIs are table stakes in corporate governance forums.** Our data shows **few CSOs use KPIs that relate to executive-level concerns**, and many confuse metrics and KPIs. CSOs must elevate their reporting to a level that is appropriate for these forums, and properly distinguish between metrics and KPIs.

3. Intelligence is a key mechanism through which corporate security can create enterprise value, but an impact gap persists

- Changes in the risk environment mean that **organisations increasingly require capabilities that can identify relationships, assess implications, and support decisions across multiple business domains**. Corporate security intelligence is an enterprise asset that can deliver these critical insights.

- **The audience for corporate security intelligence products has grown since 2025,** with greater take up from business leaders and cyber security teams, although the corporate security teams themselves remain the principal beneficiary.
- **The data shows a corporate security intelligence impact gap**: only one-quarter of CSOs said that their intelligence products frequently influenced business decisions and one-third said they influenced either rarely or not at all.
- **Intelligence teams can deliver enterprise-wide value** through shifting to demand-side delivery, stepping forward to lead the enterprise intelligence ecosystem, using AI to elevate their impact, getting serious about competing with their AI-enabled C-suite, and building the skills and competencies of the intelligence team of the future.

4. Corporate security is undergoing a tech-enabled transformation that will deliver efficiency and enhance integration, but maturity levels remain low overall

- **CSOs are prioritising technology spending that will transform corporate security into an enterprise integrator** by connecting previously fragmented data, systems, and teams. This includes AI and automation, physical security system modernisation, integration platforms, and intelligence and data platforms.

- Our data points to **three tiers of AI maturity**, from efficiency-led adopters who constitute the majority to insight-driven users (a small but growing group), and transformational leaders (a tiny minority). Corporate security teams continue to invest in professional development to enhance staff use of AI.
- There are signs of that **AI use is maturing**. Adoption has increased across all areas of corporate security and there is evidence it is being used for operational as well as intelligence purposes, and for decision enabling as well as reporting. There is also increased usage of AI in frontline activities and governance.
- **AI is reshaping work and increasing capacity rather than reducing headcount**, and CSOs are firmly of the view that human judgement remains critical to the work of the corporate security team.

5. Corporate security teams are adapting to align with their role as an enterprise connector, but there are talent issues to address

- **The composition of corporate security teams is changing, with a shift away from labour-intensive security roles and towards analytical, intelligence-led, and technology-enabled capabilities**. The roles showing the largest growth are in intelligence, higher-value GSOC positions, and crisis and resilience; while guarding, site-security positions, and operator-level GSOC roles are declining. CSOs continue to value competencies that enable their team to partner with the business.

- This shift in workforce composition is also reflected in **corporate security spending, with the largest investments in intelligence and security technology and AI, and decreases in guarding**.
- A notable exception to this is **executive protection**, with CSOs investing in both people and budget because of heightened concerns about threats to senior executives.
- **Several CSOs are experimenting with hybrid roles,** organising around integrated capabilities rather than traditional silos as a way of increasing agility, encouraging collaboration, and creating greater value from relatively small teams. **Our data suggests four hybrid hubs around intelligence, protection, risk, and finance/ insider risk.**
- **Professional development** is critical if the corporate security team is to capitalise upon its opportunity to deliver optimal value, and **there are talent pipeline risks** that must be addressed.

Our data shows a very clear direction of travel for corporate security. It also highlights a wide spectrum of maturity; the picture we paint will be very familiar to some, within reach for many, and a distant aspiration for other CSOs.

Whatever their maturity levels, we hope that all CSOs can find within the report useful and practical recommendations to drive functional innovation – and deliver enhanced operational resilience for their organisation.

Three recommendations for CSOs for 2027

CSOs drafting their strategy and resourcing plans for 2027 should focus on three priorities. For those adopting these recommendations, we include suggested metrics to track progress.

1. **Prioritise measures to strengthen corporate security's role as an enterprise integrator**

- **Invest in relationships with operational risk colleagues**.
- **Advocate for formal involvement in governance forums** to maximise the impact of corporate security.
- **Invest time and resource in getting KPIs right** to enable corporate security to present appropriately in governance forums. 'It's difficult' is not a reason to stall.
- In team development, **prioritise competencies that assist in partnership building and influence**.
- **Prioritise technology investments that will enhance integration capabilities**, such as automation and 'single pane of glass' tools.

- **Create an AI-maturity roadmap** to guide your investment, team building, and professional development plans for the next 2–3 years.

Suggested metrics:

- Formal committee memberships
- Stakeholder satisfaction
- Cross-functional projects/exercises
- Executive-level KPIs reported

2. Switch from supply-side to demand-side intelligence to maximise business impact

- **Prioritise business impact:** know your customer.
- **Switch to a demand-side intelligence model** that over indexes high-demand customers, delivers more tailored content to them, stops serving those who don't consume, and shifts perceptions of the intelligence capability across the business.
- **Step forward to coordinate the enterprise intelligence ecosystem**, convening intelligence producers from across the business to bring coherence to insight.
- **Use AI to elevate the impact of intelligence**, for example through achieving scale in collection and monitoring, improved signal-to-noise ratios, more tailored products, and enhanced decision support.
- **Get serious about competing with your AI-enabled C-suite** by getting ahead of their demands.
- **Invest in the skills you need for the intelligence team of today and tomorrow.** Complement specialist analytical skills with communication and influencing competencies.

Suggested metrics:

- Business decisions influenced
- Intelligence customer satisfaction
- Repeat demand for intelligence
- Request-to-delivery time
- AI-supported intelligence activities

3. Build a 2–3-year talent strategy to deliver on the transition from protection function to enterprise capability

- **Build a bold and ambitious 2–3-year talent strategy capable of realising the shift from a labour-intensive protective function to an enterprise capability** that delivers insight, coordination, technology-enabled decision making, and effective crisis management.
- **Investigate hybrid operating models** as a means of increasing agility and collaboration.
- **Invest in professional development,** especially in relation to technology and AI.
- **Prioritise the competencies that matter for business partnership, strategic leadership, and agility and adaptability.**
- **Address talent pipeline risks** through succession planning.

Suggested metrics:

- Succession plan coverage
- AI literacy rate
- Percentage of analytical/intelligence/ technology roles
- Hybrid role adoption

1. Security Risks

"The security threats facing my company are more complex and intense, and business leaders are far more attuned to them."

— CSO

Key findings

- **The most critical security risks are strategic and interconnected and call for structured collaboration**. These are: cyber security attacks, geopolitical risk, data/IP theft, insider risk, supply chain security and reputational risk.
- **Once again in 2026, cyber security and geopolitics dominate** as the most significant risks cited by CSOs.
- **Security risks are intensifying.** The number of risks that more than half of CSOs ranked as 'critical' or 'high' almost doubled between 2025 and 2026.
- **UK CSOs trend higher than US CSOs on overall risk rankings,** as well as specifically for conflict, geopolitics, protest/activism, and workplace violence.

The most important security risks are interconnected and strategic

Cyber security, geopolitics, data/IP theft, reputation, and insider risk dominate once again in 2026 as the most significant risks of concern to CSOs (see Figure 1). This reinforces the importance of enterprise-wide collaboration, and our data shows that corporate security teams are collaborating more regularly with operational risk partners (see Section 6 for the data on collaboration and partnership). As one CSO told us, 'The shift we're seeing is from discrete security risks to interconnected, enterprise-wide challenges.'

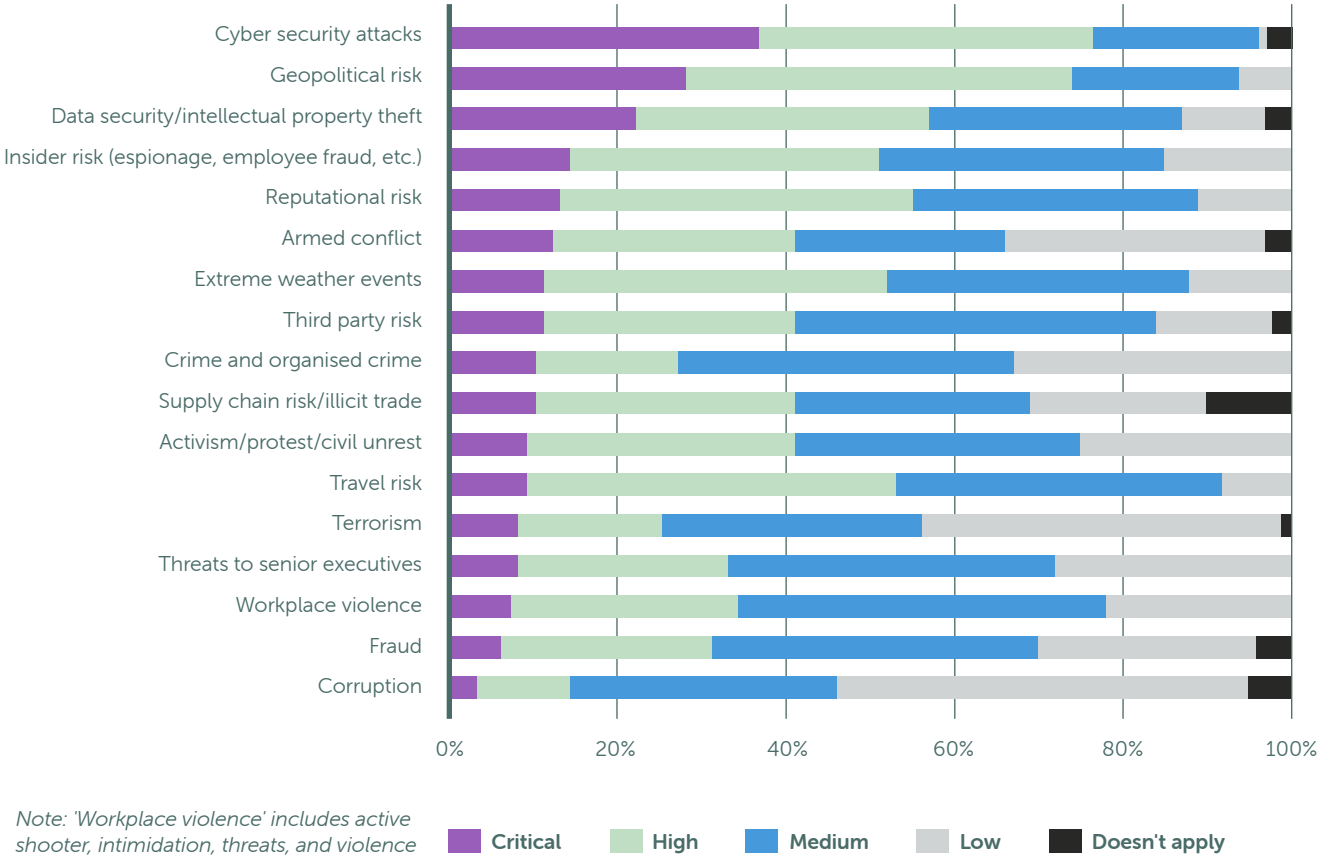
> *"The shift we're seeing is from discrete security risks to interconnected, enterprise-wide challenges."*
>
> — CSO

Our data also shows that formal and structured partnering (versus informal and ad hoc working relationships) correlates with greater influence and a strategic-level contribution for corporate security.

Security risks in 2026

- **The top 'critical' security risks** are cyber security attacks, geopolitical risk, data/IP theft, insider risk, and reputational risk.
- **Security risks are intensifying.** In 2025, four security risks were categorised as 'critical' and 'high' by more than half of CSOs. In 2026, seven risks were in this bracket.

Figure 1
Security risks impacting your organisation
CSOs from MNCs



Note: 'Workplace violence' includes active shooter, intimidation, threats, and violence

Cyber security remains the top security risk, with around one-third of CSOs categorising it as 'critical' and three-quarters as 'critical' or 'high'. One CSO summed up a view shared by all those we interviewed: 'The big existential risk for our company is cyber risk. As Jaguar Land Rover found out, a cyber attack can be near fatal for a corporation. That's the thing that could bring our company to its knees.' As our data on collaboration (Section 6) shows, corporate security is playing an enhanced role in bolstering companies' cyber security resilience, although more work is needed.

Geopolitical risk is a much bigger concern in 2026, with more than twice as many CSOs categorising it as 'critical' (28% up from 13% in 2025) and three-quarters (74%) categorising it as 'critical' or 'high' (up from 67% in 2025).

Armed conflict is seen as a higher security risk in 2026, with 41% of CSOs categorising it as 'critical' or 'high' (compared to 31% in 2025). 'Ongoing conflict' as a geopolitical risk has also risen from a second-tier issue to a key concern for CSOs. It should be noted, however, that the 2026 survey opened just as the conflict with Iran started, which might have impacted results.

Travel risk has also increased, with a majority of CSOs ranking it as 'critical' or 'high', up from around one-third in 2025. This is likely due to increased conflict and geopolitical risks.

Traditional security risks – including threats to senior executives, workplace violence, and terrorism – remain important but are seen as having a lower impact on the business.

Differences between US and UK CSOs

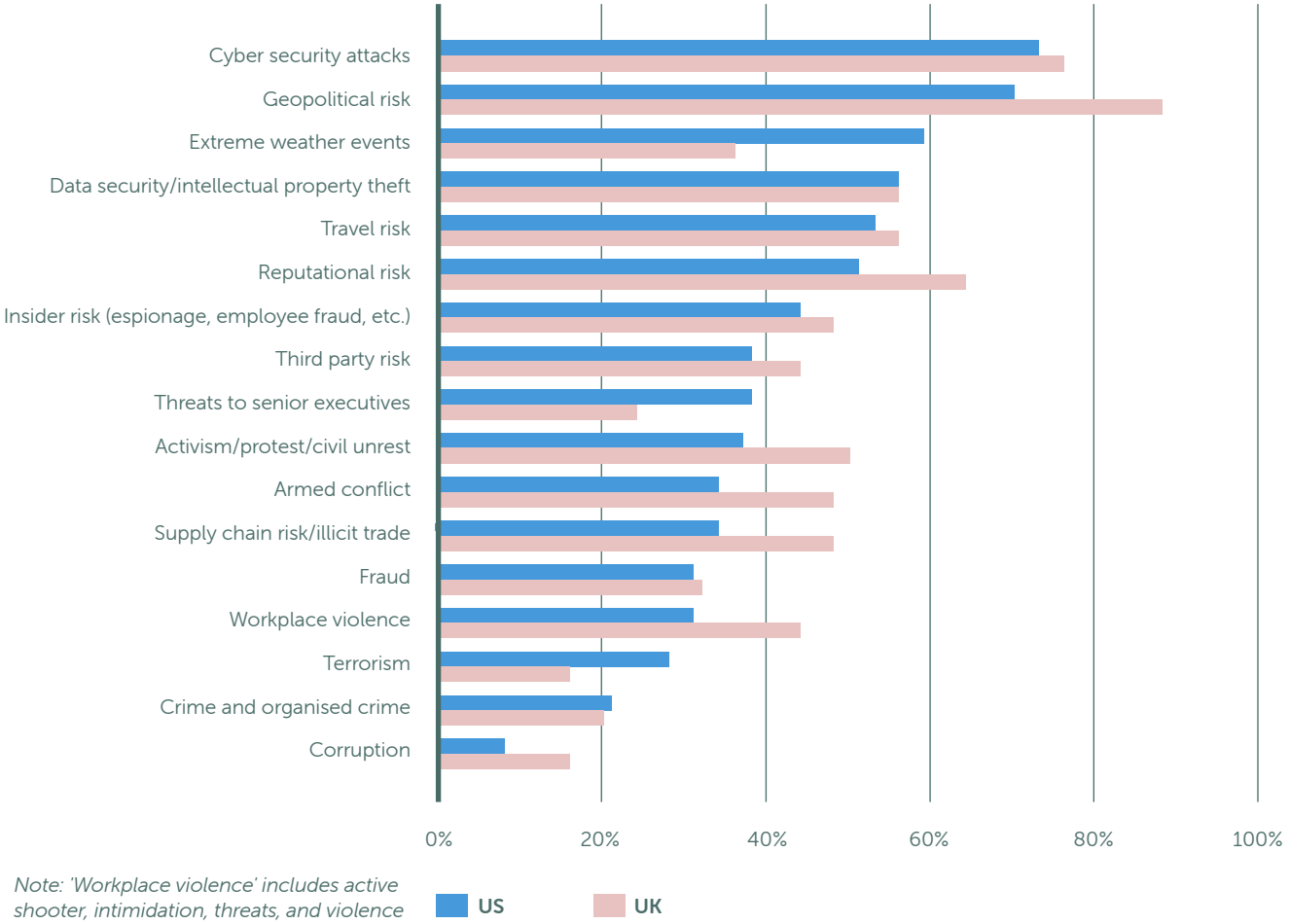
Our data (see Figure 2) revealed the following:

- **Risk ratings:** US CSOs trend lower than UK CSOs in overall risk ratings.
- **Geopolitical risk and armed conflict:** UK CSOs trend higher than US CSOs, perhaps due to proximity to wars in Ukraine and the Middle East.
- **Protest/activism and workplace violence:** US CSOs trend lower than UK CSOs, which is surprising, especially for workplace violence.

