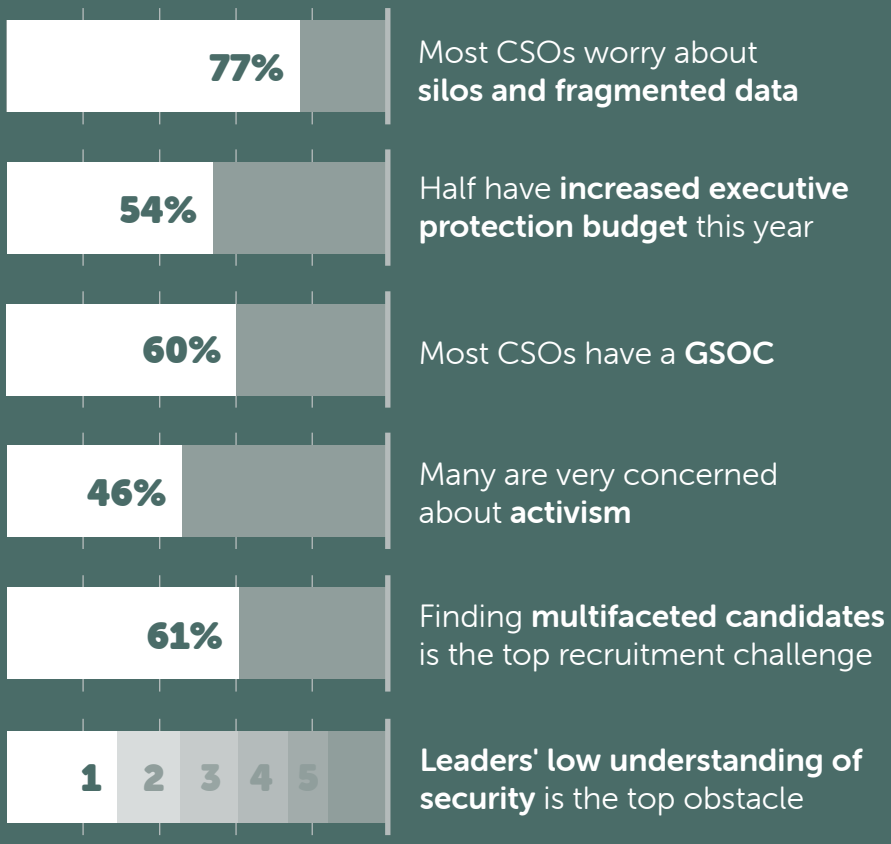
the clarity factory

Rachel Briggs OBE

Annual Chief Security Officer Survey 2025



Platinum partner

Gold partners

The 2025 Chief Security Officer (CSO) Survey is kindly sponsored by Ontic, ASIS International and Emergent Risk International. The views expressed in this report are those of The Clarity Factory and do not necessarily reflect the views or positions of the sponsors.

The following individuals acted as members of the 2025 CSO Survey Advisory Council: Steve Brown, Alex Hawley, Wayne Hendricks, Charles Lacy, Joshua Levin-Soler, Duncan Manning, Kirsten Meskill, Jules Parke-Robinson and Derek Porter.

The 2025 CSO Survey was conducted between April and June 2025. It received 200 responses, 96 of which were from CSOs at international companies with more than 3,000 staff globally. The data referenced in this report refers to the dataset of 96 CSOs. The survey was open to all and anonymous. We also interviewed CSOs, representatives from sponsors, and industy experts.

While job titles vary, this report uses the term 'CSO' as shorthand for the most senior corporate security leader within the organisation. The report refers to 'corporate security', which in some companies is known as 'physical security'.

ISBN: 978-1-7384176-2-9

Contents

Clarity Up Front

> *"It's not a case of 'if', but rather 'when?' and 'where?' Increasingly, the answer is 'now' and 'everywhere'."*
>
> **— Bill Tenney, ASIS International**

In July 2024, a bug in CrowdStrike's security software update led to a global IT outage. For the CSOs accountable for business continuity, the incident highlighted the importance of a holistic approach to security and resilience and of reinforced relationships with cyber security and IT colleagues.[1]

On 4 December 2024, UnitedHealthcare CEO, Brian Thompson, was shot dead in Manhattan. In a perverse turn of events, the alleged killer was lauded as a folk hero by some online, who saw his crime as an act of justice and donated hundreds of thousands of dollars towards his defence.[2] Corporate leaders immediately reached out to their CSOs for reassurance about executive protection.

On 23 January 2025, the British Museum suffered an IT outage after a terminated technology contractor gained access to an unauthorised area of the building and turned off the IT systems. Cyber security colleagues got a lesson in the futility of cyber defences if the server room door is left open and physical security measures are lacking.[3]

In April 2025, British retailer Marks & Spencer suffered a ransomware attack that left shelves empty, customer data compromised, and its online ordering system down for months. Criminals gained access to the system after they socially engineered an employee of the company's IT supplier to provide login details. The company estimated the financial costs to be in the region of £300 million.[4] The incident offered a fresh reminder of the importance of a strong security culture.

In May 2025, external contractors working for Coinbase accessed sensitive customer data. They shared it with cyber criminals, who demanded a USD 20 million ransom.[5] It was another reminder of the growing threat from insider risk.

On 28 July 2025, a 27-year-old drove into Manhattan, double-parked his BMW, walked into a Park Avenue office building with an assault-style rifle, and murdered four people. Coming months after Brian Thompson's murder in the same city, it resurfaced fears about protecting executives, staff, and buildings.[6]

The past 12 months have been challenging for global corporate security leaders. They have grappled with everything from the fallout of geopolitical events and social and political shifts, to heightened threats to senior executives, growing insider risk, and sophisticated cyber security attacks.

Like all parts of the business, they are being asked to deliver more with less; make sense of the challenges and opportunities of AI, emerging technologies, and data; and ensure their talent strategy is fit for purpose.

The Clarity Factory Annual CSO Survey 2025 contains a wealth of data to help CSOs understand industry trends, benchmark their programmes, and make resourcing and talent decisions. This year, its first, the survey report offers baseline data that will be repeated on an annual basis. It is delivered in partnership with our sponsors, Ontic, ASIS International, and Emergent Risk International.

There has never been a more important time to get security right. This survey arms security leaders with the data they need to protect and enable their organisations.

Five insights stand out in 2025

1. Effective security is holistic security

- Three-quarters of CSOs agree that 'Corporate security's ability to protect my organisation's people, assets, and reputation is **negatively impacted by organisational silos and fragmented data'.**

- **The risks that CSOs ranked most critical are those that can only be managed effectively through partnership:** cyber security; data security and intellectual property theft; geopolitical risk; extreme weather events; activism, protest, and civil unrest; insider risk; and third-party risk.

- **A majority of corporate security teams are involved in supporting the delivery of adjacent areas of risk management,** providing an increasingly holistic security service for their organisation. These areas include information protection and assurance, cyber security, disaster recovery, third-party risk, disrupting fraud, due diligence, supply-chain security, business intelligence, and business continuity.

- **Corporate security teams support a wide range of partners across the business,** with more than half of CSOs partnering with facilities, executive leadership, legal and compliance, human resources (HR), cyber security, health and safety, communications, marketing or external relations, and IT.

- **A growing proportion of corporate security is delivered by vendors and third parties,** working alongside the organisation's full-time security employees (FTEs). Almost half of CSOs outsource up to 25% of the roles in their function, and one-in-five outsource more than one-quarter. The roles most often outsourced are within the team's core areas of responsibility: global meetings and events, threat intelligence, executive protection, and travel security.

2. There is a renewed focus on physical and people security

- **The corporate security portfolio has grown in recent years,** both in direct areas of accountability and in expectations that they will partner across the business.

- CSOs recognise that a small number of security-related risks – **cyber security attacks, geopolitics, and data security and IP theft** – are exercising business leaders, and that these have the most critical impact on organisational resilience.

- **But senior leaders are now also paying attention to physical and people security** again. Recent events – the murder of Brian Thompson, the Park Avenue attack, protests at investor meetings, and a call to arms against corporations – have put executive protection, event security, physical security, workplace violence, and access control firmly back on the agenda. While CSOs in 2025 ranked these risks as relatively low, our research shows that executives are seeking enhanced reassurance. We will continue to watch these trends.

- For UK CSOs, there is heightened concern about the impact of other physical and people security risks, including armed conflict, crime and organised crime, travel risk, and terrorism.

- **A key area of personnel growth within the function is in regional security management:** in an increasingly volatile world, CSOs are staffing up to make sure they have experienced boots on the ground.

3. Geopolitics creates challenges and opportunities for corporate security

- **Geopolitics sits in the middle of the Venn diagram between business and security leaders' concerns.** As Saadia Zahidi, Managing Director of the World Economic Forum, put it: 'Today, geopolitics – and specifically the perception that conflicts could worsen or spread – tops the list of immediate concerns.'[7]

- The geopolitical risks that CSOs rank as most important to their organisation are **global economic uncertainty, cyber threats from state and non-state actors, and China–Taiwan.**

- **Two-thirds of CSOs have intelligence teams with geopolitical capabilities** that could be harnessed by senior business leaders. Their challenge is to ensure they understand business need, effectively partner with other geopolitical experts in the business, remain up to date with changing needs and risk appetite, and choose the products that will best serve their audiences.

- **Corporate security intelligence has potential to be a game-changing business resource in the management of geopolitical risk and beyond – but only if it is visible.** Almost one-third of CSOs ranked 'low understanding of security among business leaders' as the top obstacle to the effectiveness of the function (excluding budget and headcount). CSOs should not assume that business leaders understand their intelligence capacity or wait to be invited in. They should hone storytelling skills to communicate the impact and possibilities of their intelligence offering.

- Intelligence products should be fine-tuned to meet executives' demands for impact insights over lofty analysis.

4. Changing social and political dynamics impact corporate security

- Social and political shifts mean global corporations are now seen as 'players', whether they intend to be or not. This impacts the company's risk profile, with many experiencing **increased activism and protest, threats to senior executives, and insider risk.**

Clarity Up Front

- **Almost all CSOs run an executive protection programme;** a majority cover digital as well as physical risks, and personal as well as professional exposure. CSOs are increasing staffing for executive protection, and just over half have increased their executive protection budget in the last 12 months. Almost all CSOs allocate resources using a risk-based model.

- **CSOs rank insider risk among the most impactful threats facing their organisation:** for 8% it has a 'critical' impact and for 34% the impact is 'high'. Three-quarters said their company has an insider risk programme, with most covering all staff rather than just high-risk roles like system administrators or executives. Half of the CSOs we surveyed are accountable for insider risk; the others are not accountable, but still involved. CSOs are increasing staffing for insider risk.

- **Almost half of CSOs ranked the impact to their organisation of activism/protest/civil unrest as 'critical' or 'high'.** Activists target people, products, buildings, and technology systems. Whether violent or not, their actions place an added burden on the corporate security function.

- Corporate security teams must forge partnerships with their peers – typically **community relations, government affairs, or external relations** colleagues – who are involved in monitoring, managing, and responding to these social and political trends.

- Corporate security can add value by leveraging its intelligence team and on-the-ground network to help the business understand and anticipate problems.

- Corporate security teams will be accountable for responding to security incidents via executive protection, physical security, and insider risk programmes, as well as GSOC and crisis management capabilities.

5. Corporate security enhances operational resilience

- **The risks managed by physical and cyber security teams increasingly sit in the middle of the Venn diagram between the two functions.** Critical touch points include IT security, data security, access control, people security, insider risk, activism and protest, and fraud prevention.

- **A comprehensive and effective response requires partnership that draws together each function's knowledge, data, processes, and resources.** The Clarity Factory's Holistic Security Maturity Model offers a nimble, organisation-model agnostic approach to partnership between physical and cyber security teams, flexible to organisational need, culture, risk level, and appetite. Holistic security is an outcome, not an organisational structure.

- **Companies that reach full maturity in their cross-functional partnerships boost operational resilience.** Holistic security improves risk management, creates enduring enterprise-wide partnerships, and integrates the three critical processes of operational resilience: business continuity, crisis management, and disaster recovery.

Three recommendations for CSOs for 2026

CSOs drafting their strategy and resourcing plans for 2026 should:

Prioritise partnership working

- **Build a culture that values and rewards partnership.** Introduce behavioural objectives that measure partnership working within the function and across the business.

- **Seize the initiative to build enduring structures for partnership with key functions,** including legal, IT, cyber security, community or government affairs, and HR. Good interpersonal relationships between leaders are crucial, but partnerships only endure when underpinned by resources, processes, and incentives.

- **Measure your holistic security maturity** to provide accurate data about your current situation and chart next steps to strengthen partnerships.

- **Don't wait to be invited into discussions about geopolitical risk.** Build a compelling story about the value of your intelligence capability, tailor products to meet business needs, and approach partnerships with colleagues across the business with curiosity and humility, recognising their wealth of complementary knowledge.

Invest in communication and storytelling skills

- **CSOs say that poor understanding of security among business executives is the biggest obstacle to their effectiveness.**
- But executives don't need to be educated about the *functions* of security – and **metrics are a management tool, not a communication technique.**
- Instead, do what all corporate leaders do: build your story. Stories generate trust. Stories are sticky – and more likely to be remembered and retold. **Effective stories will generate compound interest for corporate security brand equity.**
- **Invest in communications and storytelling** training and create a functional narrative to build trust, awareness, and influence. This is what will secure the focus, time, and resource you need to be effective.

Tighten up your talent strategy to meet your needs head on

- **Multifaceted teams deliver better in complex, fast-moving environments** – but CSOs say finding multifaceted candidates is their biggest recruitment challenge. If you want to be different, do different. Change your recruitment strategy to find a broader range of candidates.
- **Reprioritise social skills alongside technical ones,** and follow through by revising job descriptions, recruitment scoring systems, and professional development strategies.
- **Support your team to become 'technology curious' and foster a culture of 'fail fast and pivot'.** Technology is evolving and corporate security must keep pace with the rest of the business.
- **Invest in professional associations** that keep you and your team connected with new ideas, enabling them to bring innovation back to the home team.

1. Security Risks

> *"It's not a case of 'if', but rather 'when?' and 'where?' Increasingly, the answer is 'now' and 'everywhere'."*
>
> **— Bill Tenney, ASIS International**

CSOs in multinational corporations are managing a highly complex environment:

- **Cyber-attacks** have grown significantly in scale and frequency.
- **Volatility** has created regional hotspots in the supply chain, impacting products, people, and reputation.
- **Social and political changes** have made companies and executives 'fair game' for protest, attacks, and insider threat.
- **Climate change** is triggering extreme weather events and social upheaval.
- **Nation states** are targeting corporations for their resources and IP.
- **Terrorists** pose a threat in parts of the world.

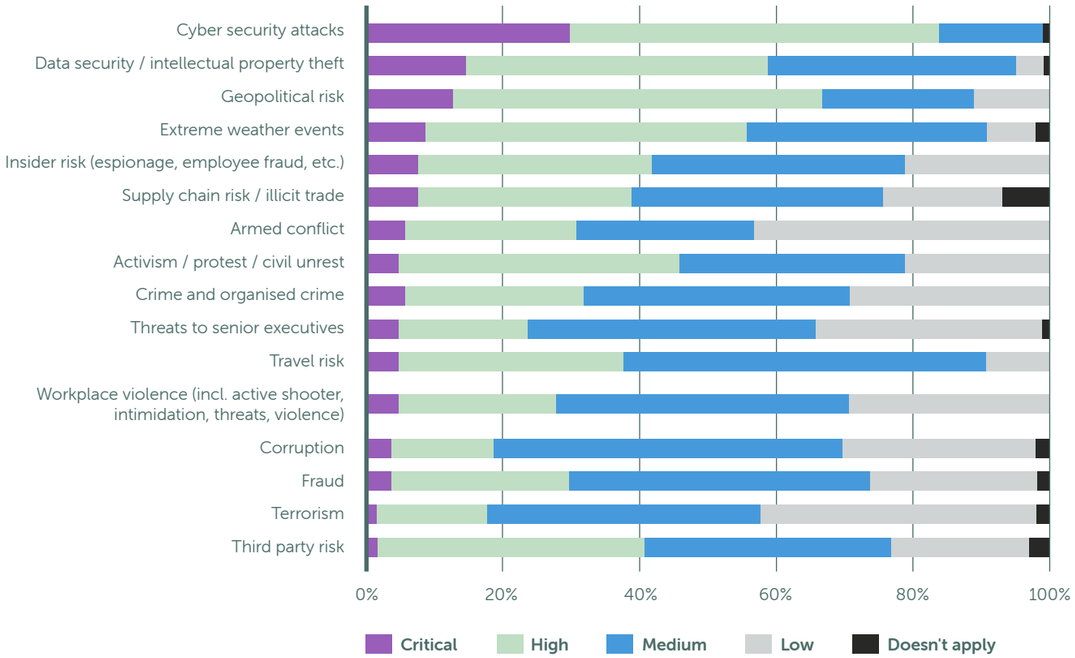
When we asked CSOs to rate a series of security risks based on the extent to which they impact their organisations, 'cyber security attack' was the only risk to be rated 'critical' by more than one-in-five respondents (Figure 1).

Only four security risks were ranked 'critical' or 'high' by more than half the CSOs: **cyber attacks, geopolitical risk, data security/IP theft, and extreme weather events.**

Figure 1

Security risks impacting your organisation

CSOs from MNCs



Five key insights on security risks

Cyber security attacks is the top security risk, followed by data security/IP theft, geopolitics, and extreme weather events.

The threat of activism and protest is growing as companies and executives are seen as 'fair game'.

Armed conflict and terrorism are ranked low overall.

CSOs rank traditional security risks as having a lower impact on the business, e.g. armed conflict, crime, threats to senior executives, travel risk, workplace violence, and terrorism.

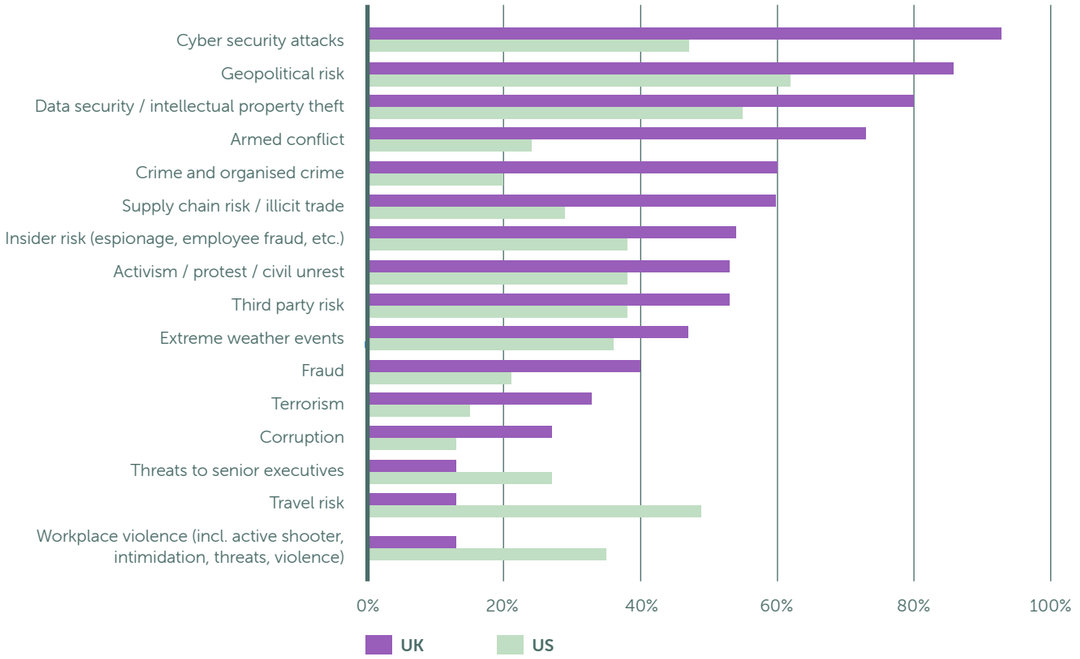
The highest-ranked risks require partnership working, such as cyber security attacks, data security/IP theft, geopolitical risk, extreme weather events, insider risk, and activism/protest/civil unrest.

Differences between US and UK CSOs (Figure 2)

- **People-related security risks:** US CSOs rate workplace violence, travel risk, and threats to senior executives much higher than UK CSOs.
- **Conflict, crime, and terrorism:** UK CSOs are much more likely than US CSOs to rank these as 'critical' or 'high'.

- **UK CSOs are more concerned about cyber and data security** than US CSOs.
- **UK CSOs adopt higher risk ratings across most security risks,** rating 'critical' or 'high' much more often than US CSOs.
- **US CSOs are twice as likely as UK CSOs to rank threats to senior executives** as 'critical' or 'high risk' to their organisation. This almost certainly reflects concerns in the US following the murder of Brian Thompson in December 2024 and subsequent attacks on corporate leaders.

Figure 2
'Critical' and 'high' security risks to your organisation
US and UK CSOs from MNCs



2. Accountability and Partnership

"By working together, we can bring a holistic picture about risk and what it means for our company."

— CSO

In a global business environment characterised by heightened security risks and greater volatility, effective corporate security enables multinationals to operate safely, be resilient in the face of shocks, and manage through crises with confidence.

There is no 'standard' corporate security portfolio, because each must meet the needs of its company in terms of risk profile, risk appetite, and geographical footprint (Box 2). Accountability will also differ because some perform a light-touch governance role, where others are highly operational and have full vertical visibility through the function.

Our survey shows that the majority of CSOs have accountability for a core group of tasks (Box 1).