Figure 2

'Critical' or 'high' security risks to your organisation

US and UK CSOs from MNCs



Note: 'Workplace violence' includes active shooter, intimidation, threats, and violence

2. Geopolitical Risks

"Most organisations struggle to understand the potential tangible impacts [of geopolitical dynamics] on the business. This is where corporate security can add value."

— CSO

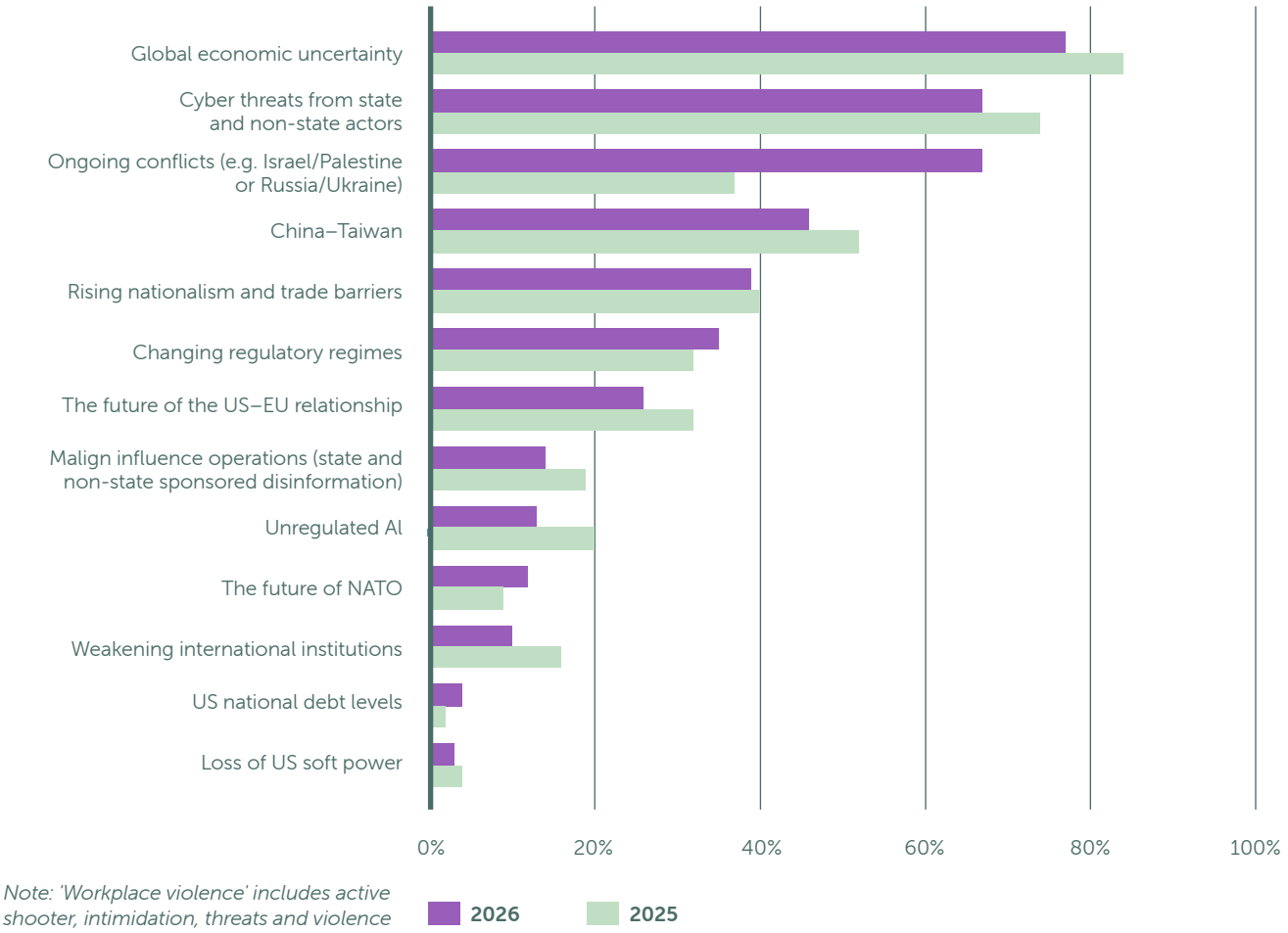
Key findings

- **Conflict moved from a second-tier risk in 2025 to a top-tier risk in 2026,** with twice as many CSOs ranking it as a top-five geopolitical risk in 2026.
- **UK CSOs trend higher than their US counterparts** when ranking almost all geopolitical risks.
- **Corporate security teams have three key assets to offer their company in managing geopolitical risks:** insight on threats; crisis and incident response capabilities; and trusted external networks.
- **Corporate security teams are more likely to contribute at a strategic level when operating through formal structures within the company.**

Figure 3

Top five geopolitical risks to your organisation (2026 vs 2025)

CSOs from MNCs



Note: 'Workplace violence' includes active shooter, intimidation, threats and violence

Top five geopolitical risks in 2026:

1. Global economic uncertainty
= 2. Cyber threats from state and non-state actors
= 2. Ongoing conflicts
3. China–Taiwan
4. Rising nationalism and trade barriers
5. Changing regulatory risks

Ongoing conflicts: From second- to top-tier risk

67%

of CSOs ranked 'ongoing conflicts' in their top-five geopolitical risks.

Conflict has moved from a second-tier to top-tier risk. **The proportion of CSOs who ranked 'ongoing conflicts' as one of their top-five geopolitical risks almost doubled between 2025 and 2026,** jumping from 37% to 67% (see Figure 3). This represents the most significant risk increase across the dataset and puts conflict on a par with cyber threats as a geopolitical risk. UK CSOs were more likely than their US counterparts to rank ongoing conflicts in their top-five (48% versus 34%).

The recent wave of conflicts is causing many security teams to revisit their plans to ensure they can cope with elevated worst-case scenarios. As one CSO put it: 'We have gone back to our scenarios to stress test them. We need to confirm that we have thought about the most realistic worst-case scenario and pushed the boundaries a little more than before.'

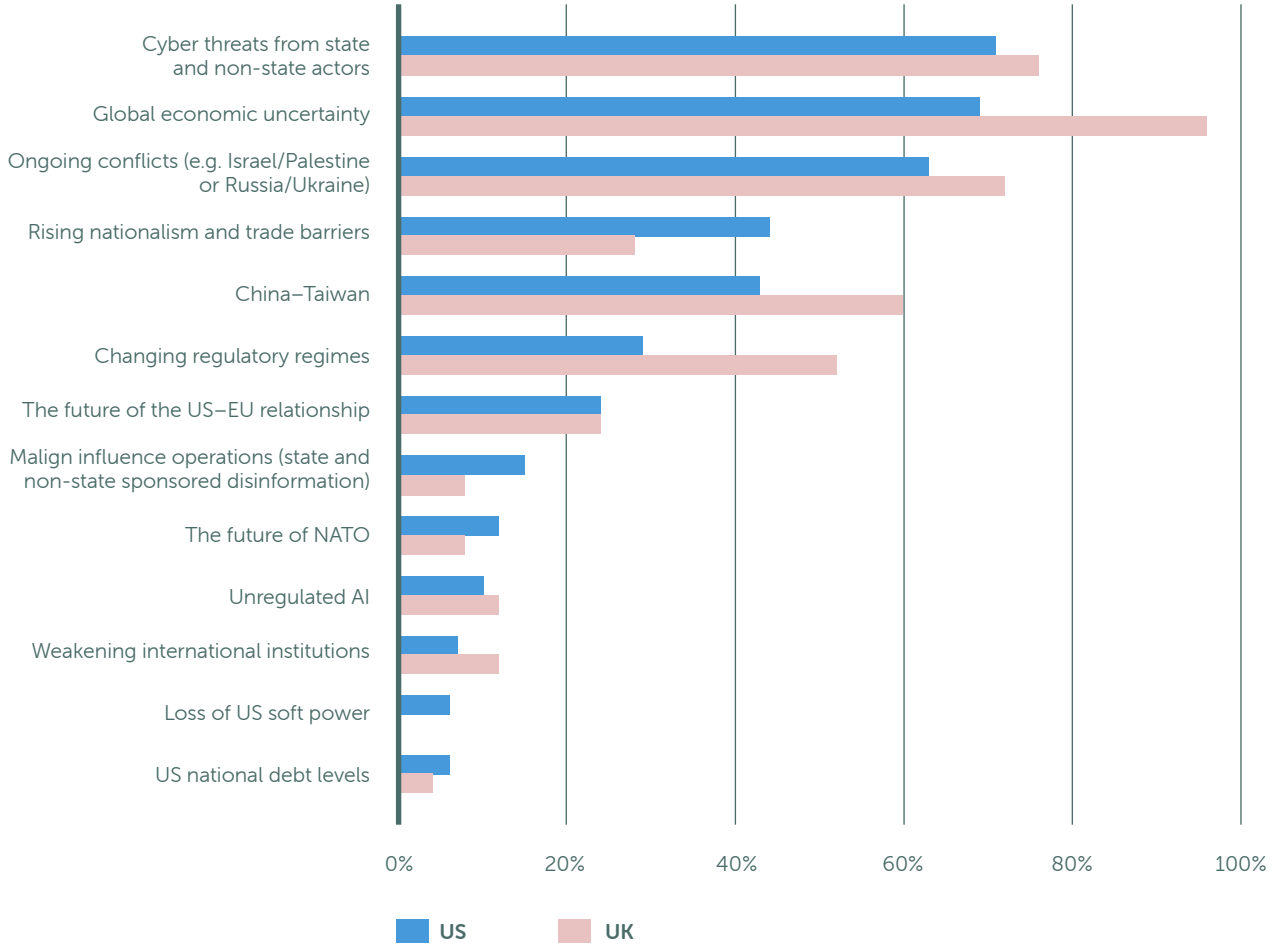
Differences between US and UK CSOs

- **UK CSOs reported a greater intensity of geopolitical risks,** ranking them higher than their US counterparts did across almost all risks (see Figure 4).
- **The geopolitical risks that UK CSOs ranked higher were:** global economic uncertainty (+27%), changing regulatory regimes (+23%), China–Taiwan (+17%), and ongoing conflicts (+9%).
- **US CSOs were more concerned about rising nationalism and trade barriers.**

Figure 4

Top five geopolitical risks to your organisation

US and UK CSOs from MNCs



Corporate security's contribution to geopolitical risk management

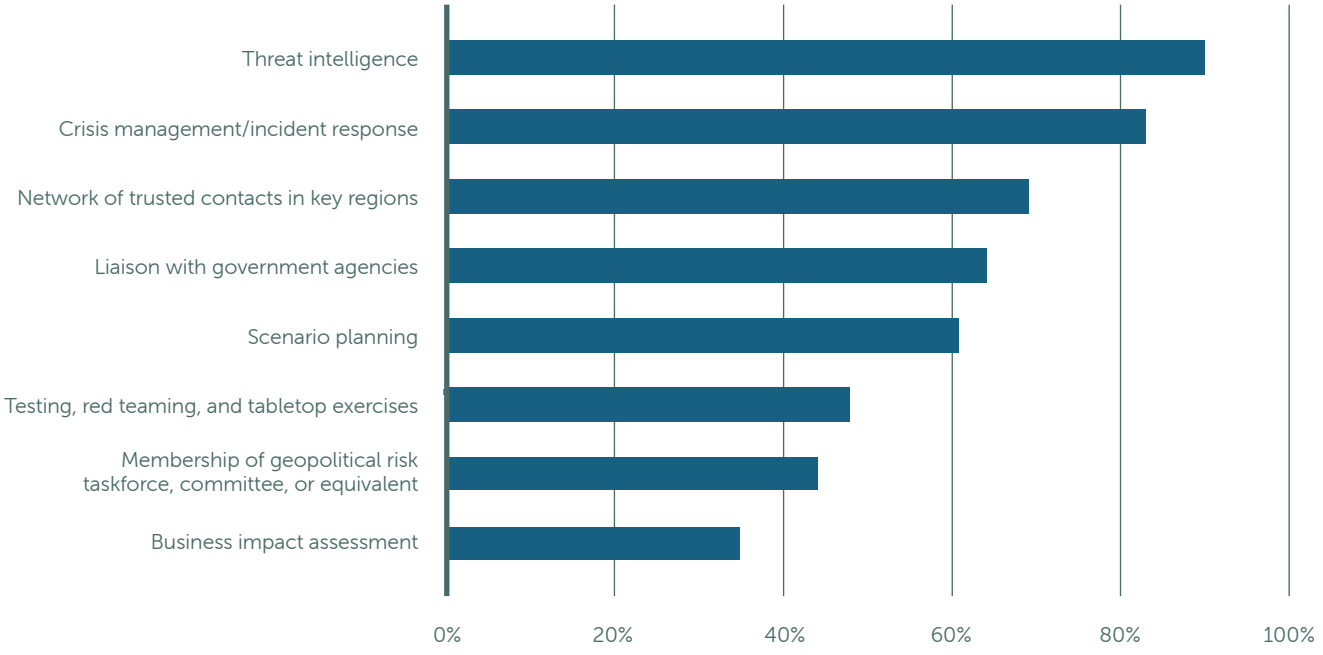
As Figure 5 shows, corporate security teams support responses to geopolitical trends in several ways. These are centred around three capabilities:

- **Insight:** intelligence about threats and trends
- **Response:** crisis management and incident response
- **External connections:** trusted networks and connections with government agencies

As one CSO described his team's role: 'We are clear, [we] act fast and we'll cut across lines of business if we think it needs to be done.'

Figure 5
Corporate security's contribution to geopolitical risk management

CSOs from MNCs



Integration into formal governance structures elevates the role of corporate security

In companies with a structured approach to managing geopolitical risk, such as an enterprise-wide taskforce or committee, corporate security teams are much more likely to play a strategic as well as tactical role in managing the impact of geopolitical risks. For example, they are twice as likely to be involved in scenario planning and red teaming and exercises.

CSOs should advocate for formal rather than ad hoc involvement in such structures. As one CSO told us: 'Most organisations struggle to understand the potential tangible impacts [of geopolitical dynamics] on the business. This is where corporate security can add value, through scenario planning, exercises and red teaming, which can make a significant difference to a company's resilience in the face of geopolitical shifts.'

3. Risks Stemming from Social and Political Polarisation

"The external noise generates a lot more heat and concern, especially with executives, but it's the insider threat I worry about most."

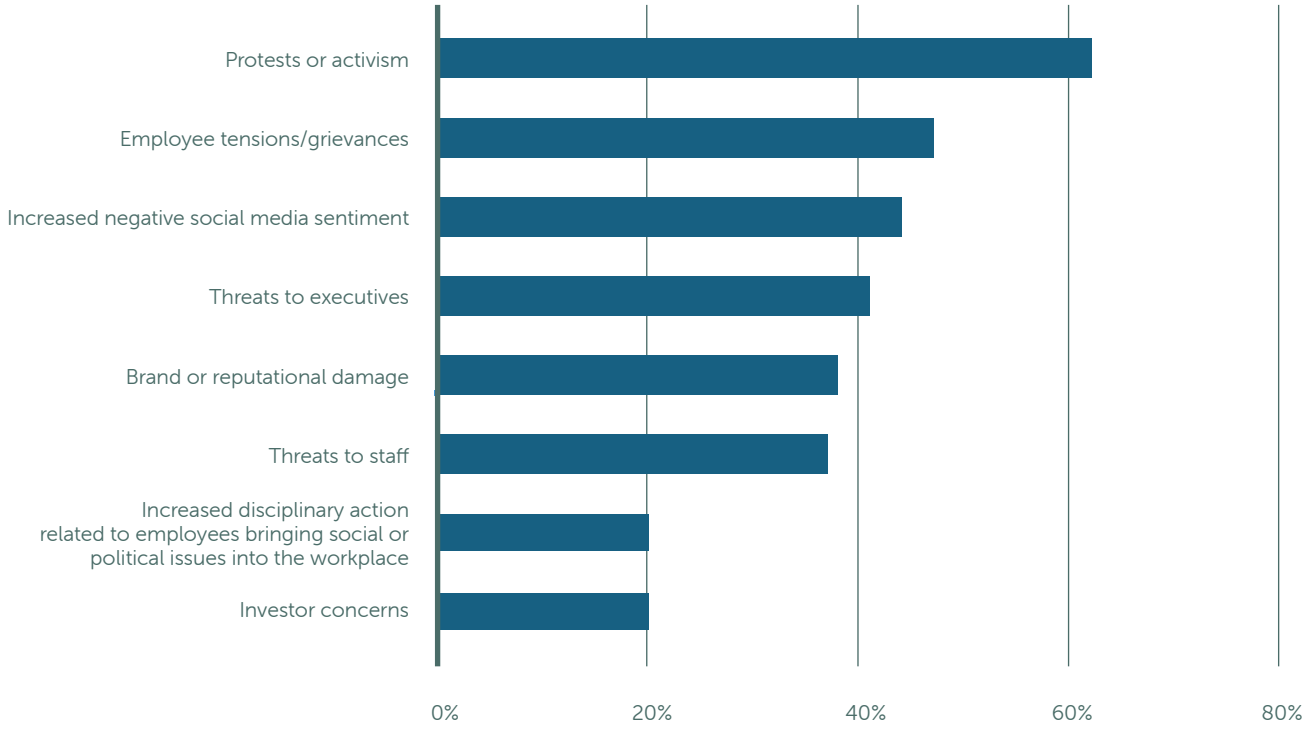
— CSO

Key findings

- **Widespread impact:** 90% of CSOs said their company was impacted by these risks.
- **Activism and protest:** Two-thirds of CSOs (62%) said their company had been affected by this last year, making it the top-rated risk linked to social and political polarisation.
- **External positioning:** 44% of CSOs said their company was impacted by negative social media sentiment and one-third by reputational damage.
- **Corporate security teams make an important contribution to managing these impacts**.
- **Participating in a formal taskforce elevates the contribution of corporate security.**

Figure 6
Impacts of social and political polarisation in last 12 months

CSOs whose companies experienced these impacts



Multinational companies experience a range of security-related impacts stemming from social and political polarisation

The top impact cited in our survey was protest and activism; two-thirds of CSOs said their company had experienced this in the last twelve months (see Figure 6). This chimes with two-fifths of CSOs ranking the risk of activism/protest as either 'critical' or 'high' (see Figure 1). UK CSOs were more concerned than their US counterparts, with 82% of the former experiencing activism or protest against their company in the past year compared to 58% of US CSOs.