Box 1

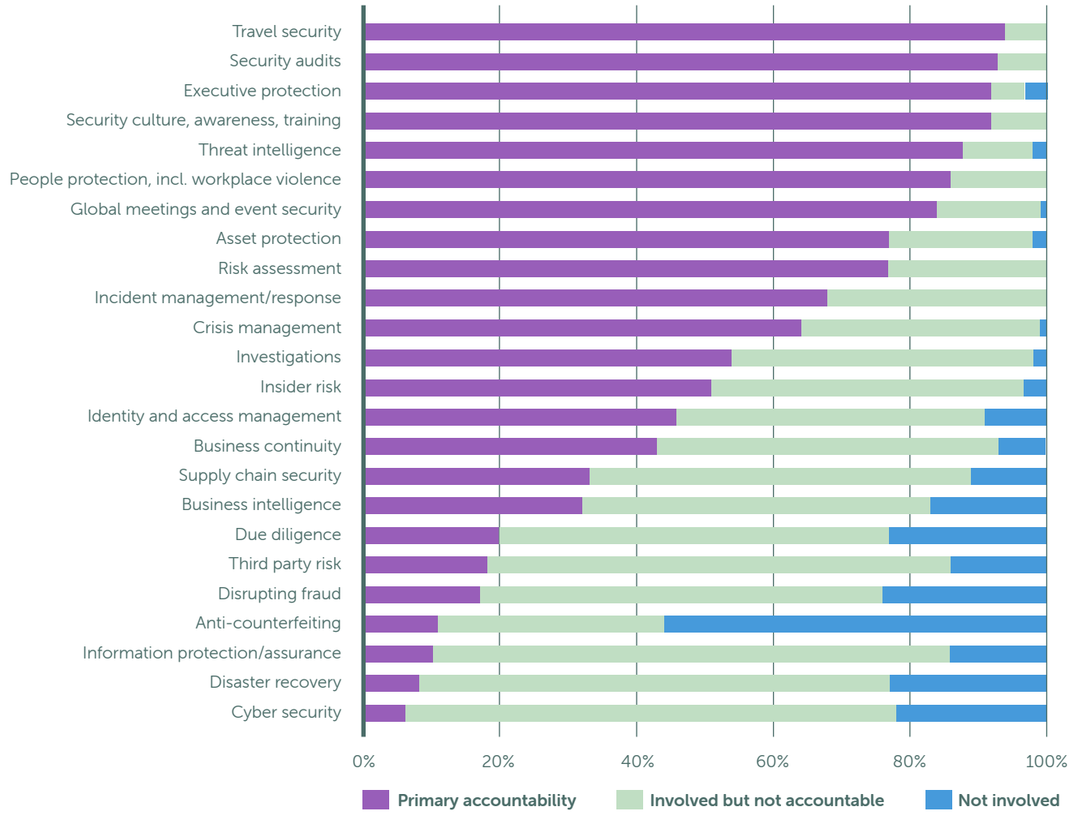
A majority of CSOs are accountable for:

- Travel security
- Security audits
- Executive protection
- Security culture, awareness, and training
- Threat intelligence
- People protection, incl. workplace violence
- Global meetings and event security
- Asset protection
- Risk assessment
- Incident management/ response
- Crisis management
- Investigations
- Insider risk

Figure 3

Areas of accountability

CSOs from MNCs



Box 2

Company-specific responsibilities

Effective corporate security functions enhance their value by adopting additional responsibilities specific to their company, based on factors that impact a multinational corporation's security risk profile:

Sector

- **Intellectual property** tends to be higher risk for pharmaceutical companies.
- **Brand integrity** is especially important in the luxury goods sector.
- **Fraud** will usually be high on the risk register for banks and retailers.
- **Information security** is especially critical for legal firms and those holding sensitive client or customer data, such as healthcare providers.
- Companies handling highly valuable goods, such as precious metals, are likely to have **organised crime** at or near the top of their security risk register.

Geography

- Some risks are geographically specific, such as **kidnap, piracy,** or **civil war**, so firms tied to those locations, such as extractives, are more likely to be impacted.
- Some organisations, such as NGOs and the media, run towards danger, taking them into the path of **wars and conflicts** that others would avoid.

Profile

- Some sectors are more prone to **political activism**, such as banking, energy, and pharmaceutical companies.
- **Social and investor pressure** is making a wider range of sectors a target for activism.

Products

- Companies with high-value products, such as precious metals or luxury brands, will require much higher security around their transport and **supply chains**.

Activities

- Certain risks are time-limited, such as those associated with mergers and acquisitions or divestment activities, when **insider risk** or **espionage** might be more likely to occur.
- New market entry can spike an organisation's **travel risks** due to new travel patterns.

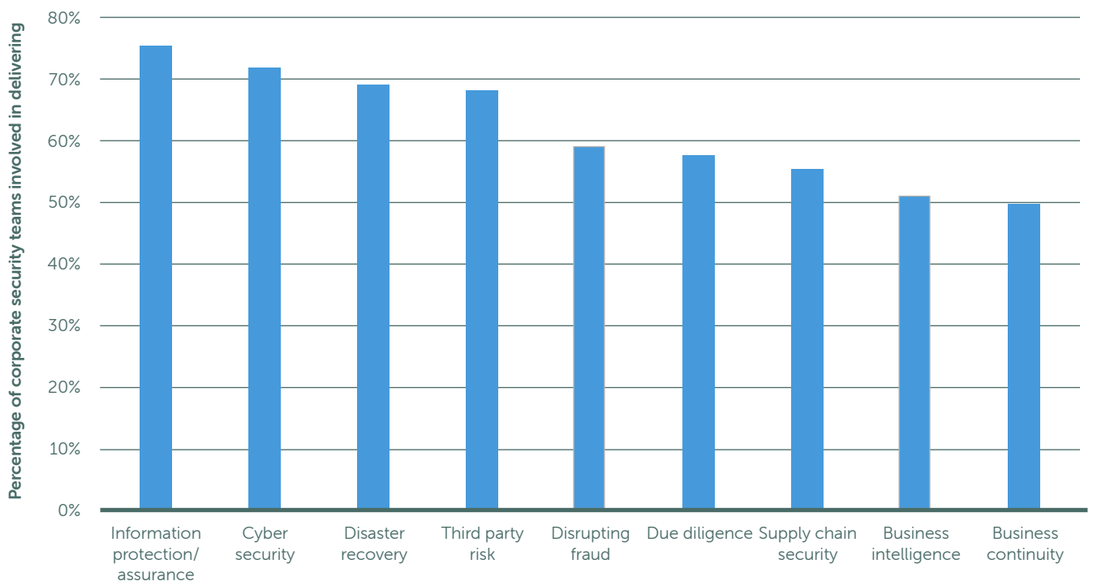
> *It's important to acknowledge that silos continue to exist. The importance of bridging silos resonates in a big way.*
>
> — Manish Mehta, Ontic

Holistic security requires corporate security to partner with other security-adjacent teams

CSOs increasingly see partnership across the business as non-negotiable to the success of corporate security. They rank **'data and organisational silos' as one of the top three obstacles to the effectiveness of corporate security**.

Alongside their core areas of accountability, a **majority of CSOs are involved in adjacent areas along the holistic security spectrum** (Figure 4).

Figure 4
Corporate security involvement in adjacent areas
CSOs from MNCs



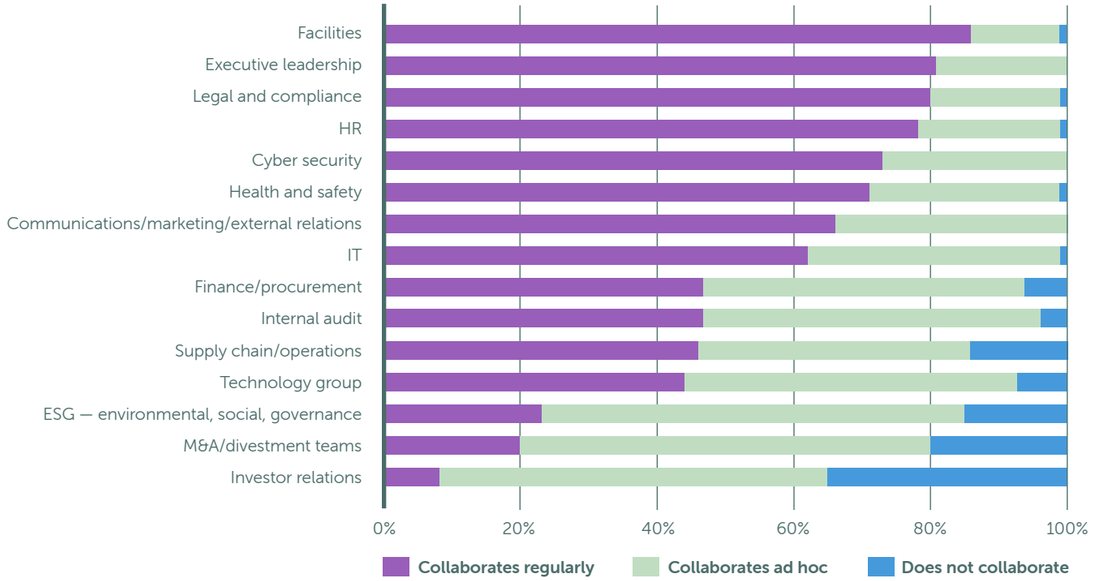
> *Security is unique in their ability to reach right across our business.*
>
> — Senior business executive

Corporate security collaborates with partners across the business

Multinational corporations increasingly manage risks that span functions, and are dealing with multiple risks concurrently. In this context, silos cause missed opportunities, obscure risks, and create blind spots. **Business leaders want risk functions to collaborate to provide a more holistic view of risk.**

A majority of CSOs collaborate with: facilities, executive leadership, legal and compliance, HR, cyber security, health and safety, communications/ marketing/external relations, and IT (Figure 5).

Figure 5
Collaboration across the business
CSOs from MNCs



77%

of CSOs agree their effectiveness is negatively impacted by organisational silos and fragmented data

Partnerships between corporate security and other business functions will vary based on the company's sector. For example,

- **Pharmaceutical**: legal and compliance, supply chain, government affairs.
- **Fast-moving consumer goods:** supply chain, corporate communications/brand.
- **Extractive:** health and safety, government affairs.
- **Healthcare:** legal and compliance, IT, cyber security, HR.
- **Finance:** IT, legal and compliance, cyber security.

Two partnerships in particular are critical for most companies and are likely to feature more heavily in 2026:

Digital security: CSOs ranked cyber security/ data security and IP theft among the most critical security risks impacting their companies, so it is positive that such a high proportion of CSOs partner with cyber security and IT colleagues.

The Clarity Factory's Holistic Security Maturity Model is a practical tool that CSOs and CISOs can use to start a conversation about partnership, rank their partnership maturity, and create an action plan for enhanced collaboration. (See Section 8 on Holistic Security and Operational Resilience.)

One CSO told us how he has used the maturity model to revive and enhance the relationship with his CISO: '*It allowed us to discuss some of the misunderstandings, and enabled us to iron out the friction points. It also allowed us to discuss resources and as we talked about how we were supporting the business together, the CISO put forward some of his budget to enable us to do something that otherwise would not have been possible given constraints on the corporate security budget.*'

Communications/marketing/external relations: Social and political changes are having a profound impact on a company's risk profile. These changes include increased activism, disinformation and deep fakes, disenfranchised employees and customers, threats to senior executives and facilities, regulatory change, and growing nationalism.

A growing number of **CSOs are building internal relationships with the teams that help leaders understand social and political issues and their impact on the business.** Depending on the sector, this might be a government affairs, community affairs, or external relations team. CSOs recognise that they have intelligence pertaining to these trends and will be responsible for mitigating related security risks and managing incidents and crises (see Section 5 on Shifting Social and Political Dynamics).

3. Geopolitics

> *"The geopolitical axis is forever twisting and turning, which makes it somewhat unpredictable. It can be all good today, and then up in arms tomorrow."*
>
> — C-Suite member[8]

Geopolitics is a boardroom priority

Geopolitics is consistently ranked by senior business leaders as one of the key risks facing their corporations. As Saadia Zahidi, Managing Director of the World Economic Forum, put it: '*Today, geopolitics – and specifically the perception that conflicts could worsen or spread – tops the list of immediate concern.*'[9]

Geopolitics sets the backdrop for the work of corporate security teams. While CSOs must develop a sound understanding of how these trends could impact the business, many geopolitical events are too large, complex, and broad-ranging to mitigate. As one CSO put it: '*For the most part, whether it's criminality, activism, terrorism, they are all relatively straightforward to mitigate against. Where I'm really exposed is in relation to armed conflicts like South China Seas, China-Taiwan, strikes on Iran, which are completely out of my control. There is a limit to the amount of mitigation I can put in place, and it really is consequence management.*'

We asked CSOs to rank the top five **geopolitical risks** to their organisation (Figure 6). Three stand out: **global economic uncertainty, cyber threats from state and non-state actors, and China–Taiwan.** As Meredith Wilson, CEO of Emergent Risk International, told us: '*I'm not surprised these three stand out. Almost all multinational corporations have some kind of China nexus, are rattled by global economic uncertainty, and see a real and present cyber risk.*'

Figure 6
Top five geopolitical risks to your organisation
CSOs from MNCs

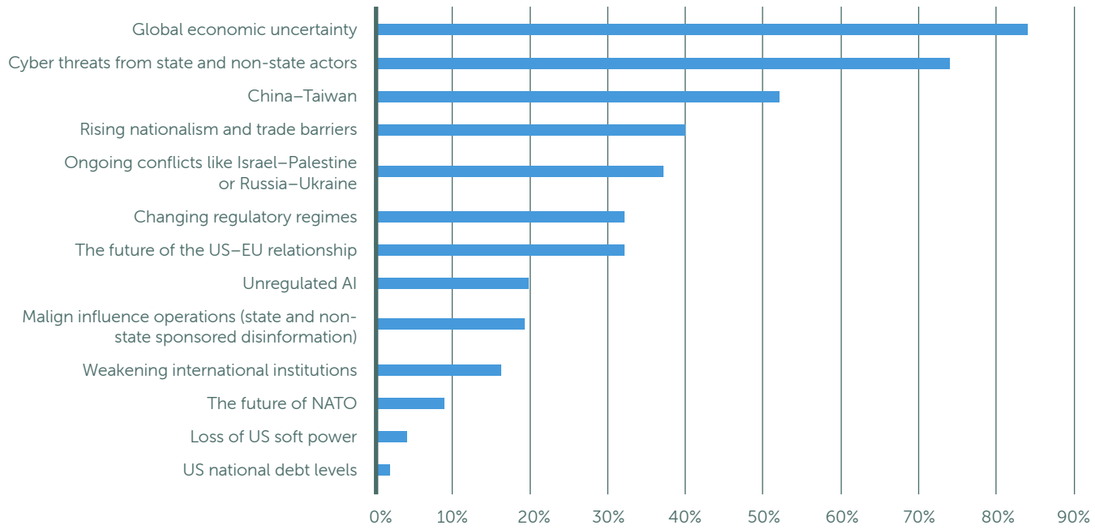
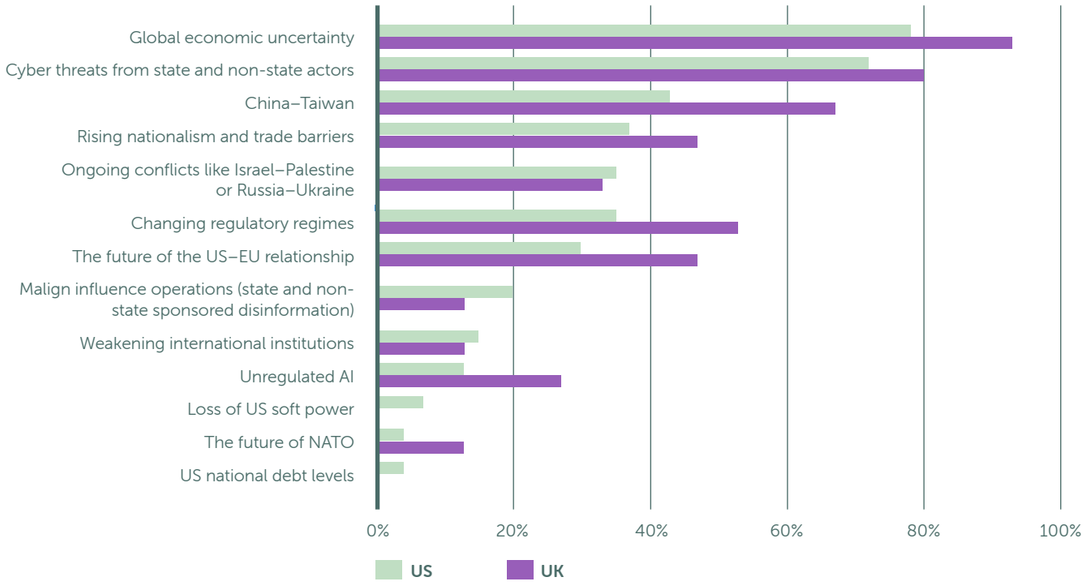


Figure 7

Top five geopolitical risks to your organisation

UK and US CSOs from MNCs



Differences between US and UK CSOs include (Figure 7):

- **UK CSOs were more likely to rank China–Taiwan** in their top-five geopolitical risks.
- **UK CSOs were significantly more concerned about institutional geopolitical risks:** changing regulatory regimes, the future of the US–EU relationship, and the future of NATO.
- **US CSOs were slightly more concerned about weakening international institutions.**
- **UK CSOs were twice as concerned about unregulated AI.**

> *You need to grow a voice and credibility and show people that you are worth engaging on geopolitics. You can't achieve that overnight, and you have to be proactive rather than waiting to be asked.*
>
> — CSO

Geopolitics: An opportunity to deliver insight

Many corporate security functions have intelligence teams that provide information, intelligence, and analysis – from tactical to strategic.

For a growing number, this capability includes geopolitical expertise that can be harnessed to inform business decisions and strategy. Some corporate security intelligence teams are already contributing in this way – for others, this role is aspirational.

Corporate security intelligence teams seeking to turn their geopolitical knowledge and expertise into usable insights for the business should consider the following questions:

- **What does the business need,** and how can we find out?
- **Who else has geopolitical expertise** and how can we coordinate to avoid duplication, confusion, or conflict? Other functions to consider might include: external relations, government affairs, corporate affairs, community relations, supply chain, enterprise risk management, and business intelligence.
- How can we get around **sensitivities about information sharing?**
- **How can we keep ourselves up to date with business risk appetite and operating context** to ensure our products are well-timed and appropriately calibrated?

- What **products** work best?
- What **skills and expertise** do we need to deliver business-focused analysis via a multi-stakeholder approach?

Corporate security must live by four maxims when contributing geopolitical expertise to the business:

1. **Do not assume business leaders know what expertise you have.** C-Suite members may not be aware that their security function has any interest in and knowledge of geopolitics, as was the case with one CFO who asked us: '*I know why the board is interested in geopolitics, but why is my security team interested in it?*'
2. **Fine-tune reporting** to meet the needs of busy business leaders who are interested in business impact rather than lofty analysis.
3. **Don't wait to be invited in.** Demonstrate what you know, share your insights, and persist over the long term. It will take time for executives to get used to turning to you for insights.
4. **Communicate for impact.** Focus on the 'so what?' for the business and invest in communications and storytelling skills to ensure you land the message in a way that sticks.

> ***It's vital to talk to the business. You can't provide the right product for internal clients if you don't know what they need.***
>
> — Meredith Wilson, Emergent Risk International

4. Corporate Security Intelligence

> *One of the key challenges for CSOs right now is ensuring that their intelligence function understands the business it is serving and communicates in a way that delivers maximum value.*
>
> — CSO

Intelligence has become an established feature of corporate security over the past decade. Today more than **two-thirds (69%) of CSOs have professionally trained intelligence analysts** on their team. CSOs use a mix of permanent FTEs and embeds/contractors to deliver their intelligence capability, with just over **one-quarter (27%) of CSOs using embedded analysts**.

There are pros and cons to in-house versus external contractors, with some opting for the latter due to a desire for flexibility, the ability to scale up or down quickly, a cap on raising headcount, and the benefits of having analysts' professional development handled by an expert vendor. Others prefer FTEs with longevity in post and a deeper insight into corporate context.

Corporate security intelligence end users

CSOs report that their intelligence products reach a wide range of internal clients.

Two key untapped opportunities are evident:

Supply chain: Because of shifting geopolitics, almost half (46%) of CEOs surveyed by PwC said they were considering adjusting supply chains,[10] and in another study, three-quarters (73%) cited supply chain security as one of the main challenges facing corporate security in the next five years.[11]

Corporate security has vital intelligence and data that can improve insight on critical supply chain decisions, but **fewer than half (48%) of CSOs identified supply chain as an end user for their intelligence products.**

Cyber security: CSOs rank cyber security attacks as the top security risk impacting their company - a view shared by business leaders and boards. From cyber espionage and intellectual property theft to fraud, threats to senior executives and deep fakes, criminals, terrorists, and nation states use the full spectrum of methods to target simultaneously across digital and physical domains. A siloed approach in the face of joined-up security threats leaves companies exposed - yet **only 43% of corporate security intelligence teams target their products for cyber security end users.**

The Clarity Factory Holistic Security Digital Assessment Tool is being used by threat management teams from physical and cyber security functions to assess the maturity of their partnership and map out opportunities to collaborate.

From security intelligence to business insight

Corporate security intelligence teams play a vital role in serving the needs of the corporate security function. Additionally, they can generate significant value by meeting the needs of the business.

> ***Different companies have different needs in their intelligence analysts, but you always need people who are business-oriented and flexible.***
>
> — Meredith Wilson, Emergent Risk International

Business leaders recognise the value of security intelligence,[12] and effective CSOs look for ways of using it to enhance outcomes across the business. This includes intelligence-driven decision making, supply-chain visibility, de-risking of product cycles, enhanced visibility of risks around M&A/divestment activities, and stakeholder insights to feed into environmental, social and governance (ESG) efforts.

CSOs looking to apply corporate security intelligence to business needs should:

- **Position corporate security intelligence as a business asset**, not just a functional one.
- **Identify ways to connect intelligence data with data from other parts of the business**, such as operations, supply chain, and cyber security. As one CSO said: '*You can't assess risk if you don't have the internal data that enables you to understand the impact of security incidents.*'
- **Find ways to connect analysts with the business**, e.g. working groups or rotations, or situating them within the business rather than in the corporate security team.
- **Be surgical**: less is more when it comes to business-focused intelligence.