58%

of UK CSOs said their company experienced negative social media sentiment in the last 12 months.

External positioning

Companies are increasingly impacted by their external positioning. Almost half of CSOs (44%) said that their company had experienced negative social media, and more than one-third (38%) had suffered reputational damage.

UK CSOs were more exposed to public and online backlash compared to those in the US, with +14% having experienced negative social media sentiment and +8% brand or reputational damage.

These impacts can then translate into security risks, including insider risk and threats to executives. One CSO reflected: 'Companies have become much more attuned to consumer sentiment and pressure from ESG groups. That impacts the kind of intelligence we [corporate security] collect to understand what people are saying about the company and our key people and the direct messages we receive. We then need to decide when things flip to being something we should worry about from a security perspective.'

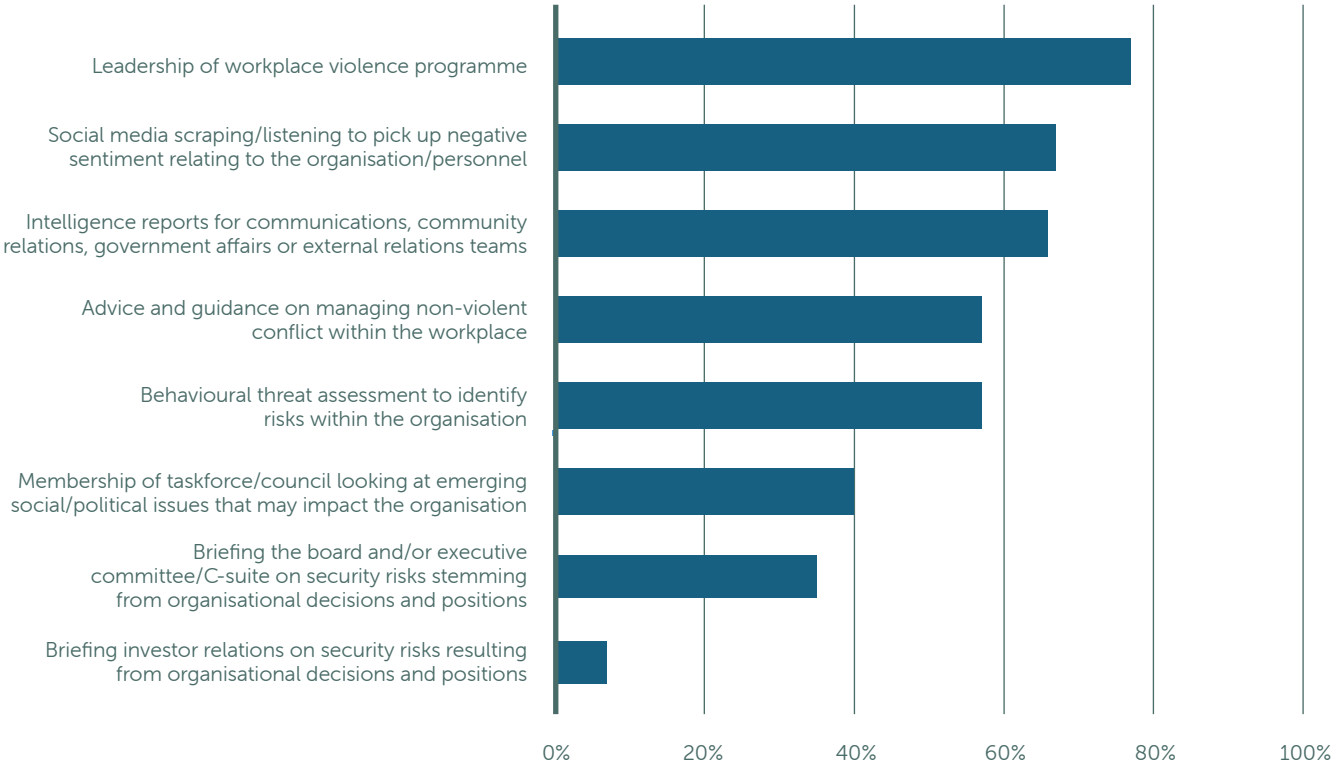
Internal workforce issues

It is getting more common for companies to experience workforce issues related to social and political polarisation. Almost half of CSOs said their company had experienced employee tensions and grievances in the previous twelve months; half said that insider risk was either a 'critical' or 'high' security risk to their company; and one-third ranked workplace violence likewise.

Figure 7

Corporate security's role in managing social and political polarisation risks

CSOs from MNCs



The majority of corporate security teams contribute towards managing these risks in the following ways (see Figure 7):

- **Leadership of workplace violence programmes;**
- **Social media scraping/listening,** to pick up negative sentiments;
- **Intelligence reports** for external facing teams;
- **Guidance on managing non-violent conflict** within the workplace; and
- **Behavioural threat assessment.**

Differences between US and UK CSOs

US CSOs play a more significant role than their UK counterparts in hands-on security execution, day-to-day security operations, and preventing and managing internal threats (see Figure 8). Specifically, US CSOs were more likely to mention the following contributions:

- Carrying out behavioural threat assessment (+30% compared to UK)
- Advising on managing workplace conflict (+15%)
- Delivering workplace violence programmes (+13%)

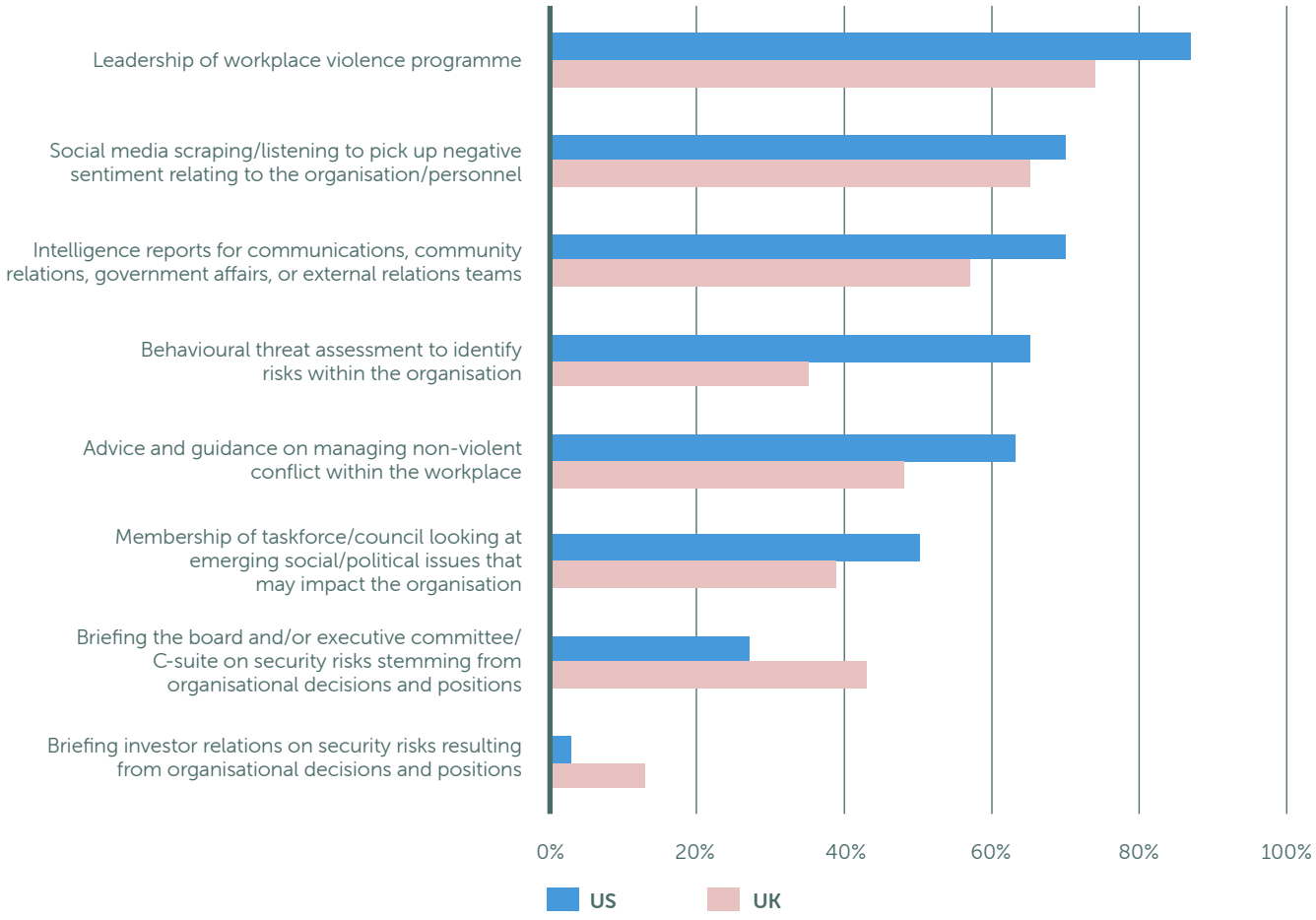
UK CSOs score higher on briefing senior leaders – perhaps due to heightened exposure to activism, protest, negative social media, and brand damage. These CSOs ranked higher than their US counterparts in their contributions to:

- Briefing the board and/or executive committee/ C-suite on security risks stemming from organisational decisions and positions (+16%)
- Briefing investor relations colleagues on security risks resulting from organisational decisions and positions (+10%)

Figure 8

Corporate security's role in managing social and political polarisation risks

US and UK CSOs from MNCs



Managing workforce tensions
Case study

One CSO described to us how he and his team collaborate with HR colleagues and business leaders to monitor and manage tensions in the workplace.

'To get ahead of low-level conflict in the workplace, we work hard on communications and campaigns. We deliver an annual compliance package that reminds staff of our code of conduct and how to use the [employee reporting] hotline. We always see a reporting spike after that's shared. We want to stay top of mind, so we are creative with how we communicate, use campaigns, QR codes, enable different ways to report. We also invest time coaching our HR colleagues on the need to bring us in earlier when there are problems within line management, such as harassment or intimidation. We are the subject matter experts and can support HR in making what can be difficult decisions. They appreciate our partnership.'

Formal integration to governance forums elevates corporate security

When CSOs are members of a formal taskforce managing social and political issues, the contribution of corporate security is both increased and elevated. They are **more likely to be involved in a higher number of activities** linked to managing these risks and their contribution is rebalanced towards **higher-value contributions**. For example, they are **three times more likely to brief the board/executive committee** (55% vs 18%). Formal membership of enterprise-wide committees is a force multiplier for corporate security teams.

Threat management council
Case study

One CSO described the forum his company has established to manage social and political issues impacting the organisation.

- **Cross-functional composition,** including representatives from HR, safety, risk, and security. It does not include business line employees.
- **Focuses on trends** for the previous quarter, hotspots, current and future initiatives.
- **Conducts quarterly reviews** with business lines, including their security-related KPIs, site assessment scores, and number and type of incidents. Quarterly reviews also provide a space to discuss emerging issues.
- **The security team has a stakeholder engagement strategy** for cross-functional and business partners to ensure tailored outreach based on business line needs.

4. Governance

> *"Put yourself in the shoes of the executives you're presenting to. Be ruthless in your focus, mindful of the level of information you're presenting, and build relationships before you enter the room."*
>
> — Jeremy Baumann, Corporate Security Advisors (CSA)

Key findings

- **Strong governance and committee-level reporting:** The majority of CSOs sit at executive committee/C-suite-1, and most report in person at least annually to key risk committees.
- **Reporting to the board is less prevalent:** Only two-in-five CSOs report at least annually to their board of directors.
- **Reporting topics:** Almost all who report to the board or executive committee cover security-related topics and three-quarters report on crisis management. Only one-third brief on business continuity, with a correlation to sector.

- **KPIs:** Most CSOs report KPIs to their company's governance forums, but **fewer than half use indicators that relate to key executive-level concerns**.
- **Low understanding of security among business leaders** is ranked again this year as the top challenge to the effectiveness of corporate security.

CSOs continue to have senior access at the top of their companies

61%

of CSOs sit at C-suite-1.

The majority of CSOs (61%) are located at executive committee/C-suite-1 – a similar proportion to that seen in 2025. Two-thirds (68%) expect their level of seniority to stay the same over the next five years, and one-quarter (26%) think it will increase. In Section 6, on collaboration, we present data that points to a shift from regular to ad hoc partnership working with senior executives – a trend we will watch in 2027.

Board and committee reporting

The majority of CSOs report in person at least annually to the key leadership and risk committees of their company, including the executive committee, internal risk committee, and risk and audit committee or equivalent (see Figure 9). Two-thirds of CSOs expect to make a larger contribution to enterprise risk management in the next five years.

The growing importance of governance reflects the changing nature of risks that organisations face. As cyber threats, geopolitical developments, insider risks, reputational risks, and operational disruption become more interconnected, managing risk

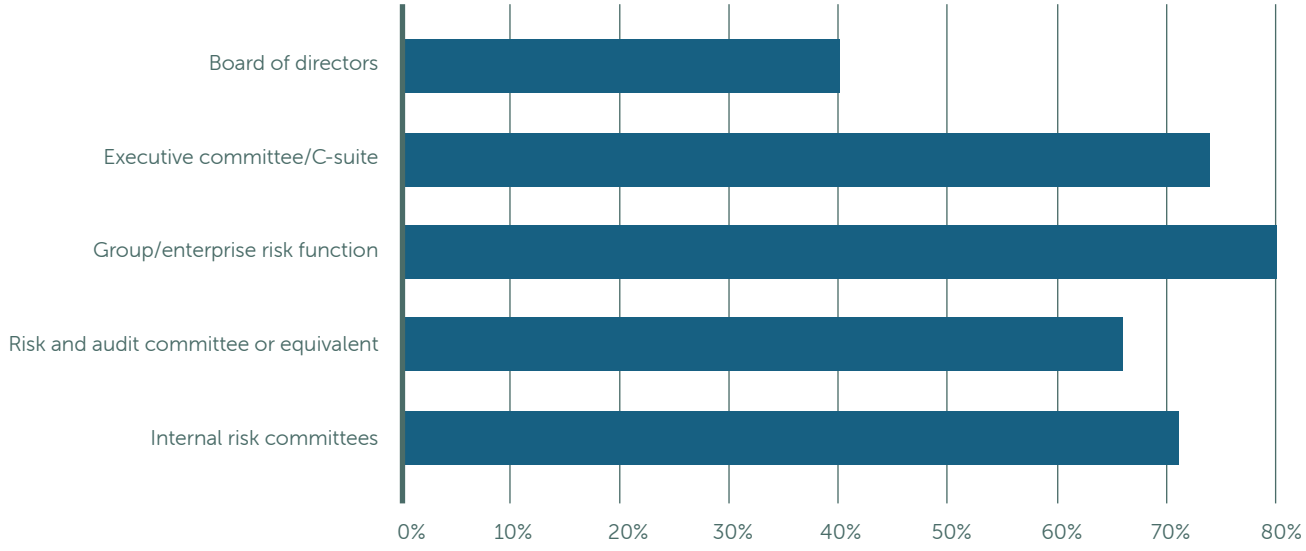
requires decisions that cut across multiple functions and business units. Governance forums provide one of the primary mechanisms through which those trade-offs can be understood and managed at an enterprise level.

The proportion of CSOs reporting to the board is low; only two-in-five CSOs report into the board of directors in person annually (see Figure 9), and US CSOs are significantly less likely to do so than their UK counterparts (33% versus 52%). The respective vertical reporting positions of US and UK CSOs are very similar to one another, meaning this difference cannot be explained by level of seniority or proximity to the board.

Figure 9

CSO reports (in person, at least once per year)

CSOs from MNCs



Topics for board and executive committee/ C-suite reporting

The issues increasingly reaching boards are rarely standalone security problems. Rather, they are interconnected business challenges that combine elements of cyber security, geopolitics, resilience, reputation, workforce risk, and operational continuity. This makes it **more important than ever that CSOs have the ability to communicate risk in business terms** rather than security language.

We asked CSOs whether they present on security, crisis management, and/or business continuity (see Figure 10):

- **Security:** Of those CSOs that report to the board or executive committee, almost all (97%) present on security.
- **Crisis management:** Three-quarters of CSOs report on crisis management, with UK CSOs more likely to do so than their US counterparts (80% versus 65%). This higher reporting rate in the UK might reflect increased concern about geopolitical risks, including conflict.

Reporting on business continuity is lower and varies by sector

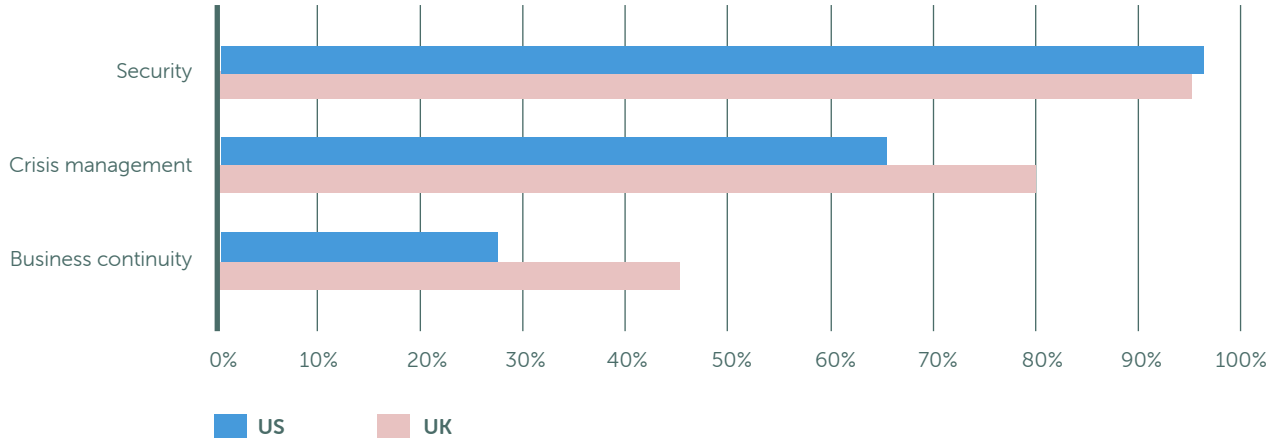
Only one-third of CSOs report to the board or executive committee on business continuity, with UK CSOs again more likely to do so compared to those in the US (45% versus 27%; see Figure 10). **Reporting on business continuity was not correlated with corporate security having primary accountability for this area, but the results do show a connection to sector.**

CSOs in the professional services and media, aerospace and defence, and energy and utilities are all more likely to report to their board or executive committee on business continuity (more than 50%), compared to their counterparts in banking and financial services, healthcare, or technology and digital (ranging from 0–20%).

Figure 10

Reporting topics to board and executive committee

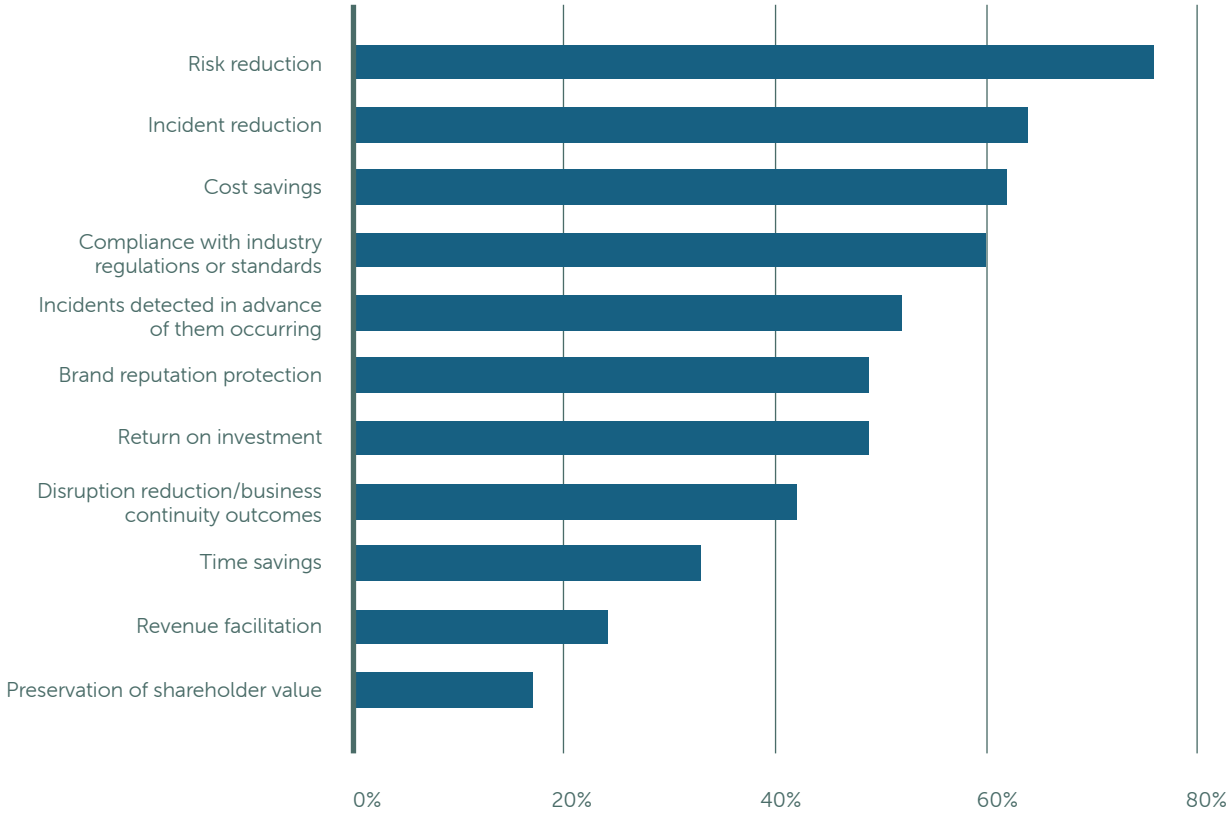
US and UK CSOs from MNCs



Use of KPIs

Two-thirds of CSOs use key performance indicators (KPIs) when reporting to the governance bodies mentioned above. The majority report risk reduction, incident reduction, cost savings, compliance with industry regulations and standards, and incidents detected in advance of their occurring (see Figure 11).

Figure 11
KPIs used by corporate security
CSOs from MNCs



CSOs are much less likely to use KPIs that relate to executive-level concerns, such as preservation of shareholder value, revenue facilitation, business disruption and business continuity outcomes, return on investment, or brand reputation protection. This is likely to become more important as risks are increasingly interconnected. Senior leaders are often less interested in security activities than in understanding how multiple risk factors affect business continuity resilience, growth, and organisational performance. It is the job of CSOs

to do that translation. As Jeremy Baumann, CEO of Corporate Security Advisors, put it, 'You need to understand your business and your executives and what matters to them personally. Then tailor your data for maximum impact.'

Metrics versus KPIs

> *You need to understand your business and your executives and what matters to them personally.*
>
> — Jeremy Baumann, CSA

Anecdotally, we know that some CSOs conflate metrics and KPIs, referring to data such as the number of incidents, investigations, visitors, or GSOC responses as KPIs. These measures of activity can be useful in calculating workload and identifying some trends, but they are not KPIs. As one CSO put it during a recent Clarity Factory webinar, 'All KPIs are metrics, but not all metrics are KPIs. KPIs are the critical sort of subset of metrics, which indicate whether you're achieving a specific objective. They must be tied to an objective, have a clear target, an owner, and a defined cadence for measurement and review.'

Presenting to the board and risk committees

For the second year running, **CSOs cited 'low understanding of security among business leaders' as the top challenge** to the effectiveness of corporate security (**ranked joint top this year alongside 'data and organisational silos'**). Presenting at board and executive or risk committee level offers an opportunity to level set understanding and demonstrate that security is aligned with and sensitive to business realities.

The content of presentations will vary, of course, but the following principles are applicable to any senior setting:

- **Know your audience:** Ensure you understand the audience you are presenting to and build relationships before you need them.
- **Focus and discipline:** Tailor your content to what the audience needs to know, not everything you know. For example, one CSO we spoke to suggested that: 'If it's a commercial leader, you might focus on risk and value, whereas for operations it might be business continuity or a governance focus for an assurance function.'
- **Make the ask appropriate:** Be mindful of the level of decisions in front business leaders and pitch accordingly. As Jeremy Baumann pointed out, 'CSOs must be careful about what they take to their executives. If you go to them with a $50,000 problem, they might be polite or they might be direct, but they probably won't invite you back.'

5. Accountability

"Our job is to come up with security solutions to business problems."

— Bill Tenney, ASIS International

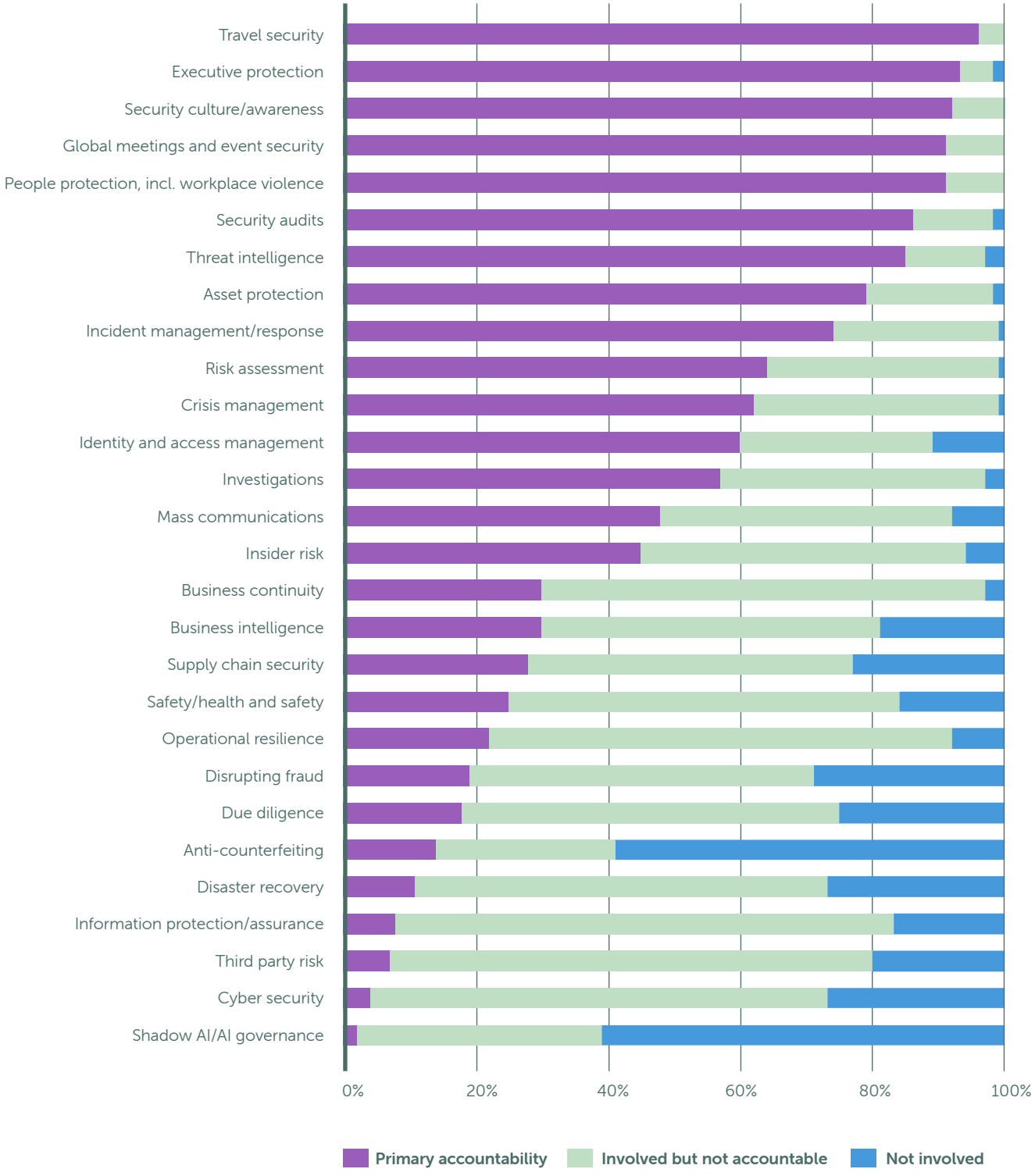
Key findings

- **Core areas of accountability** remain unchanged from 2025.
- **Identity access management** saw the largest growth as an area of primary accountability for CSOs in 2026.
- **The role of corporate security teams in business continuity, supply chain, and third-party risk is shifting** from one of primary accountability to involvement alongside other business partners.
- **A new design principle may be emerging,** placing ownership with the most specialist function and execution with the most coordinated one. Corporate security teams with well-developed partnership capabilities can provide critical enterprise-wide integration capability.

Figure 12

Areas of accountability

CSOs from MNCs



More than half (58%) of all CSOs we surveyed anticipate growing accountability over the next five years, but this view was more prevalent among US CSOs than those in the UK (62% versus 48%). Our data suggests a consolidation of accountability around the areas shown in Box 1, with growth most likely to occur through enterprise-wide involvement rather than functional ownership.

The areas experiencing the highest levels of uplift in terms of primary accountability between 2025 and 2026 were generally within this core group:

- **Global meetings & event security (+7%),** likely due to heightened geopolitical and reputational risks and threats to executives impacting risk at corporate events.
- **Incident management/response (+6%),** likely due to the increased frequency of multi-domain incidents and demand for a coordinated response.
- **People protection (including workplace violence) (+5%),** likely due to rising concerns about workplace violence and threats to executives and staff.
- **Identity and access management (+14%):** outside the core group, but experiencing the largest growth in primary accountability. This could be due to the blurring of physical–digital boundaries, gaps in ownership for physical/hybrid environments, or a convergence of physical access and workplace safety.

Box 1

Areas of accountability

The core areas of accountability for corporate security teams remain unchanged from 2025. As shown in Figure 12, the majority of CSOs are accountable for:

- Travel security
- Executive protection
- Security culture/ awareness
- Global meetings and event security
- People protection, including workplace violence
- Security audits
- Threat intelligence
- Asset protection
- Incident management/ response
- Risk assessment
- Crisis management
- Identity and access management
- Investigations

From risk owner to enterprise operator and integrator

Our data suggests companies are becoming more likely to place risk ownership in the most specialised function, impacting the role of corporate security.

- **Corporate security teams have shifted from holding primary accountability for business continuity to being 'involved, but not accountable',** with primary accountability falling from 43% in 2025 to 30% in 2026. We found anecdotal evidence of it shifting to the COO organisation or closer to business processes.
- There is a similar trend of **shifting accountability for third-party risk,** potentially due to the formalisation of enterprise risk ownership.

- Likewise, **fewer CSOs in 2026 have primary accountability for supply chain security,** and more said they were not involved in this area at all – potentially as companies embed risk in commercial operations.

Rather than reducing corporate security's role, this shift appears to be accompanied by increased collaboration with operational risk functions. The message seems to be less 'stay in your lane' and more 'specialise and connect'.

6. Collaboration with Business Partners

"Collaboration is not the future – it's today. Given the risks their companies face, enterprise integration is where corporate security teams can make a significant contribution."