CSOs that fail to apply corporate security intelligence for broader business use leave valuable insight on the table, and lose an opportunity to influence.

5. Shifting Social and Political Dynamics

"Given shifting social and political dynamics impacting corporations, CSOs need to have ever closer connectivity with government affairs departments."

— CSO

Social and political shifts mean global corporations are now seen as 'players', whether they intend to be or not.

Corporations face growing pressure not only to operate fairly and ethically, but also to take a stance on political and social issues, whether directly linked to their business or not.

As Lucien Alziari, Chief Human Resources Officer at Prudential, put it: '*There was a time when a CEO could say, 'But what does this have to do with my company? Isn't this a matter in the personal or political sphere?" Such a perspective is unlikely to serve any executive well in the times ahead.*'[13]

Social and political changes impact a company's risk profile, directly impacting the work of the corporate security function.

- **Activism and protest:** Taking a public stance on social or political issues can make companies a target for attack; **almost half (46%) of CSOs ranked the impact to their organisation of activism/protest/civil unrest as 'critical' or 'high'.** Activists target people, products, buildings, and technology systems, and whether violent or not, their actions place an added burden on the corporate security function.

- **Threats to senior executives:** There is growing expectation for CEOs to be the personal face of their corporation's public positions; 81% of investors globally say CEOs should be personally visible when discussing public policy with external stakeholders, and a majority of employees expect business leaders to speak publicly about controversial social and political issues.[14] This can increase the CEO's risk profile, and **one-quarter (24%) of CSOs ranked the impact to their organisation of threats to senior executives as 'critical' or 'high'.**

- **Insider risk:** Insider risk is growing, with **42% of CSOs ranking the impact on their organisation 'critical' or 'high'.** CSOs are not alone in this view; almost all (90%) cyber-security professionals believe their organisation is vulnerable to insider threats, which cost a median of USD 4.45 million to resolve.[15]

"Issues that impact companies economically tend to have a security nexus, whether because they lead to insider threats, reputational damage, boycotts, or direct attacks."

— Meredith Wilson, Emergent Risk International

The rise of mis- and disinformation generates a range of risks

The World Economic Forum identifies mis- and disinformation as the top global risk in the short-term.[16] The consequences include decreased share price, attacks on senior executives, protests, disruption to operations, and damage to stakeholder relationships. The rise of AI and deep fakes will heighten these risks.

Companies must manage risks related not just to what they **have** said and done, but also what they **have not.** For example, a 2020 conspiracy theory that Wayfair was involved in child trafficking led to threats to its CEO and attempts to short the company's stock. And a fake press release purportedly from the Grand Hyatt in Seattle announcing shelter to the homeless impacted by wildfires generated protest from those against housing the homeless and later, when the deception was exposed, from those berating the hotel for failing to provide shelter.[17]

The rise of mis- and disinformation creates challenges and opportunities for corporate security intelligence teams, who must join forces with communications colleagues, widen their focus from threat actors to monitoring emerging disparate narratives,[18] and create a virtuous information loop with business colleagues to ensure market-based ground truth informs their intelligence assessments. They must listen as well as transmit.

Corporate security can add value to improve how the business manages social and political issues

The CSO at a fast-moving consumer goods company told us about how the relationship between corporate security and community relations grew. His intelligence team were reporting on shifts in politics and activism and the potential impact on the company and its brands.

This generated concerns from community relations colleagues who were worried about the content of the briefings. It became an opportunity to learn, build a relationship, and understand the strengths both teams brought to the company.

He told us: '*I realised we needed to make our intelligence products more operationally focused, so we shifted our posture. It also helped community relations to understand that corporate security has valuable insights and access to data that can be helpful for them. The problem and how we all responded to it created synergy, and we now work together incredibly effectively.*'

The CSO went on to describe how they have now systematised the relationship to ensure continuity and due process:

- Regular **information flows** between key personnel.
- Corporate security includes community relations on the distribution list for their weekly intelligence bulletin.
- Both teams sit on their organisation's crisis management group.
- The CSO is invited to certain community relations **standing meetings.**
- Both teams look for **opportunities to learn and collaborate informally,** including joint business trips.

6. Executive Protection

> *"We have a bigger focus on executive protection and visibility on threats to our Executive Committee."*
>
> — CSO

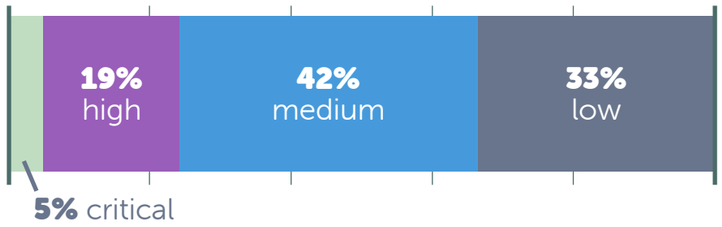
> *"Given the Brian Thompson execution, the attack on legislators in Minnesota, and the attack on Park Avenue, we are seeing the pendulum swing back towards core corporate security issues, including executive protection and threats to the workplace."*
>
> — Bill Tenney, ASIS International

The threat to executives has intensified as violence becomes a more accepted form of political expression. **Over half (54%) of CSOs have increased their executive protection budget in the last 12 months, with no significant difference between US and UK CSOs.** The threat was brought into tragic focus with the murder of UnitedHealthcare CEO Brian Thompson in December 2024, and the subsequent celebration, in some quarters, of his alleged murderer, whose actions were framed by some as an 'act of justice'.[19]

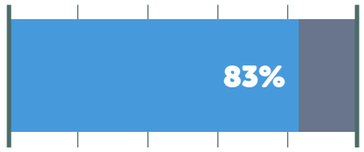
Thompson's murder **heightened concern in boardrooms,** and many CSOs have been asked to reinforce or stand-up executive protection programmes. CSOs report that executives are more cognisant of the threat and are more willing to tolerate the disruption associated with enhanced protection for themselves and their families.

Executive protection in numbers

Risk

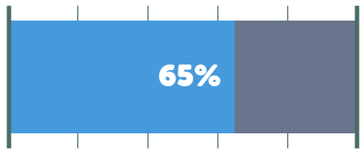


CSOs rank **'threats to senior executives'** as one of the lower risks in terms of impact to the organisation.



83% of CSOs have an **executive protection programme.**

Personnel

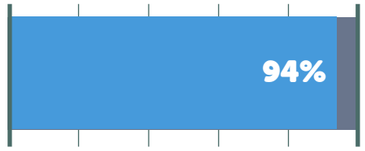


Two-thirds say their programme is delivered through a combination of **in-house and vendor** capability.

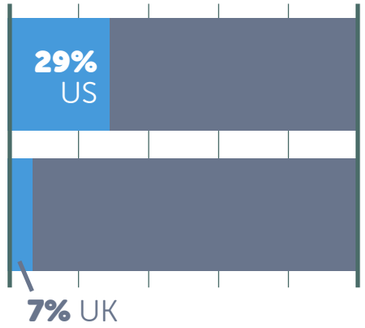
One-quarter deliver their programme using **only in-house** staff.

One-third have some **dedicated executive protection capability** who work exclusively on executive protection.

Resource allocation



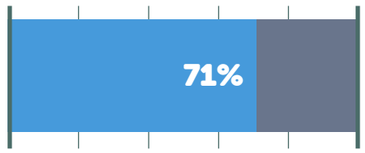
Almost all allocate executive protection resources using a **risk-based model.**



US-based CSOs are four times more likely than their UK counterparts to allocate executive protection resources **based on job title.**

Holistic executive protection

Most programmes include a **digital component.**



A large majority of executive protection programmes cover **personal as well as business** exposure for their executives.

7. Insider Risk

"Insider risk is in the left lane starting to speed ahead as a key security risk for corporate security functions."

— Manish Mehta, Ontic

"Companies often fail at insider risk by not defining their 'crown jewels.' An effective programme requires a top-down understanding of what assets are so vital that their loss would be catastrophic."

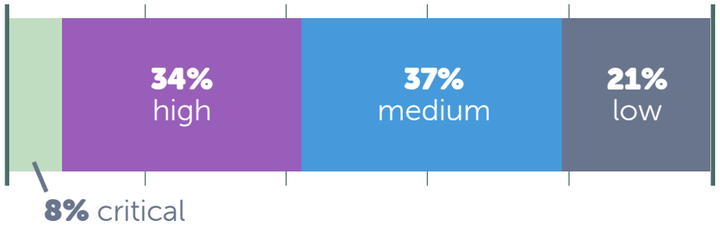
— Robin Welch Stearns, Pacific Resilience Group

Insider risk is a growing concern for multinational corporations, with corporate security playing a critical role in prevention, detection, mitigation, and response. It can take several forms, from malicious to negligent insiders; those seeking to extract money or information for nation states, criminal networks, or themselves; and those whose motivation is sabotage or reputational damage.

Partly driven by disillusionment or disengagement,[20] the social and political trends we are seeing certainly play into the rise of insider risk for major corporations; with insider events costing a median of USD 4.45 million to resolve.[21]

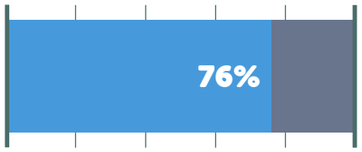
Insider risk in numbers

Risk



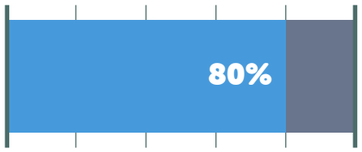
CSOs rank **'insider risk'** as one of the higher risks in terms of impact to the organisation.

Programme



Three-quarters of organisations have an **insider risk programme.**

Personnel



A majority of insider risk programmes **cover all staff** rather than just high-risk roles (e.g. system administrators, IT, help desk, executives).

Most insider risk programmes encompass a range of activities (Figure 8). There is considerable opportunity to strengthen them by integrating automated monitoring, including SIEM tools, which can spot behaviour patterns and help to divert unintentional or accidental insider actions through discreet interventions.

Tackling insider risk is a team sport

Corporate security is a critical part of managing insider risk. **Half of CSOs (51%) are accountable for their organisation's insider risk programme, with a further 46% involved but not accountable**.

> *The thing that makes managing insider risk complex is the fact that it requires buy-in from a range of functions – HR, data privacy, legal, internal investigations and security – and there is not necessarily an obvious lead.*
>
> *— CSO*

As regulators and boards demand a holistic approach, some CSOs are being asked to help create an enterprise-wide framework for insider risk. This necessarily must include a range of partners, including cyber security, corporate security, HR, legal/compliance, and IT (Figure 9).

While partnership is critical, **effective insider risk programmes must have a single owner** to avoid fragmentation and lack of focus. A number of the CSOs we interviewed described how their programme had stumbled as a result of poor governance, and boards and business executives are increasingly understanding the value of singular leadership alongside devolved delivery.

Figure 8
Elements of insider risk programme at your organisation
CSOs from MNCs

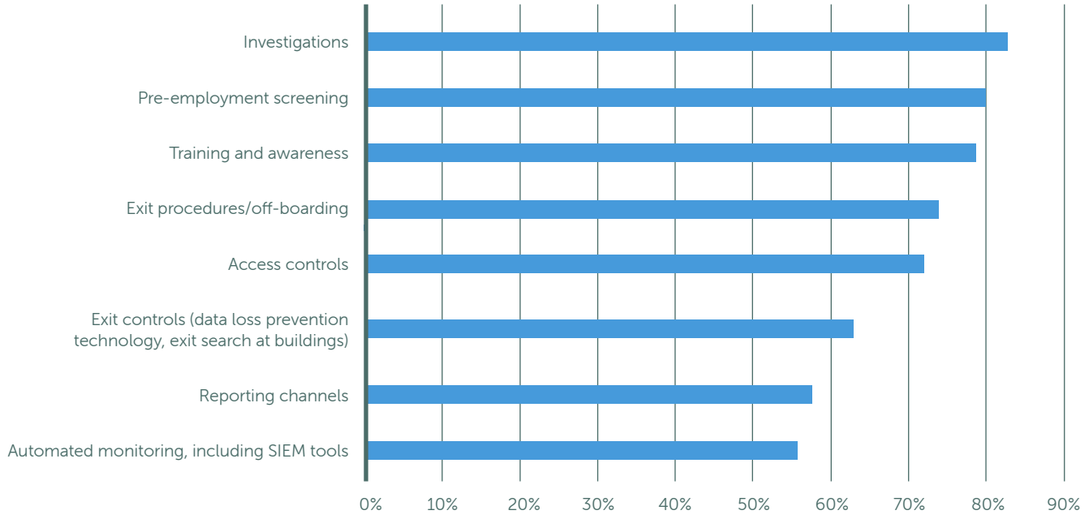
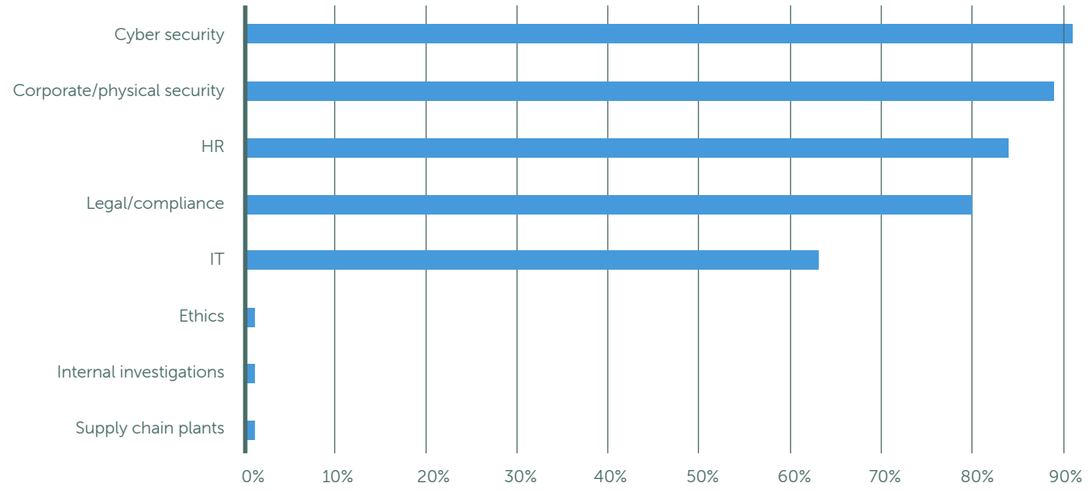


Figure 9
Insider risk stakeholders at your organisation
CSOs from MNCs



8. Holistic Security and Operational Resilience

"Fragmentation doesn't help risk management because you end up with siloed thinking and what we want is more integrated approaches and processes."

— CISO

The risks managed by physical and cyber security teams increasingly sit in the middle of the Venn diagram between the two functions. A comprehensive and effective response requires partnership that draws together their knowledge, data, processes, and resources.

Some of the most critical touch points include IT security, information security, access control, people security, insider risk, activism and protest, and fraud prevention.

'Convergence' has emerged as the 'best practice', whereby physical and cyber security are brought together into a single function. There is much to be commended about this model, but **only 15% of companies have converged.**[22]

The Clarity Factory Holistic Security Maturity Model (Table 1) offers a nimble, organisation-model agnostic approach to partnership between physical and cyber security teams. It is flexible to organisational need, culture, risk level and appetite, and is cognisant of the considerable difficulties of bringing together two very different groups of professionals.

Holistic security is an outcome, not an organisational structure that delivers a wraparound security service through smart team working and the use of shared technology and resources.

Achieving holistic security depends on:

- **creating an identity** where partnership is something that 'someone like me would do in a situation like this';
- **celebrating wins;**
- **building and incentivising new habits** through nudges, reminders, or check lists to help teammates to do the right thing, even when it doesn't feel natural;
- **making the right behaviour easier and the wrong behaviour harder**, through team structures, working groups, and co-location;
- **being specific** about exactly how teammates should behave and work differently; and
- **breaking down the change into bite-sized chunks** to get started with early wins.

Table 1
The Clarity Factory Holistic Security Maturity Model

	Level 1 >>>>>>>>>>>	Level 2 >>>>>>>>>>>	Level 3 >>>>>>>>>>>	Level 4
Identity and culture	People identify with their own team and see partnership as a distraction Leaders celebrate their own wins, but don't acknowledge other security team success	People identify with their own team and see partnership as an ad hoc 'nice to have' Leaders celebrate their own wins and acknowledge other security team success	Partnership is part of how the team works Leaders celebrate wins by both security teams	Partnership is non-negotiable Leaders celebrate success through partnership
Leadership	Leaders strongly identify as functional heads; incurious about partnership Separate functional strategies; no areas of partnership identified	Leaders identify as functional heads; see limited value in partnership Separate functional strategies; disjointed approach to third parties and vendors	Leaders identify as risk leaders; value partnership across security functions Separate functional strategies; elements of partnership; disjointed approach to third parties and vendors	Leaders identify as enterprise risk leaders; partner across business with other functional risk leaders Joint cross-functional strategy; shared approaches to technology, third parties, government contacts and vendors
Incentives	Team members have outcome goals linked to their role	Team members have outcome goals linked to their role and functional objectives	Team members have outcome goals linked to their role, functional objectives and cross-functional work	Team members have behavioural goals as well as outcome goals, and objectives related to holistic risks
Clarity of roles	No discussion about respective areas of accountability	Ad hoc partnership; no clarity of accountability	Clear roles and areas of accountability	Clear and documented accountability of roles; regular reviews
Professional development	Learning focused on individual roles Focus on role-specific technical skills	Learning focused on individual roles; limited learning across functions Focus on role-specific technical skills; social skills 'nice to have'	Learning about other areas of security actively encouraged Social skills 'desirable'	Dedicated resources for cross-functional learning Social skills 'essential'
Reporting lines	Separate reporting lines, no supervisor expectation of collaboration	Separate reporting lines, some supervisor expectation of collaboration	Joint reporting lines, limited effort to realise opportunities of partnership	Joint reporting lines, opportunities for enhanced insight are embraced
Operational	No joint working groups Separate functional processes and resources	Ad hoc joint working groups in limited areas Separate processes and resources; ad hoc input from other function (e.g. intel, SOC, technology, data)	Working groups in critical areas and effort to co-work in same location Separate processes and resources; active input from other function (e.g. intel, SOC, technology, data)	Established working groups and co-location of teams Co-design of processes to benefit from diverse views and joint decision-making
Governance	Separate board reporting No governance structures to coordinate security No governance oversight to coordinate physical- and cyber-security roles in operational resilience processes (business continuity, crisis management, and disaster recovery)	Separate board reporting; joint discussions with board Nascent governance structures to coordinate security Operational resilience is aspirational; board and risk committee take ad hoc interest in operational resilience processes	Separate board reporting; proactive coordination of data Governance structures to coordinate security Expectation of joined up approach to operational resilience; limited governance structures to drive and incentivise partnership	Joint board reporting presenting holistic view of risk Mandated governance structures to coordinate security Established oversight of operational resilience processes; expectation of partnership across risk functions

8. Holistic Security and Operational Resilience

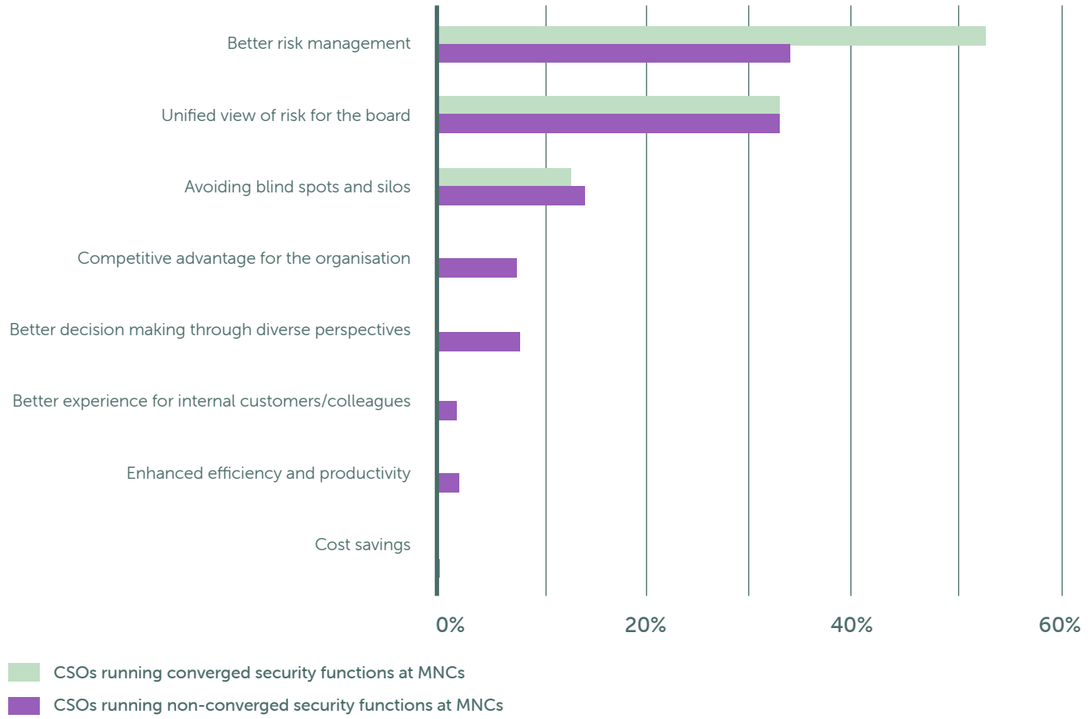
Annual CSO Survey, 2025

> *A robust and integrated security approach instils confidence in our partners and investors.*
>
> — CSO

Companies that reach full maturity also boost operational resilience because holistic security improves risk management (Figure 10), creates enterprise-wide partnerships, and integrates the three critical processes of operational resilience: business continuity, crisis management, and disaster recovery, which are usually overseen by corporate and cyber security. As a result, holistic security enhances regulator and investor confidence.