— Bill Tenney, ASIS International

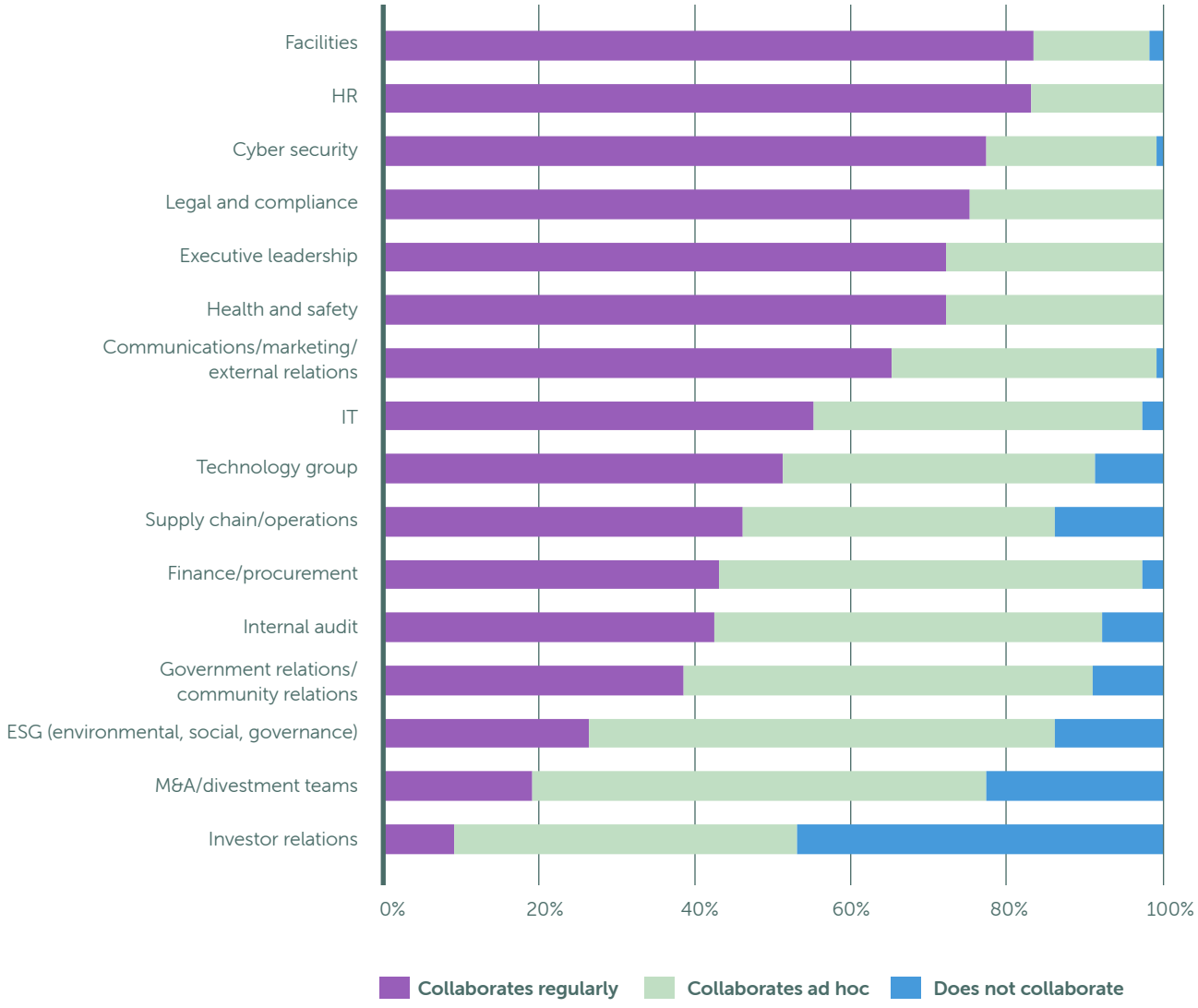
Key findings

- **Overall levels of collaboration have increased** since 2025, and CSOs agree that organisational silos negatively impact effectiveness.
- **Corporate security teams enjoy stronger collaborations with operational risk partners,** including technology, HR, and cyber security teams.
- **Collaborations are becoming more ad hoc with governance partners,** including executive leadership, IT, finance, and internal audit teams.
- **Cyber security partnership remains critical and is growing,** but there is scope for enhanced contribution.

Figure 13

Areas of collaboration

CSOs from MNCs



Box 2

Top five collaborators for corporate security

Top collaborators 2026

1. Facilities
2. HR
3. Cyber security
4. Legal and compliance

= 5. Executive leadership

= 5. Health and safety

Top collaborators 2025

1. Facilities
2. Executive leadership
3. Legal and compliance
4. HR
5. Cyber security

Trends in collaboration

Corporate security teams are responding to changing needs, triggered by an interconnected risk environment that requires coordinated responses.

- **Increased collaboration:** There has been an overall increase in collaboration in 2026, and three-quarters of CSOs anticipate this will grow even further in the next five years. This year, CSOs also agree more strongly with the statement 'Corporate/physical security's ability to protect my organisation's people, assets and reputation is negatively impacted by organisational silos and fragmented data'.

- **Heightened collaboration with operational risk partners:** Corporate security teams are strengthening ties with operational risk partners, shifting from ad hoc to regular collaboration with

the technology group, HR, and cyber security (see Figure 13). Almost two-thirds of CSOs said they expect the corporate security team to make a larger contribution to enterprise risk management over the next five years.

- **More ad-hoc collaboration with governance partners:** CSOs are now engaging more in ad hoc, rather than regular, collaboration with governance partners, including IT, finance/procurement, legal/compliance, and internal audit teams. This could be further evidence of the trend to consolidate approaches to enterprise risk management.

- **Less regular collaboration with executive leadership:** There was a notable 9% drop in the proportion of CSOs who said they collaborate regularly with executive leadership, with a shift from regular to ad hoc collaboration.

Partnership with cyber security is growing

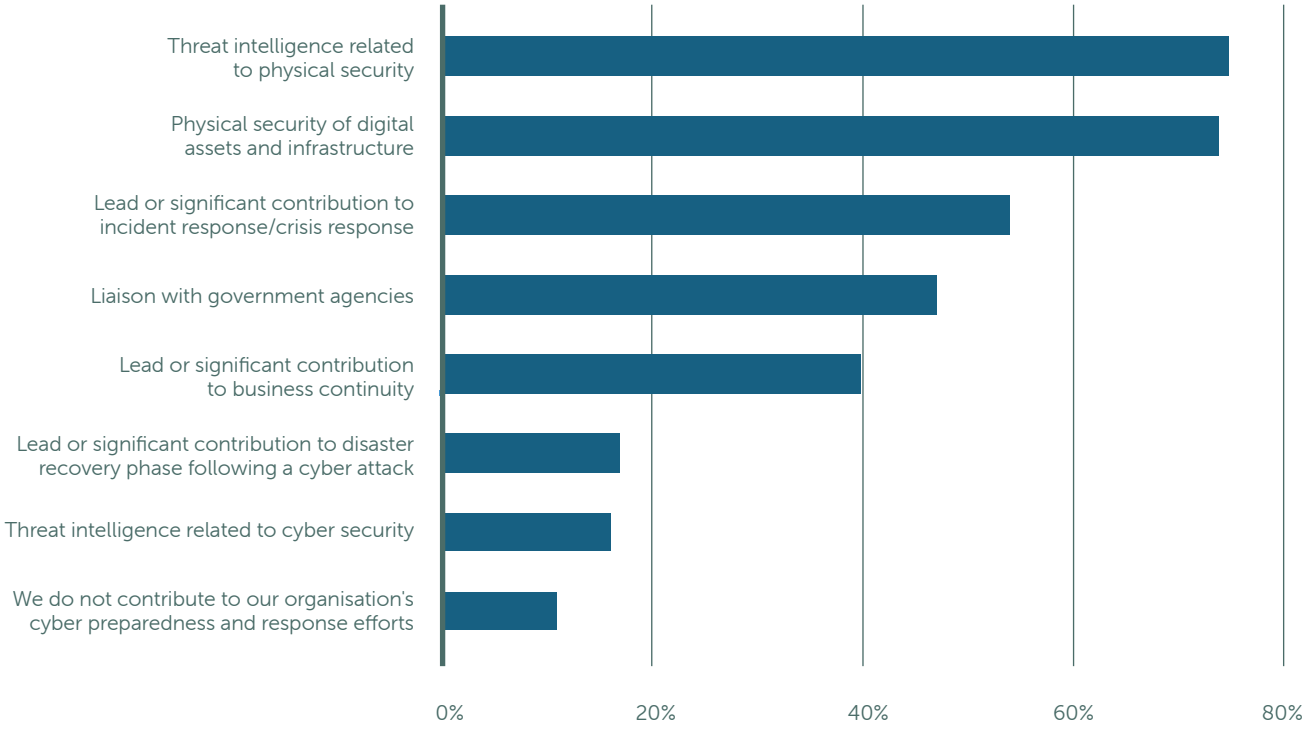
Three-quarters of CSOs said their team regularly collaborates with cyber security (see Figure 13). This is slightly up from 2025 (77% vs 73%), with more than half of CSOs expecting collaboration with cyber security to grow even further in the next five years.

Partnership is non-negotiable. As one senior security leader told us: 'One of the most significant changes I've seen in the last 5–6 years is the fact that our adversaries now work across all threat vectors, taking a multispectral approach to disruption. In this threat environment, you cannot afford to have gaps between your physical and cyber security capabilities.'

Figure 14

Corporate security's role in preparation for and mitigation of cyber attacks

CSOs from MNCs



We came across examples of governance structures that oversee the relationship between corporate security and cyber security. For example, one CSO described their Strategic Security Risks Council, a joint physical–cyber security initiative. Leadership from corporate and cyber security meet to review the threat picture and discuss priorities and areas of collaboration. The forum provides structured governance for partnership activities. Figure 14 highlights the various ways that corporate security teams play a role in preparing for and mitigating the risk of cyber attacks.

Cyber resilience programme Case study

A CSO told us about his company's cyber resilience programme. The initiative has three strands – defence, resilience, and recovery – with the corporate security team leading on resilience.

The team has established the company's critical processes and minimal viable operations and documented ways to make business processes resilient.

A Vice President of Resilience on the security team supports the business to understand its critical processes and create a cyber continuity plan.

As the CSO explained, executives want the programme to move at pace, but business unit leads often slow progress because they often don't understand their own critical pathways, see business continuity as someone else's job, and are reluctant to allocate the necessary resources.

He commented, 'Most people understand the cyber risk, but struggle to commit to making it a priority in their own area of the business. Once we have run an exercise with them, though, that changes. The risk becomes real and we immediately get traction.'

7. Use of Technology and AI in Corporate Security

"AI is going to revolutionise how we administer security. Technology has finally caught up with the needs of security."

— CSO

Key findings

- **The majority of CSOs are increasing the proportion of their budget dedicated to technology;** core investment areas include AI/automation/analytics, physical security technology, integration platforms, and intelligence and data platforms.
- AI adoption **has increased across all areas,** with particularly sizeable growth in the fields of travel risk management, risk and security assessments, and incident management and response.
- **AI maturity** remains at a basic level for most CSOs, but our data suggests corporate security teams are beginning to move through three maturity tiers.
- **As AI adoption grows, the barriers are less about technology implementation and more about organisational transformation.**

Technology transformation is underway

70%

of CSOs expect technology spending to increase over the next 2–3 years

CSOs are increasing the share of their budget dedicated to technology, and the majority (70%) expect this proportion to grow over the next 2–3 years.

CSOs are prioritising technology spending in core and emerging areas (see Box 3). These technology-focused investments also support a broader thrust towards enabling corporate security to act as an enterprise integrator. Many of the technologies are designed to connect previously fragmented data, systems, and teams, enabling more coordinated responses to increasingly interconnected risks.

Box 3

Core and emerging areas of technology investment

Core investment areas

- **AI/automation/analytics:** process automation, decision support, and detection and analytics
- **Physical security technology modernisation:** our data suggests a large-scale cap-ex refresh cycle is underway
- **Integration platforms:** push for consolidation due to fragmented tools and overlapping systems
- **Intelligence and data platforms:** OSINT and data analytics tools, and intelligence platforms

Emerging areas

- **GSOC transformation:** from monitoring to analytics and coordination hubs
- **Identity, access, and digital credentials:** upgrading systems (links to increased corporate security accountability for identity access management)
- **Crisis/resilience technology:** mass communications, crisis platforms, and business continuity/disaster recovery systems

Increased AI adoption

AI adoption has increased across all areas of corporate security in the past year (see Figure 15). More than 90% of CSOs said their team uses AI and their company's internal AI tool or system, and that they expect their team's use of AI to increase in the next five years.

However, it should be noted that our dataset is likely to skew positive on AI adoption. We limit participation to CSOs from multinational corporations with more than 3,000 employees, and CSOs opting to take part in a survey of this kind are likely to be more focused on innovation compared to the general CSO population.

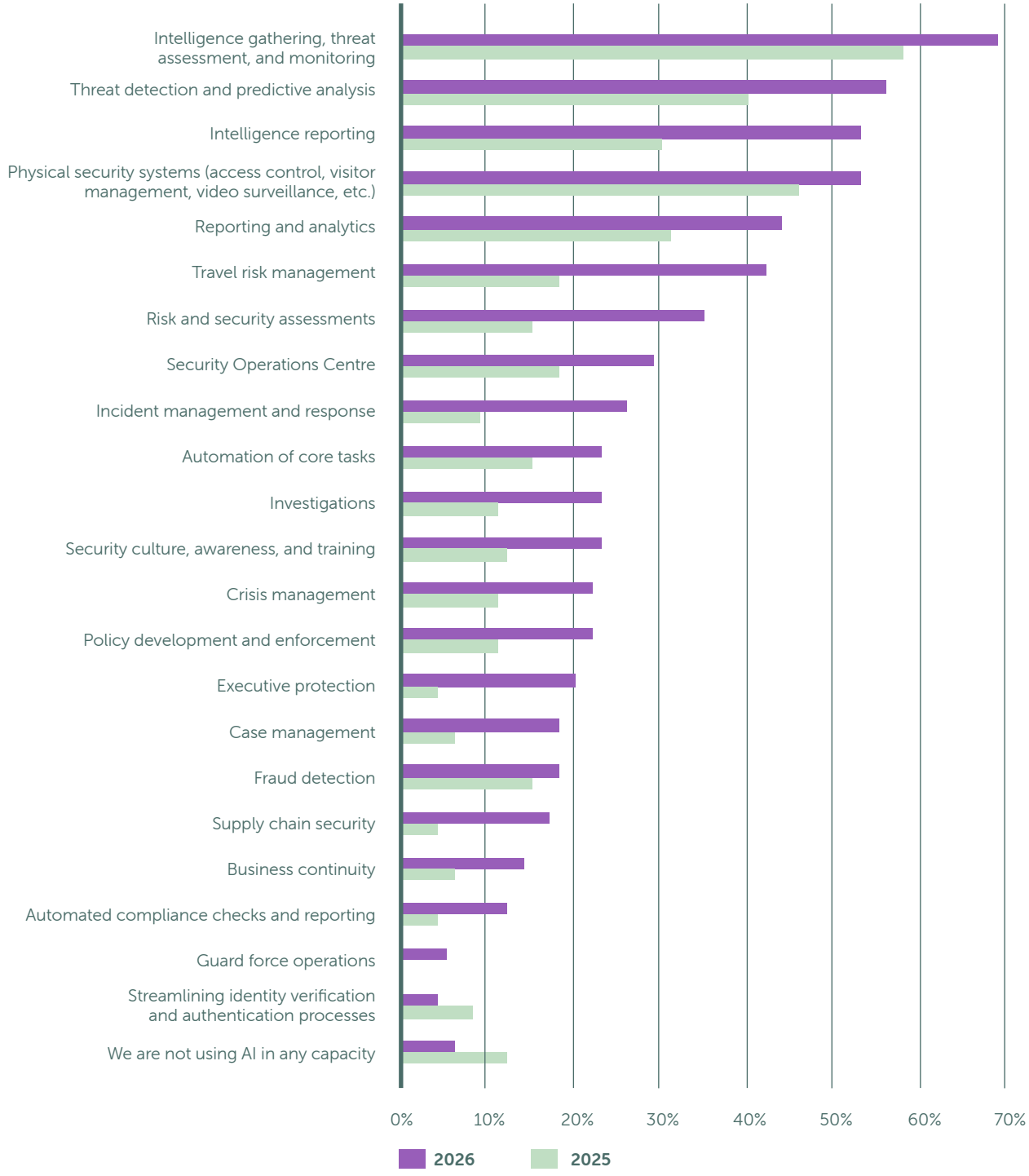
Top five applications of AI

1. Intelligence gathering/threat monitoring
2. Threat detection & predictive analysis
3. Intelligence reporting
4. Physical security systems
5. Reporting & analytics

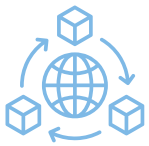
Figure 15

Applications of AI (2026 vs 2025)

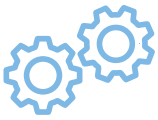
CSOs from MNCs



Our data shows that patterns of AI use are beginning to change:



AI is now present across the full security lifecycle: Prevention, preparedness, detection, response, and recovery, and our data shows that the level of value a team derives from AI (see Figure 16) corresponds to the number of areas where it is applied.



From intelligence to operational purposes – from understanding risk to managing and responding to risk: While intelligence-related use cases still dominate, AI is increasingly being used in incident response, investigations, crisis management, and case management.

From reporting to decision enabling: AI is starting to help corporate security teams make decisions, through increased application in reporting and analytics, and risk assessments. It can also help corporate security step into the role of an enterprise integrator by connecting business-wide information and translating it into insights for decision makers.

Increasing use in frontline activities: including executive protection, travel risk, and guard force operations.

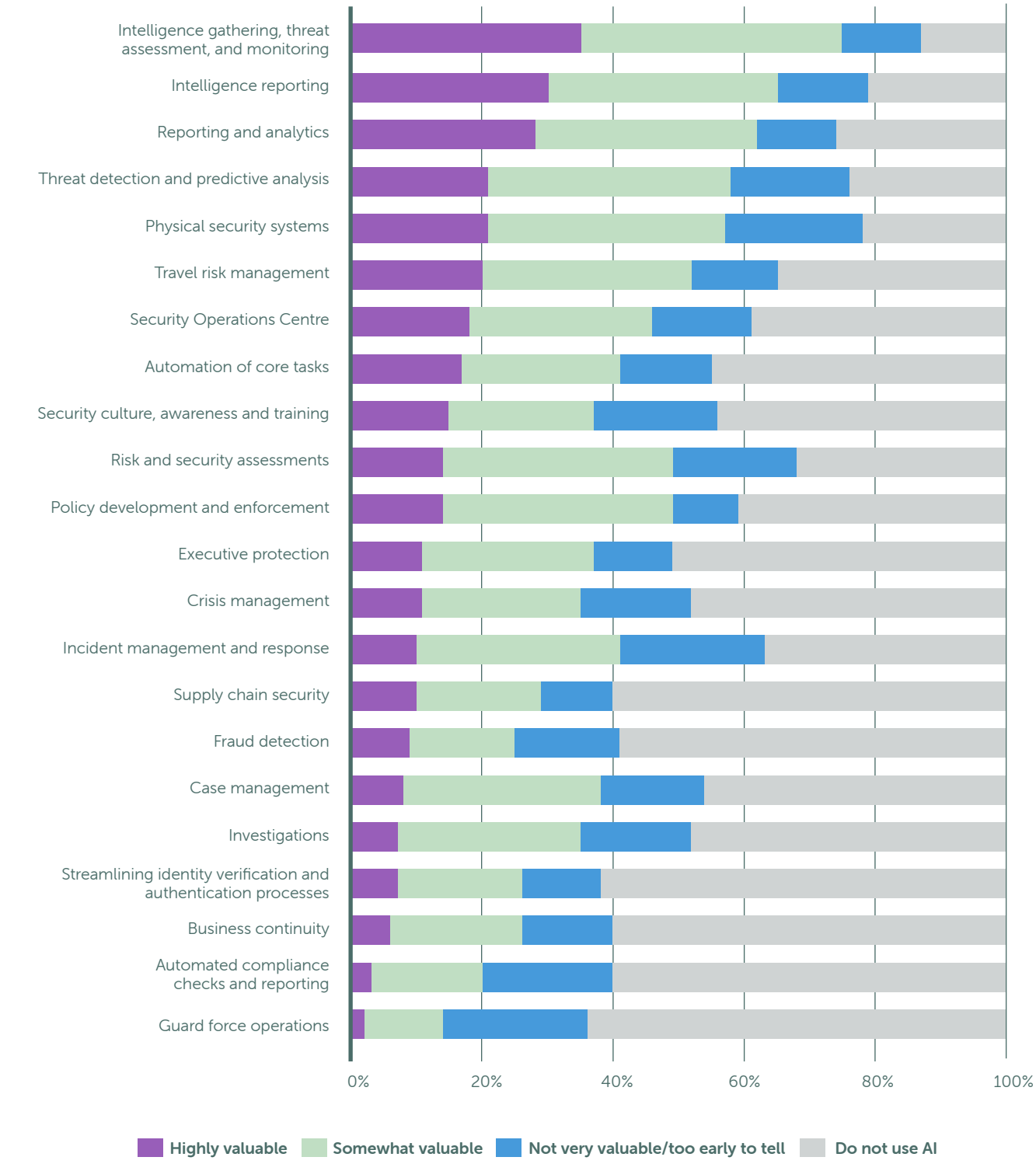
Expansion into governance and compliance: CSOs are increasingly using AI in security and risk assessments, policy development, and compliance automation.

Significant growth in AI adoption in certain areas: Since 2025, the largest expansions of AI use have been in travel risk management, intelligence reporting, risk and security assessments, and incident management and response.

Figure 16

Perceived value of AI, by area of application

CSOs from MNCs



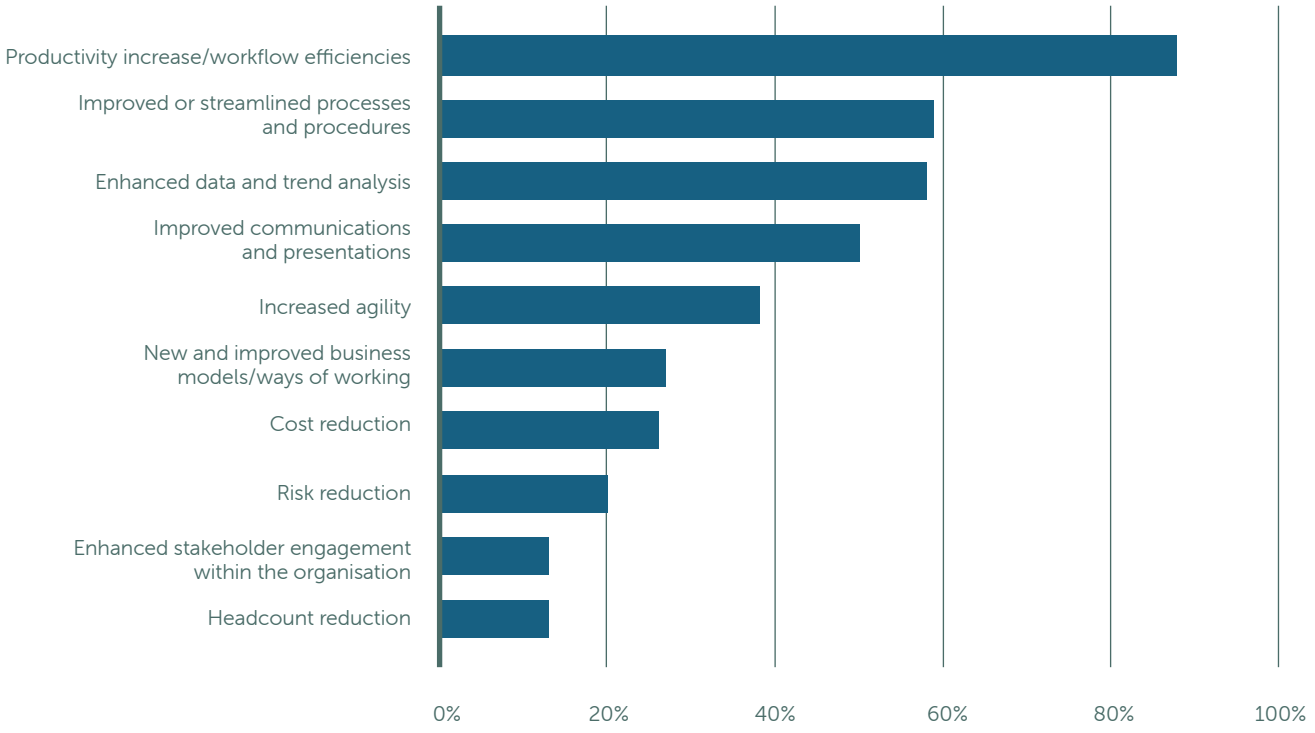
Benefits of AI adoption

88%

of CSOs say AI use has led to increased productivity and workflow efficiencies.

CSOs derive a range of benefits from AI adoption, with the **majority citing increased productivity, more streamlined processes and procedures, and enhanced data and trend analysis** (see Figure 17). There is a very strong relationship between the level of a corporate security team's AI usage and the benefits they report deriving from that use. High AI users report experiencing more than three times as many benefits as low users.

Figure 17
Benefits of AI use
CSOs from MNCs



Corporate security AI maturity model

Corporate security teams fall into three tiers of AI maturity (see Box 4). The vast majority are at tier one, with the large 'do not use AI' segments (see Figure 15), showing that adoption remains low in many areas. A growing number of CSOs are at tier two using AI to become more insight-driven. A tiny minority are moving into the most mature category.

Box 4

Corporate security AI maturity model

Tier 1: Efficiency-led adopters (large majority)

Focus: productivity, process improvement
Use cases: intelligence, reporting, analytics
Outcome: faster delivery, lower effort

Tier 2: Insight-driven organisations (small but growing group)

Focus: analytics, decision support, agility
Use cases: above, plus risk assessment, travel risk management, incident response, operational decision support, enhanced GSOCs
Outcome: better decisions, improved responsiveness

Tier 3: Transformational leaders (tiny minority)

Focus: new operating models, new value creation
Use cases: above, plus physical execution, compliance automation, workforce-heavy domains
Outcome: competitive differentiation

AI use cases

During interviews, CSOs shared AI use cases:

Reporting, analytics, and decision support

There is a notable shift taking place from AI-assisted reporting to AI-enabled decision support. The following case study demonstrates how AI can strengthen corporate security's role as an enterprise-wide connector – bringing together information from multiple functions to generate insights that no single team could generate independently.

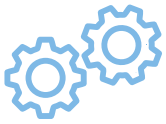
Site health dashboard Case study

One CSO has created a site health dashboard to collate leading indicators at site level.

Data include legal cases and litigation; equality charges and demand letters; reporting on safety incidents and near misses; ethics and compliance investigations; cases of workplace violence, theft, or code of conduct violations; employee tenure and turnover averages; data on employee engagement; and morale survey results.

The team uses AI to analyse this data and deliver insights to help the security team and local management get ahead of any problems. CSO told us: 'AI is the first tool we've developed to help us think better. We've had other tools that help us to work faster, but this is making our decisions better.'

Operational security and service delivery



AI is increasingly being applied to frontline security activities and operational workflows. Examples shared by interviewees include:

- **An AI travel assistance agent**, providing travellers with immediate access to information on risk levels at their destination.
- An **AI agent to manage out-of-hours office access requests**.
- **An AI avatar to deliver security briefings**, enabling the team to meet growing demand against a backdrop of declining resources.

Risk, resilience, and enterprise-level decision making

More advanced users are beginning to **integrate security data with broader enterprise data, using AI as a mechanism to connect security, operational, and commercial information to support enterprise-wide decision making**. For example, one CSO we interviewed is exploring how corporate security, supply chain security, and operations can bring their respective data together into a shared data lake to improve supply chain planning, distribution, and security.

This example reflects another emerging shift visible in the survey results: corporate security is creating value through integration of information, insight, and decision support rather than direct ownership and responsibility.

Facilitating corporate security integration and collaboration

Several interviewees described how **AI is helping corporate security to strengthen its capacity for collaboration**. One CSO gave the example of being able to: '... use AI on calls to decipher documents and understand technical terms, which enables me to contribute and add value. Without AI, I would struggle to contribute [in] real time.'

Compliance, governance, and data protection

New use cases for AI are emerging in risk assessments, policy development, and compliance automation. One CSO described how his team is starting to use AI to help tackle data exfiltration – AI can spot and block high levels of confidential information leaving the servers, filter at scale, and either block it or flag it very quickly.

Challenges with AI

As AI use matures within companies, the barriers to progress are becoming less about the technology itself and more about organisational transformation. Challenges mentioned by CSOs we interviewed include:

- **Data quality and readiness:** Many security teams work with patchy datasets, which must first be cleaned and rationalised. As Manish Mehta from Ontic put it: 'Clean data is at the very core of getting AI right. Garbage in, landfill out.'
- **Disjointed data:** Even where data exists, it often sits across multiple disconnected platforms. The challenge is therefore not just about implementing AI technologies, but about enabling information sharing.
- **Executive trust and confidence:** Corporate security information often informs high-stakes decisions, and many CSOs worry that executives won't trust AI-generated data.
- **AI skills gap:** Many corporate security teams are still at the beginning of their AI journey and are building both technical capability and user confidence. While some organisations are recruiting specialists, most rely on upskilling existing team members.

> *Clean data is at the very core of getting AI right. Garbage in, landfill out.*
>
> — Manish Mehta, Ontic

- **Understanding the true value of AI:** Corporate security teams often struggle to recognise the difference between efficiency gains and transformational value. Manish Mehta of Ontic explains: 'Most CSOs are envisioning AI in terms of generative AI, which amounts to synthesising and analysing information. When I think about AI as a technologist, this is a limiting view of what's possible. If CSOs don't understand the true potential, they will see huge value where I see much less.'
- **Keeping pace with rapid technological change:** Many CSOs struggle with the challenge of making investments and operating decisions in an environment where AI capabilities are evolving at pace.
- **Governance, ethics, and company restrictions:** Some companies are limiting staff use of AI for security, cost, or ethical reasons, and some security use cases conflict with ethical or privacy concerns.
- **Human oversight and accountability:** CSOs are still learning to determine where AI should support decisions and where decisions should remain firmly under human control.

8. Intelligence

"The role of my corporate security function is now less about managing incidents and more about enabling the business to navigate uncertainty with confidence. Intelligence is critical."

— CSO

Key findings

- **Intelligence** has the potential to be a principal mechanism through which the function **generates enterprise-wide value**.
- **The audience for corporate security intelligence has grown**, notably among business leaders.
- **Audience growth has not been matched by influence** – there is an impact gap, with only 25% of CSOs saying their intelligence frequently influences business decisions.
- **To realise their potential, corporate security intelligence teams must overcome several challenges.**
- **CSOs must build the intelligence team of the future,** with an emphasis on business curiosity, communication, and adaptability.

Intelligence is a key mechanism through which corporate security can create enterprise value

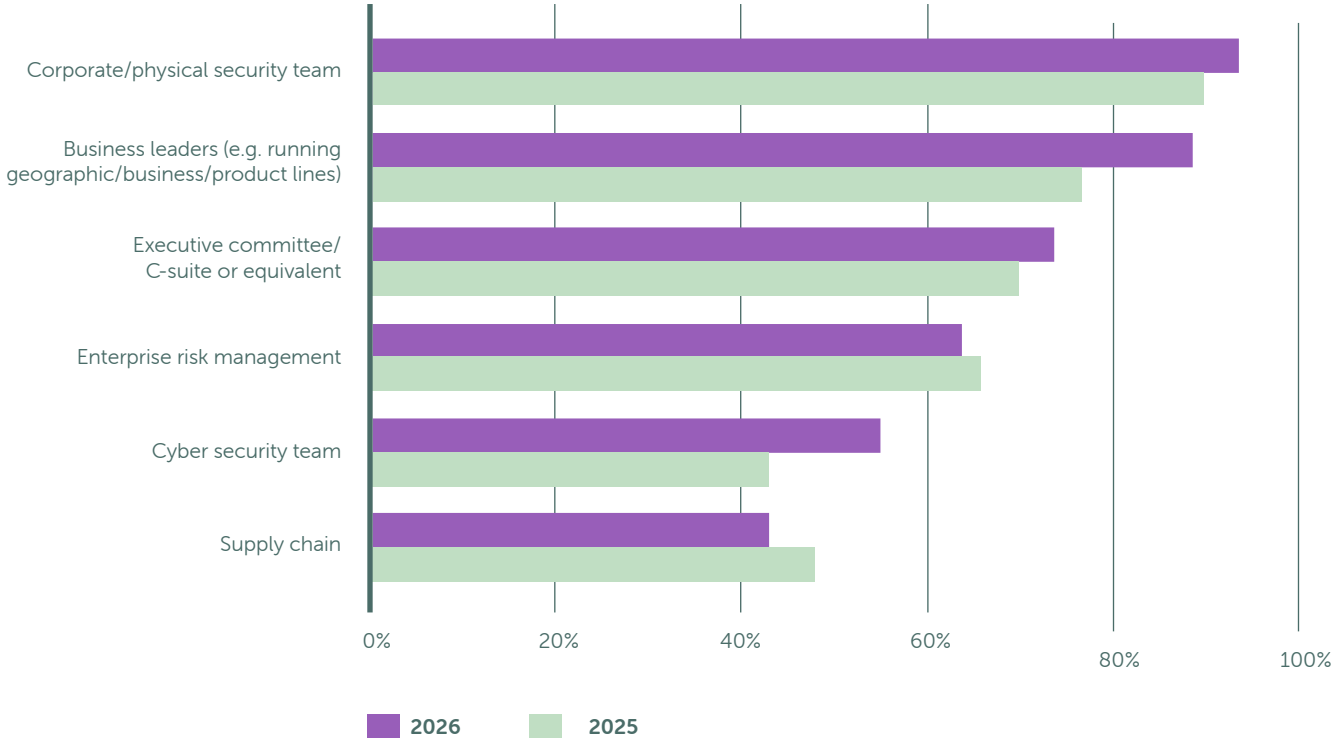
The changes in the risk environment that we have described mean that organisations increasingly need the capability to identify relationships, assess implications, and support decisions across multiple business domains. In this context, intelligence should be one of the key assets corporate security can offer the company.

> *First you serve the corporate security team, but over time you ask yourself how your intelligence and geopolitical insights could serve the broader company.*
>
> — Bill Tenney, ASIS International

The audience for corporate security intelligence has grown since 2025 – most notably among business leaders and cyber security teams, which are now served by 12% more CSOs than in 2025 (see Figure 18). While the corporate security team remains the principal audience for intelligence output, it is promising to see a shift towards a broader audience. As Bill Tenney said: 'There is often an evolution in corporate security intelligence. First, you serve the corporate security team, but over time you ask yourself how your intelligence and geopolitical insights could serve the broader company.'