Figure 10

Benefits of collaboration between corporate and cyber security



Source: 'Holistic Security', The Clarity Factory, 2025

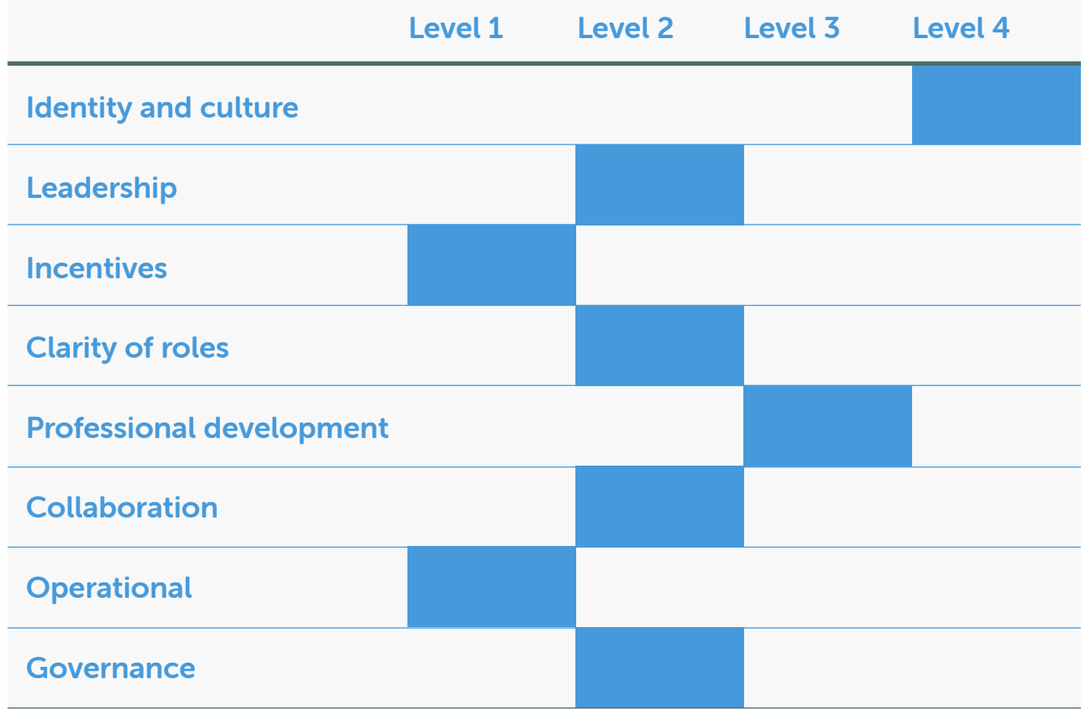
The Clarity Factory's Holistic Security Self-Assessment Tool (Figure 11) offers CSOs, CISOs, and their teams a practical way of measuring the maturity of their partnership. To learn more about the tool, visit www.clarityfactory.com/holistic-security

Figure 11

Holistic Security Maturity Self-Assessment Tool

2.12 Your Team's Holistic Security Score

Your Team's Holistic Security Scorecard



9. Technology and AI

"I hear from security leaders that they want to use technology to make their whole operation more efficient, but CSOs are limited by what's available on the market, which are largely siloed tools."

— Manish Mehta, Ontic

Technology is transforming almost every aspect of how multinational corporations operate. Corporate security, like all functions, is expected to embrace the opportunities offered by technology, in terms of productivity, interoperability, and cost savings.

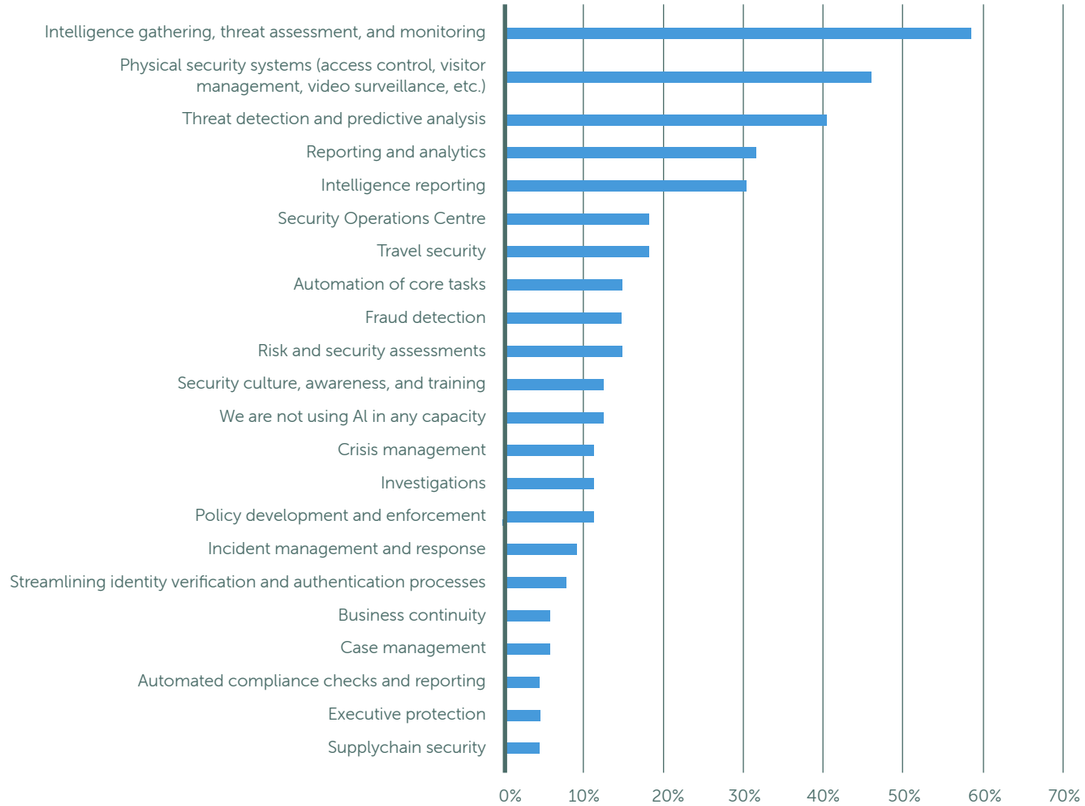
CSOs are increasing technology spending

Two-thirds (67%) of CSOs are increasing the proportion of their budget that they spend on technology, and are exploring ways that off-the-shelf and bespoke emerging technology solutions can increase efficiency, productivity, and effectiveness of processes across the work flow of the function.

Corporate security teams are selectively adopting AI to enhance their work

CSOs and their teams are applying AI in a range of areas of the function's responsibilities, with the **highest uptake in intelligence gathering, threat assessment and monitoring, physical security systems, and threat detection and predictive analysis** (Figure 12).

Figure 12
Adoption of AI in different areas of the corporate security team's work
CSOs from MNCs



Some key trends in AI adoption:

- **Intelligence gathering, threat assessment, and monitoring:** Almost 60% of CSOs use AI in this area.
- **Physical security systems:** Almost half of CSOs are using AI within access control, visitor management, and video surveillance systems. This is an area of early adoption of AI, so it would be reasonable to expect continued growth in this area.
- **Reporting and analytics, including intelligence reporting:** Almost one-third of CSOs are using AI within these processes. Given recent advances in AI, it is anticipated this will be an area of rapid adoption in the next 1-2 years.
- **Low adoption across all other areas:** Fewer than one-in-five CSOs are using AI within other areas of the function's work. As uptake grows, we can expect it to drive efficiency and productivity gains.
- **Legacy technology systems:** Many CSOs struggle with legacy technology systems, which hamper AI adoption. They also find it difficult to secure budget or focus from technology colleagues, which negatively impacts their ability to realise the opportunities of AI.

AI-powered security risk assessment
Case study

A CSO we interviewed is working with a technology provider to develop an **AI-powered security risk assessment tool**.

It would transform a process that is manual, time-intensive, and vulnerable to human error into something that is quicker, automated in parts, and more reliable.

He outlined the key differences between the current manual assessment process and the new AI-powered one, which are outlined below.

	Manual security risk assessment	**AI-powered** security risk assessment
Site assessment	• Conducted in-person by team member who reviews threats and exposure	• Draws on external feeds for information on threat • Security team add expertise on exposure
Security risk assessment	• Team member creates recommended mitigation, writes up report, often produced by cut and paste from previous reports • Scope for human error	• AI draws on company processes and guides to create mitigation measures in keeping with policy • Team member uses judgement to qualify results and add nuance
Product	• Time-intensive • Scope for human error that detracts from quality of assessment	• Less time-intensive • Less scope for human error, which increases business trust

CSOs are over-confident about their AI competences

CSOs are over-confident about corporate security's grasp of the opportunities of AI. Two-thirds (69%) of CSOs say the corporate security team has a solid grasp of its challenges and opportunities (Figure 13), and two-thirds (64%) do not think their team is more cautious about adopting AI than the rest of their organisation (Figure 14). This does not chime with interviews and industry discussions, which suggest lower levels of knowledge about AI and its application to corporate security. This over-confidence is concerning because it could hamper the adoption of AI, putting corporate security functions at risk of being left behind within their organisations.

Figure 13
Our team has a solid grasp of the challenges and opportunities of AI

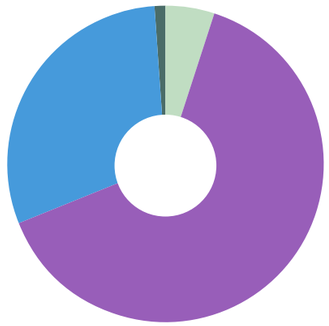
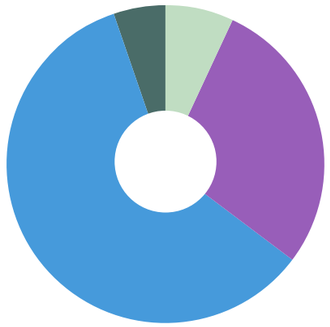


Figure 14
Our team is more cautious about adopting AI than the organisation as a whole



CSOs from MNCs

Technology and jobs

> *We still have a lot of opportunities to reduce low-grade jobs that would be better done by a machine. One of the things holding us back is the lack of skillset within middle management to identify these opportunities.*
>
> — CSO

In the short term, CSOs do not anticipate that emerging technology will have a significant impact on jobs. In fact, most are increasing or holding their team size constant. In the medium term, it is inevitable that headcount will reduce as routine tasks are automated. While corporate security will have to adjust to this, skilled security leaders will use their influence to maintain sufficient capacity, and use the AI efficiency gains to free up time for higher-value contributions to the business.

Talent is critical to effective technology adoption

Talent strategy is critical to corporate security's ability to harness the opportunities of emerging technology, and **CSOs rank 'insufficient technology and digital skills within corporate/physical security' as the second biggest obstacle to the effectiveness** of the function.

A tiny minority (13%) of CSOs themselves have specialist technology skills, such as software engineering, data science, software development, machine learning engineering, agile coaching, UX/UI, or coding. There are **higher levels of specialist skills among corporate security staff** more widely, however. According to a 2024 SI Placement/Clarity Factory survey, almost half (49%) of respondents across the function said they have specialist technology expertise.[23]

As emerging technology develops and becomes more user friendly, **it will become less important for corporate security functions to have specialist technology skills, and more important that team members are tech confident and curious**, and are

willing to explore how technology can enhance the work of the function.