Figure 18
End users of corporate security intelligence (2026 vs 2025)

CSOs from MNCs



25%

of CSOs said their intelligence products frequently influence business decisions.

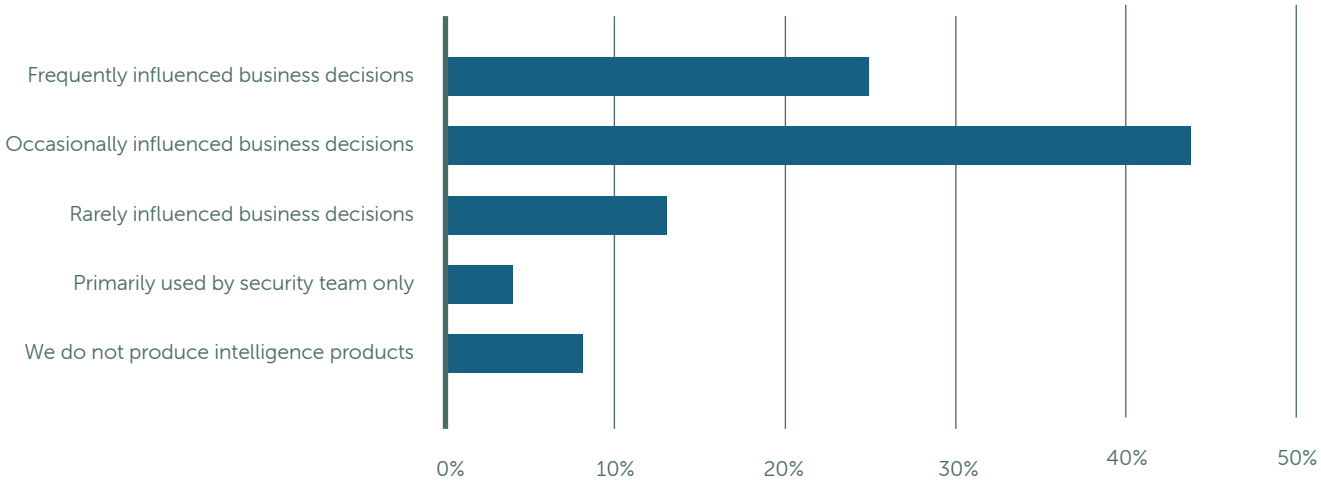
The corporate security intelligence impact gap

Measures of the sharing and consumption of intelligence do not necessarily equal impact. **Only one-quarter of CSOs said their intelligence team's products frequently influence business decisions** and one-third said they influenced either rarely or not at all (see Figure 19).

Figure 19

Direct impacts of corporate security intelligence on business decisions in last 12 months

CSOs from MNCs



There are five ways corporate security intelligence can better meet business needs:

1. From supply-side to demand-side intelligence models

Corporate security teams can enhance their value to the business by switching from a supply-side to demand-side model. As one CSO told us: 'We need our intel analysts to stop producing and spend more time listening to the business and what they need.' The most successful intelligence teams start with business requirements rather than intelligence outputs.

Demand-side intelligence model Case study

One CSO described his intelligence team's journey from a supply-side to a demand-side model.

Problems with the original supply-side model included:

- High volumes of content were being produced
- Audiences were frequently overwhelmed
- Content was mostly generic
- Emails were typically unread and content discarded

The CSO set his team the following challenge:

- Only provide products that are requested
- Over index the people you work with most: give them more, anticipate their needs, shift resources to them, be specific, and tailor the content
- Stop producing output for non-consumers

The outcome:

- Demand for products increased
- Adjacent entities saw the outputs and requested their own tailored insights
- Business perceptions of intelligence changed

The CSO told us: 'It was a revelation for my intelligence team because in limiting supply and being really focused, demand for their work increased. They didn't anticipate that. Making the shift has changed the way they are seen in the business.'

2. Step forward to coordinate the enterprise intelligence ecosystem

Corporate security increasingly operates within a wider enterprise intelligence ecosystem. Intelligence and insight are generated in various parts of the business – including enterprise risk management teams, government affairs, other risk and resilience functions, supply chain, third party risk, and business units – with leaders relying on specialist providers, government sources, and peer networks. This presents an opportunity for corporate security to act as a convenor, enabling the business to realise value greater than the sum of its parts from these various sources.

Enterprise intelligence coordination Case study

One CSO told us how his corporate security intelligence team convenes five intelligence teams from across the business every two weeks to ensure the total value of their intelligence outputs is greater than the sum of their individual contributions.

They were not tasked with this role by the business, but stepped forward on their own initiative when they saw the opportunity to drive maximum benefit for the company.

Another CSO told us: 'We have switched our view of corporate security as the main intelligence producer to [that of] the principal convenor. Not only has it greatly enhanced insight for the business, it has given us access and influence.'

3. Use AI to elevate the impact of corporate security intelligence

Historically, intelligence teams were judged on their ability to collect information. AI now increasingly shifts value towards interpretation, supporting prioritisation and decisions, and helping organisations to understand relationships, dependencies, and second-order impacts across multiple areas of the business.

AI can help intelligence teams:

- Scale intelligence collection and monitoring
- Improve signal-to-noise ratios
- Generate better intelligence products
- Support better business decisions
- Predict risk rather than simply report it
- Evolve into strategic enterprise intelligence functions.

4. Get serious about competing with the AI-enabled executive

Executives now have direct access to AI tools and can answer many intelligence questions themselves. This is changing expectations around speed and responsiveness, and increasingly corporate security teams are – in effect – in competition with their own C-suite.

Getting ahead of the C-suite
Case study

One CSO described how his team has created AI agents to run intelligence reports at 05:30 each morning, in order to pre-empt likely enquiries from C-suite members who are themselves using AI to make sense of geopolitical events.

He told us: 'We need to have our data ready so we can react immediately when the call comes. Long gone are the days when you could reasonably respond within a few hours to their requests. Today it needs to be near immediate.'

5. Build the intelligence team of the future

Corporate security intelligence teams need to develop and maintain the right skills and attributes to deliver for an increasingly demanding business. This includes curiosity about the business, willingness to embrace AI, adaptability, communication, and code switching. While intelligence tradecraft remains critical, teams need a much broader range of skills to ensure intelligence products are grounded in business concerns and communicated for impact. As one CSO put it: 'We don't need teams full of former CIA analysts. We need a mixed team consisting of analysts, engineers, scientists, and people who understand the business.'

> *"We don't need teams full of former CIA analysts. We need a mixed team."*
>
> — CSO

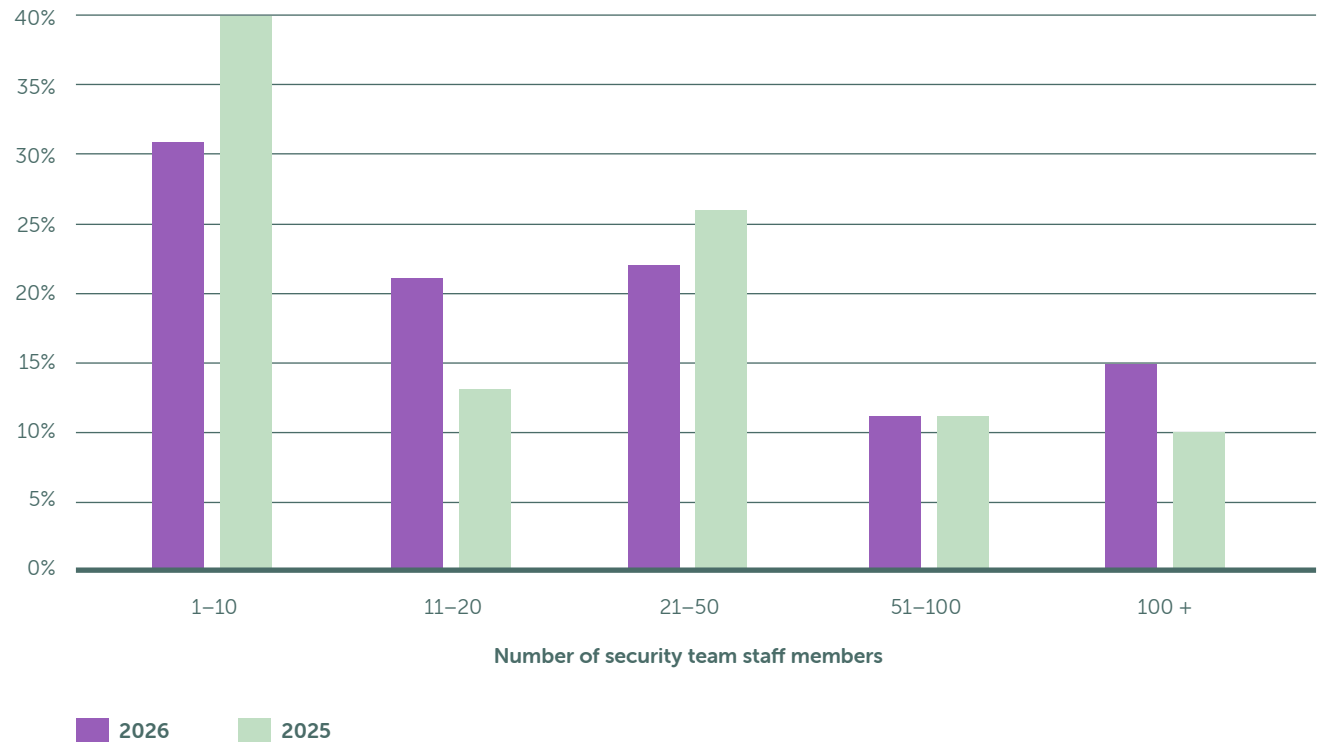
9. Corporate Security Teams

> *"Thirty-five percent of my team have already been transitioned to different kinds of work as a result of our use of AI."*
>
> — CSO

Key findings

- **Corporate security teams trend small, but with some signs of growth.** Our data shows that a larger remit does not necessarily translate into a bigger team.
- Corporate security teams are **shifting from labour-intensive security roles to analytical, intelligence-led, and technology-enabled capabilities**.
- **CSOs are starting to explore hybrid roles** to increase agility, encourage collaboration, and increase the value from relatively small teams.
- **AI is increasing capacity rather than eliminating jobs.**
- **Investment trends mirror changes in the security team,** with a shift from operational spend to investment in intelligence, technology, and resilience capabilities.

Figure 20
Corporate security team size (2026 vs 2025)
CSOs from MNCs



Corporate security team size

- **Corporate security teams still trend small:** around half have 20 or fewer members and the median size remains 11–20 people.
- **Team size is showing slight growth on 2025,** with a reduction in the proportion of teams with 1–10 people and an increase in those with 100 or more (see Figure 20).
- **Team size was not correlated to the number of areas of accountability – a larger remit does not necessarily mean a bigger team.**

- **The sectors with the largest corporate security teams** in 2026 are energy, aerospace and defence, banking and financial services, and technology.
- **CSOs have a positive but balanced view about how team size will change** over the next five years. Almost half (44%) think it will increase, one-in-five (18%) think it will decrease, and one-third (33%) think it will stay the same. US CSOs are more optimistic about team growth than are their UK counterparts.

Composition of corporate security teams is changing

The data suggests a gradual shift away from labour-intensive security roles and towards analytical, intelligence-led, and technology-enabled capabilities (see Table 1).

Table 1

	Staffing increases	Staffing decreases
Primary	Intelligence Executive protection GSOC (higher-value roles) Crisis and resilience	Guarding Operator-level GSOC roles Site security
Emerging	Data scientists AI and technology specialists Security integration roles	N/A
Drivers	Drive for intelligence-led approach Concerns for executive safety Drive for consolidation of resilience capabilities Opportunity to leverage advances in technology and AI Need for faster data analysis	Cost reduction Outsourcing Operational consolidation Automation Organisational restructuring

Increased and decreased investment

Investment trends mirror changes in team composition and reflect the deteriorating and complex threat environment, technological transformation, rationalisation of vendors and technology platforms, the need for forward-looking risk anticipation, and a drive for integration across operational risk teams (see Table 2). Overall budgets are not falling.

Table 2

Budget growth	Budget cuts
Intelligence Platforms and tools, protective intelligence, geopolitical intelligence, analysts, fusion centres, and GSOC integration	**Guarding** Often due to automation, remote monitoring, and low return on investment
Security technology and AI AI/automation, security systems (CCTV, access control, analytics), technology platform upgrades and integration, single pane of glass and system consolidation, drone detection and surveillance technology, and identity and access management	**Vendor/third party** Consolidation of fragmented intelligence tools and SaaS products
Executive protection Increased travel, residential security, protection tools, event protection, and staffing	**Travel** Reduction in travel budgets for corporate security teams, in some cases driven by increased regional hiring
GSOC Expansion, modernisation, fusion centre creation, integration of systems and intelligence, and operational centralisation	**GSOC operational staff and manual operations** Investment in GSOCs comes alongside decreased spend on manual operations
Crisis and resilience Crisis management exercises, business continuity, travel risk management, and operational risk management tools	

Reinventing the GSOC

> *GSOCs need to get away from being too tactical... We are moving towards a more strategically focused operations centre.*
>
> — CSO

Our data suggests that GSOCs are **evolving from monitoring centres to intelligence and coordination hubs**. As one CSO told us: 'GSOCs need to get away from being too tactical. We can automate many of the processes and we need to stop pumping out lots of information that has no relevance. We are moving towards a more strategically focused operations centre.' We see this shift reflected in the staffing and budget changes noted above.

Hybrid roles: A trend to watch

Several CSOs reported moving towards hybrid roles as a means of increasing agility, encouraging collaboration, and creating greater value from small teams. Hybrid roles appear to be emerging in four areas: intelligence, protection, risk, and financial/insider risk. While still at an early stage, these clusters suggest teams are beginning to organise around integrated capabilities (see Table 3).

Table 3

Cluster	Hybrid roles	Drivers
Intelligence	Intelligence + GSOC + investigations + data	Information convergence Common datasets AI adoption
Protection	Executive protection + GSOC + events	Operational overlap
Risk	Crisis + business continuity + operational risk	Convergence around resilience
Financial/insider risk	Fraud + investigations	Shared investigative skills

AI is reshaping work more than reducing headcount

Almost all CSOs think their team's use of AI will increase in the next five years. Contrary to popular discussion around AI-driven workforce reduction, our findings suggest AI is currently being used primarily to increase capacity rather than eliminate roles. **Cost is not the primary driver for the adoption of AI – only 26% of CSOs cited this as a motivation, with even fewer (13%) mentioning headcount reduction.** Where they occur, staff cuts appear to be driven more by cost pressure and delivery model changes than AI-led automation.

Only 26%

of CSOs said cost reduction was a driver for AI adoption.

Our data also suggests that staff are starting to be redeployed into higher value work. As one CSO told us: 'Thirty-five percent of my team have already been transitioned to different kinds of work as a result of our use of AI. Intelligence has been the first area we have focused on; most of the work can now be done through prompt, with the human on the loop for 15% of the workload, which now involves much higher value work.'

Diversity

Gender diversity has gone backwards since 2025: more teams in 2026 are comprised of either zero or just 1–25% women, while there are now fewer companies where women make up more than half of the team. **Gender diversity is weaker at leadership team level than across the team as a whole** (Figure 21), and there has been a slight increase in the proportion of all-male leadership teams. There are a similar proportion of individuals under the age of 40 years on leadership teams as there are women (Figure 22).

Figure 21

Proportion of corporate security leadership team who are women

CSOs from MNCs

Figure 22

Proportion of corporate security leadership team who are under 40

CSOs from MNCs

10. Talent

"If I have people on my team with good judgement, I know we can move mountains."

— CSO

Key findings

- **The key competencies for corporate security remain the same,** focused on business partnership, strategic leadership, and adaptability.
- **Talent pipeline risks** come through in the data, with a stagnation of entry-level roles, limited participation in graduate training programmes, and low levels of succession planning among leadership teams.
- **Corporate security teams are actively preparing for the era of AI,** investing in AI literacy, experimentation, and training – but CSOs are clear about the continued importance of human judgement in corporate security.
- Data on professional associations shows **increased demand for insight and knowledge** and a heightened appreciation of the **networking** benefits of membership.

> *It's soft skills that allow you to translate your technical skills into a business outcome.*
>
> — CSO

Competencies for corporate security

CSOs continue to place the greatest value on competencies that enable security team members to partner with the business, help it to navigate uncertainty, and thrive as professionals in a constantly changing environment:

Business partnership: Connecting security to the business. Communication, collaboration, teamwork, and influencing skills enable security professionals to translate technical expertise into business outcomes. These competencies are becoming more important as risks increasingly span multiple functions.

'The days of the security team working on its own are over. Today it's non-negotiable that you work across functions, with HR, IT, legal, commercial. It's soft skills that allow you to translate your technical skills into a business outcome.' (CSO)

Strategic leadership: Helping the business navigate uncertainty. Strategic thinking, judgement, and decision-making are increasingly important in a period of heightened volatility and risk. These competencies enable security teams to move beyond managing incidents and towards helping the organisation anticipate challenges and weigh competing priorities with the company's risk appetite.

'I'm big on good judgment over technical prowess or experience. A lot of what we do you can teach, but being able to understand the full context, business drivers, and different stakeholder interests and then put everything together to make a decision that you can stand behind, that's easier said than done. If I have people on my team with good judgement, I know we can move mountains.' (CSO)

Adaptability: Thriving in a changing environment. Agility, a learning mindset, and readiness for change are increasingly valuable as corporate security continues to evolve. Whether responding to new risks, adopting AI-enabled tools, or supporting changing business priorities, security professionals must be able to learn quickly and adapt their approach.

'The key attribute for me is agility, the ability to move your purpose, work ethic, and decision making, so that you can fit within a team, the corporate environment, so you can help the business where things change daily and pivot quickly.' (CSO)

Professional development

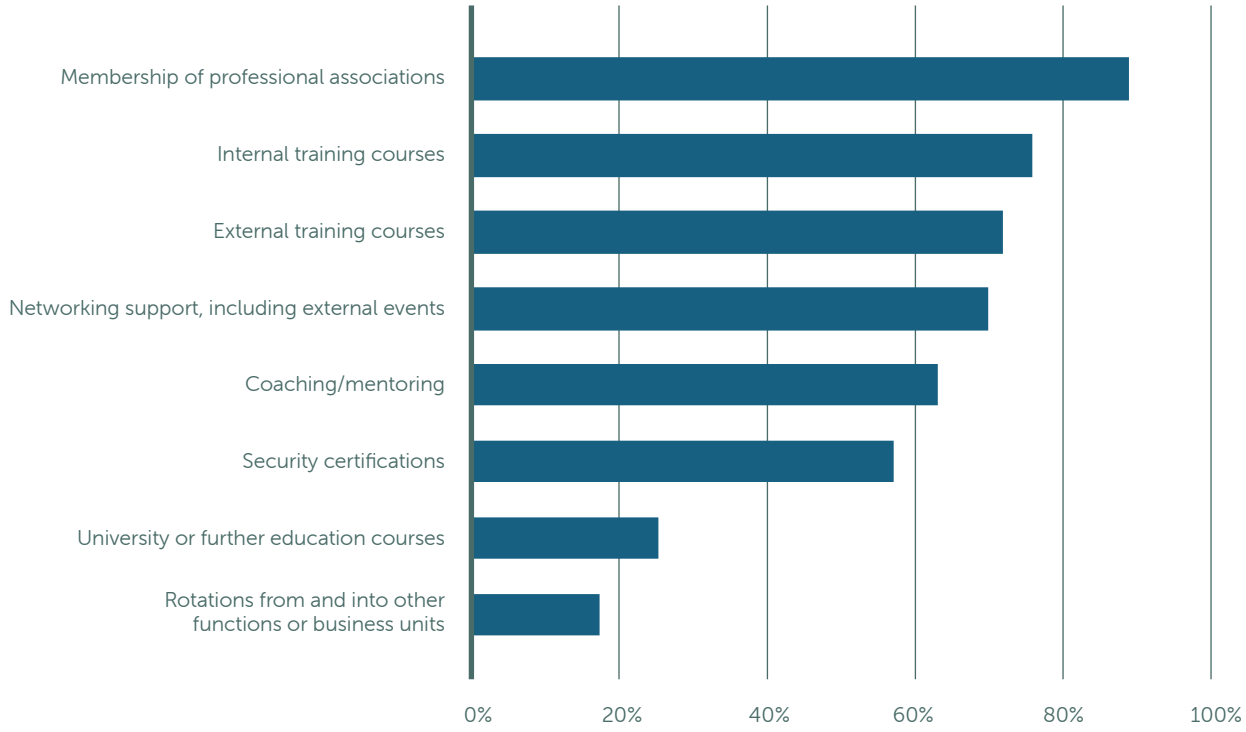
75%

of corporate security teams have access to specialist AI training.

Between 2025 and 2026, there were no material changes in the types of professional development opportunities available to corporate security teams – although the proportion whose teams had access to specialist AI training rose from 63% to 75%. The most frequent professional development opportunities offered by corporate security teams (see Figure 23) were:

- membership of professional associations
- internal and external training courses
- networking support

Figure 23
Professional development opportunities
CSOs from MNCs



Recruitment challenges

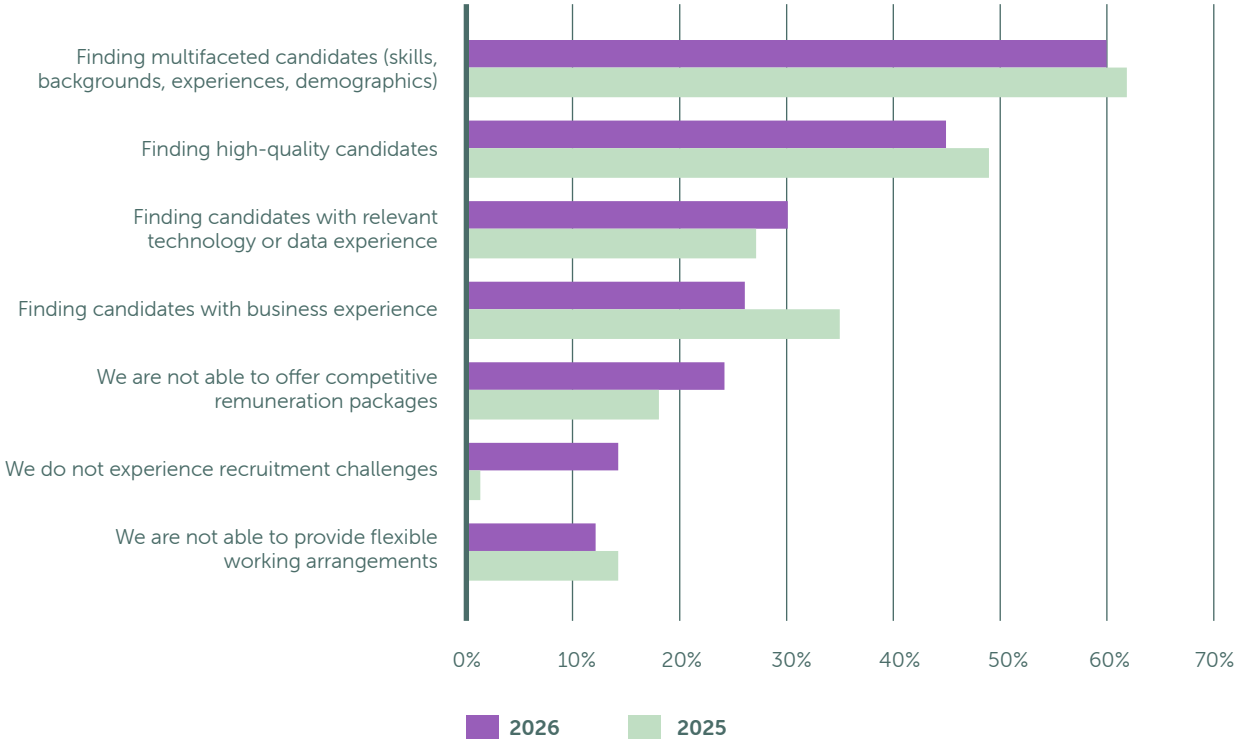
CSOs report facing similar recruitment challenges in 2026, with the top challenges remaining the same: 'finding multifaceted candidates' and 'finding high quality candidates' (see Figure 24).

As corporate security continues the transition from a labour-intensive protective function to an enterprise capability that delivers insight, coordination, technology-enabled decision making, and effective crisis management, these recruitment challenges remain critical.

Figure 24

Top recruitment challenges (2026 vs 2025)

CSOs from MNCs



A talent pipeline at risk?

Our data raises questions about the strength of the corporate security talent pipeline:

- **Stagnation in entry-level roles:** Entry-level roles are likely to stagnate, with half of CSOs expecting them to stay the same over the next five years.
- **Limited participation in graduate trainee programmes:** Fewer than one-in-five corporate security teams whose company has a graduate trainee programme are participating, missing an opportunity to plug gaps at the junior end of the talent pipeline.

- **Succession planning:** Corporate security functions fare poorly on succession planning; only one-third of corporate security leadership teams have succession plans in place for the majority of their members.

Preparing security teams for the AI era

As AI adoption accelerates, many teams are focusing on workforce readiness as much as technology implementation:

- **Building AI literacy:** Some CSOs are putting their entire team through AI training, while others are encouraging individual experimentation or embedding AI development into individual objectives.
- **Encouraging experimentation:** Many organisations are finding that practical experience is one of the most effective ways to build AI confidence and capability. One CSO described running exercises in which security managers were required to rely only on AI to complete tasks. AI provided an 80–20 solution at very short notice and revealed considerations that security managers had not identified.
- **Maintaining human judgement:** Interviewees were clear that, despite the benefits of AI, human judgement remains critical. Security context decisions frequently involve ambiguity, competing priorities, and organisational that require experience and professional judgement.

Professional or industry associations

Professional associations continue to play a vital role in professional development, networking, and raising standards across the security profession. Almost all (99%) CSOs belong to a professional or industry association, and cite the most important membership benefits as networking, conferences and meetings, education and training, standards and guidelines, and industry research.

Two changes stand out in the membership benefits that CSOs are mentioning this year:

- **Insight and knowledge:** CSOs are looking for authoritative insight and guidance in a complex risk environment. The benefit of industry research was cited by 55% of CSOs (up from 44% in 2025), alongside a similar increase for standards and guidelines (57%, up from 44% in 2025).
- **External networks:** CSOs recognise that the team's collective external network is increasingly critical to its success. Premium/exclusive networking was cited as a benefit of association membership by 32% of CSOs this year – double the proportion in 2025.

Professional associations can also help corporate security professionals to build critical leadership and influencing skills. As ASIS International CEO, Bill Tenney, put it: 'One of the key skills security professionals can build through taking on volunteer leadership roles in associations is influencing without authority. That's one of the most important skills security professionals need today.'

Appendix

Appendix

Methodology

The 2026 CSO Survey was conducted between March and April 2026. It received a total of 176 responses, of which 118 met our inclusion criteria. The data in this report relates to these 118 responses, supplied by CSOs from international companies with more than 3,000 employees. The survey was open to all and anonymous. We also interviewed members of the survey's Advisory Council and representatives from select sponsor organisations. Interviews were held in June and July 2026.

The following individuals were members of the 2026 CSO Survey Advisory Council: Ryan DeStefano, Andrew Gay, Alex Hawley, Wayne Hendricks, Charles Lacy, Joshua Levin-Soler, Duncan Manning, Kirsten Meskill, Jules Parke-Robinson, Hugh Parsons, Arlin Pedrick, Matt Sinden, and Keith White. They played an important role, shaping the survey questions and analysis.

Unless otherwise stated, all quotations, both anonymous and attributed, are from interviews carried out for the survey in June–July 2026.

Partners

The 2026 CSO Survey is kindly sponsored by Ontic, ASIS International, Corporate Security Advisors (CSA), Factal, Seerist, and Dataminr. The views expressed in this report are those of The Clarity Factory and do not necessarily reflect the views or positions of the sponsors.

Acknowledgements

We launched the Annual CSO Survey because we want to provide a reliable and longitudinal dataset for CSOs to help power their vital work protecting and enabling the organisations they serve.

This year's survey – the second – offers both a snapshot in time and a perspective on how things are changing. Last year, CSOs told me they had used the data presented in our 2025 report to finetune their programmes, benchmark their efforts, and make a strong business case for their work. I'm thrilled that our data has such tangible and positive impacts on the vital work done by corporate security teams.

I would like to extend my sincere thanks to the companies who sponsored the 2026 Annual CSO Survey. They recognised the importance of independent data and provided their support without a desire to influence the findings. Thank you to Ontic, ASIS International, Corporate Security Advisors (CSA), Factal, Seerist, and Dataminr for your leadership in our community.

A huge thank you to the members of the Advisory Council, who dedicated time to shaping survey questions to ensure our data is relevant and impactful for CSOs. They also reviewed and provided feedback on the survey data, and some were interviewed as part of the research process. My aim with The Clarity Factory is to provide data and insights that are directly and immediately useful for CSOs, and I'm always grateful that CSOs take time to help us achieve that goal. Thanks to Ryan DeStefano, Andrew Gay, Alex Hawley, Wayne Hendricks, Charles Lacy, Joshua Levin-Soler, Duncan Manning, Kirsten Meskill, Jules Parke-Robinson, Hugh Parsons, Arlin Pedrick, Matt Sinden and Keith White.

Thanks to those who have helped with the production and dissemination of this report:

Tom Hampson (Hampson Studio) and Sophie Gillespie (Inkwell Communications & Design) and valued members of The Clarity Factory team: Louise Brennan, Jo Sayer, and Paul Sizemore.

Finally, I would like to thank Paul and Dot for dragging me to the beach between edits.

All errors are, of course, my own.

Rachel Briggs OBE, 28 July 2026

About The Clarity Factory

The Clarity Factory elevates security leadership through data, insights and practical solutions. We create clarity from complexity – to enable you to thrive.

The Clarity Factory can help you in the following ways:

- **Benchmarking:** our benchmarking offers structured comparable data and insights on where you stand relative to your peers, opportunities for growth, and areas of relative advantage. Our benchmarking reports provide action-oriented recommendations to enhance performance and draw on Clarity Factory proprietary data. ClarityFactory.com/services/benchmarking

- **Maturity Assessments:** The Clarity Factory Maturity Assessment Framework provides an independent, structured and data-driven maturity assessment to drive insights on strengths and areas for development. You will receive a data-rich report, recommendations and insights suitable for sharing with the C-suite. ClarityFactory.com/services/maturity-assessments

- **Strategic Advisory:** we partner with security leaders going through change by helping you to scope the problem, gathering data to inform your thinking, benchmarking you with your peers, conducting a skills audit to future-proof your staffing model, constructing your team's value proposition, and creating a roadmap for change. ClarityFactory.com/services/advisory

- **Storytelling for Security Leaders:** Security leaders must persuade and influence the business to get the resource, position, and partnership necessary to be effective. Our storytelling workshops and coaching, delivered in partnership with HumanStory, empower CSOs, CISOs and their teams to communicate with clarity, build trust, and influence at the executive level. ClarityFactory.com/services/workshops

- **Security briefings:** our CEO, Rachel Briggs, provides high-impact briefings for security teams, providing latest industry data and actionable insights. Perfect for corporate security leadership team meetings and global all-hands off-site gatherings. Available virtually or in-person. ClarityFactory.com/briefings

Sign up to our monthly newsletter
ClarityFactory.com/subscribe

Get in touch
info@ClarityFactory.com

Thinking ahead

The Clarity Factory Annual CSO Survey, 2027

What CSOs say about The Clarity Factory CSO Survey:

"This is a must read for everyone in the corporate security profession."

"This report has become a 'must-read' for our team and the industry."

"This industry has needed an insightful product like this for a long time."

"I shared the report with my boss, and it has resulted in a useful and constructive discussion. Very helpful given the usual OPEX pressures."

Sponsorship opportunities

The Clarity Factory looks forward to working with thought-leading innovators within the security industry to deliver our **Annual CSO Survey, 2027**.

We are pleased to offer a range of sponsorship opportunities. More information about the survey and sponsorship can be found at: ClarityFactory.com/survey-sponsorship

If you would like to discuss sponsorship, please contact Rachel Briggs OBE:

rachel.briggs@ClarityFactory.com

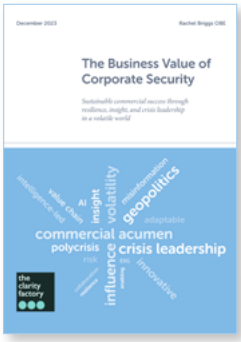
Other reports by Rachel Briggs OBE

Annual Chief Security Officer Survey, 2025

The Clarity Factory, 2025

Holistic Security: How physical and cyber security can join forces to strengthen operational resilience

The Clarity Factory, 2025



The Business Value of Corporate Security: Sustainable commercial success through resilience, insight, and crisis leadership in a volatile world

The Clarity Factory, 2023

ClarityFactory.com

the clarity factory

Annual CSO Survey, 2026

The Clarity Factory Annual CSO Survey helps CSOs track trends and prioritise resources. It offers three recommendations for 2027:

Prioritise measures to strengthen corporate security's role as an enterprise integrator: Companies are consolidating risk ownership in the most specialised function and driving increased collaboration across operational risk teams.

Switch from supply-side to demand-side intelligence to maximise business impact: Only one-quarter of corporate security intelligence teams are currently impacting business decisions on a regular basis.

Build a two-to-three-year talent strategy to deliver on the transition from protection function to enterprise capability: Teaming composition is shifting from labour-intensive security roles towards analytical, intelligence-led and technology- and AI-enabled capabilities.

ClarityFactory.com

ISBN 978-1-7384176-3-6

9 781738 417636