> *"You need a translator to help you understand and articulate your user requirements and talk in tech terms that technology colleagues or vendors can understand."*
>
> — CSO

Effective technology adoption rests on three talent needs:

- **Technology confidence and curiosity:** Corporate security teams need a critical mass of personnel who are confident enough to explore opportunities - and to risk failing - before they find the the best solution. Those without this capacity will struggle. As one CSO told us: '*One of the things holding us back is the lack of skillset within middle management to identify these opportunities.*' Leading CSOs are creating working groups, setting team AI challenges, and setting aside time in team meetings to share ideas about using AI.
- **Project management skills:** Integrating new products and services effectively requires strong project management skills.
- **Technology translators:** Corporate security teams need interlocutors who can connect with internal technology colleagues and external vendors to communicate use cases, manage communications, and translate between needs and currently available solutions. These individuals do not need to be members of the corporate security team.

Two-thirds of CSOs and their teams have access to specialist training on AI. One CSO described how he has gone about upskilling his team (see Digital Development case study).

Digital development
Case study

> *"If you don't incorporate digital upskilling, you'll get left behind."*
>
> — CSO

The CSO from a FTSE 50 company has established a mandatory training and development programme for the corporate security team to upskill and put new-found skills and knowledge to immediate use.

- Team members take 3-hour, company-wide Microsoft training packages on Copilot, provided to the company by Microsoft at no cost to the security team. The training covers topics such as AI and large language models, and Power BI.
- At the end of each module the team member is assigned a mini project, giving them the opportunity to put their training to use to solve an immediate real-world problem. This might include writing an intelligence report, conducting data analytics, creating a site remediation plan, or producing a policy document.

The CSO commented: '*I sold it to them as a unique opportunity for us to get ourselves fit for the future. If you don't incorporate digital upskilling, you'll get left behind.*'

The benefits include faster report turnaround, the ability to process larger quantities of data, and greater insight. The CSO anticipates cost reductions, including through reduced analyst headcount.

The CSO has also established a digital working group to scope specialist technology-related training needs for different roles.

10. Global Security Operations Centres (GSOCs)

"We wanted to close the gap between incidents and response, support our businesses, and take advantage of technology that we weren't using to its full effect. The only way to do that is having an ops centre that can ingest the data."

— CSO

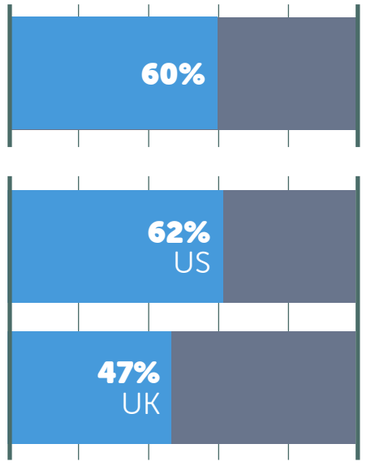
A majority of CSOs have a 24/7 GSOC – a central hub that draws on multiple data feeds to monitor, analyse, and respond to incidents globally (Figure 15).

GSOC delivery models are evenly spread between those staffed in-house, by vendors only, and by a combination of the two.

In a volatile global business environment, many CSOs have come to regard GSOCs as an essential tool.

GSOCs in numbers

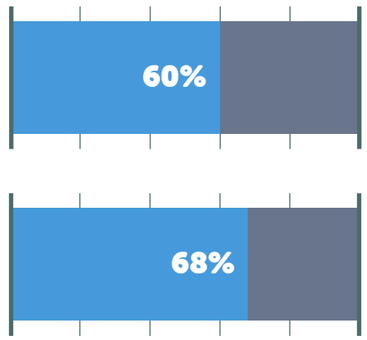
GSOCs



60% of CSOs have a GSOC.

US CSOs are more likely to have a GSOC than UK CSOs.

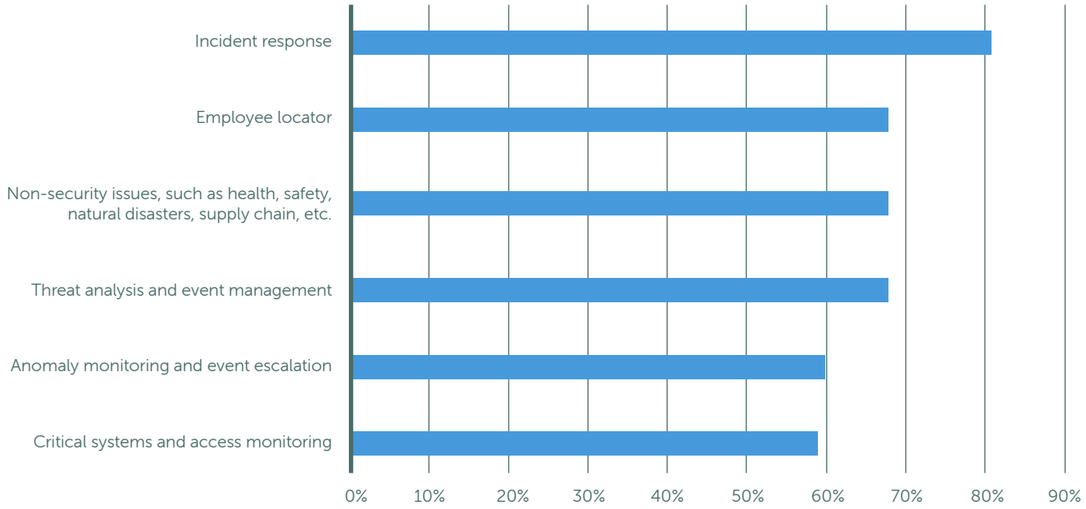
Personnel



At least 60% of GSOCs are involved in **incident response, employee locator, threat analysis, anomaly monitoring, and event management.**

Two-thirds of GSOCs are **involved in non-security issues,** making them a wider business asset.

Figure 15
GSOC activities
CSOs from MNCs



AI adoption is increasing within GSOCs and is likely to impact in a number of ways:

- the ability to process significantly **increased levels of data;**
- the ability to combine many **more data sources** from across the business to drive insights that are currently invisible;
- **enhanced visualisation** tools to make data more accessible and consumable to a business audience; and
- **automation** of tasks and **reduced headcount.**

11. Corporate Security Teams

"The biggest challenge I face is building a team of all the talents to enable us to face today's security challenges head on."

– CSO

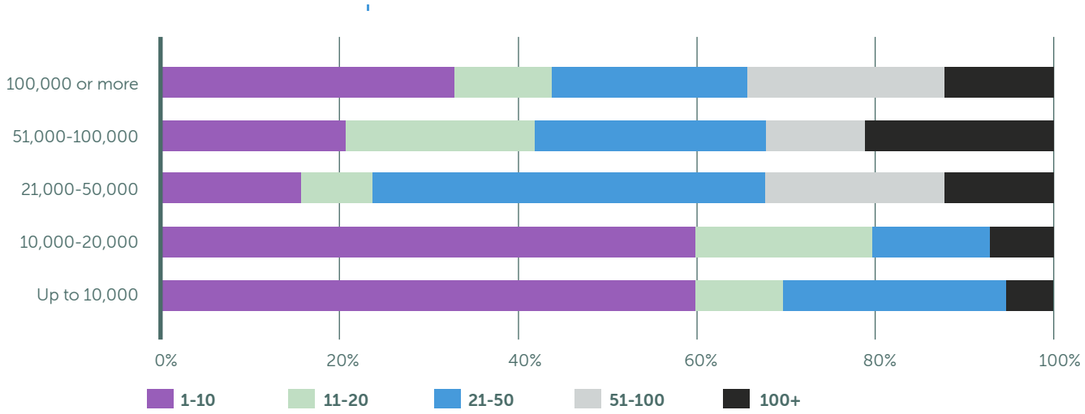
Size of team

The median corporate security team for multinational corporations is 11-20 people, but there is a very wide range of team size. This is due to the fact that the scope of responsibilities varies considerably and corporate security staffing needs will varying according to risk profile.

There is a **loose correlation between team size and company size.** One-third of companies with more than 20,000 FTE global headcount have corporate security teams with more than 50 FTE members (Figure 16).

Figure 16
Security team FTE by company headcount

CSOs from MNCs



Areas with increased staffing

CSOs are increasing staffing in the following areas:

- Intelligence
- Regional security roles
- Insider threat and investigations
- Executive protection and event security

This underlines some of the most significant trends: heightened geopolitical risk leading to investment in intelligence and regional security roles; increased insider risk; and a rise in attacks on executives, buildings, and corporate assets.

61%

of CSOs ranked 'finding multifaceted candidates' as their most important recruitment challenge.

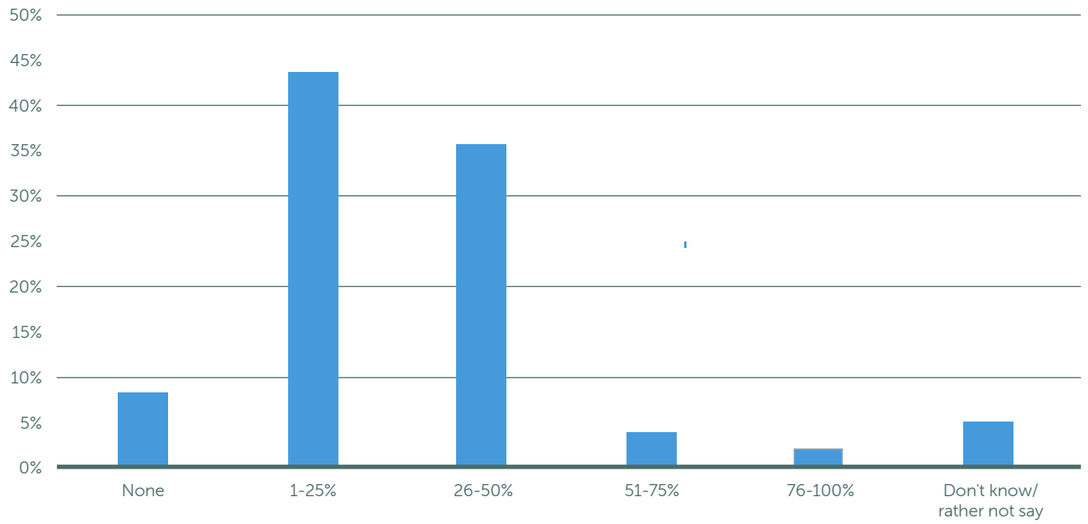
Low gender diversity in corporate security

Gender diversity remains low within corporate security. Only **6% of CSOs have achieved gender parity, 8% have teams without women, and almost half have teams with less than 25% women** (Figure 17). Larger companies are less likely to have teams that contain no women, but gender parity becomes less likely as company size increases.

CSOs ranked 'finding multifaceted candidates (skills, backgrounds, experiences, demographics)' as their most important recruitment challenge, cited by two-thirds (61%) of CSOs. CSOs articulated the benefits of mixed teams in terms of analysis and decision making.

Figure 17
Proportion of women on the corporate security team

CSOs from MNCs



Gender diversity is increasing

Data from a 2024 SI Placement/Clarity Factory survey suggests that gender diversity in corporate security is improving across generations. Whereas only 14% of survey respondents aged 45-years and over were women, those under 45-years made up more than one third.[24]

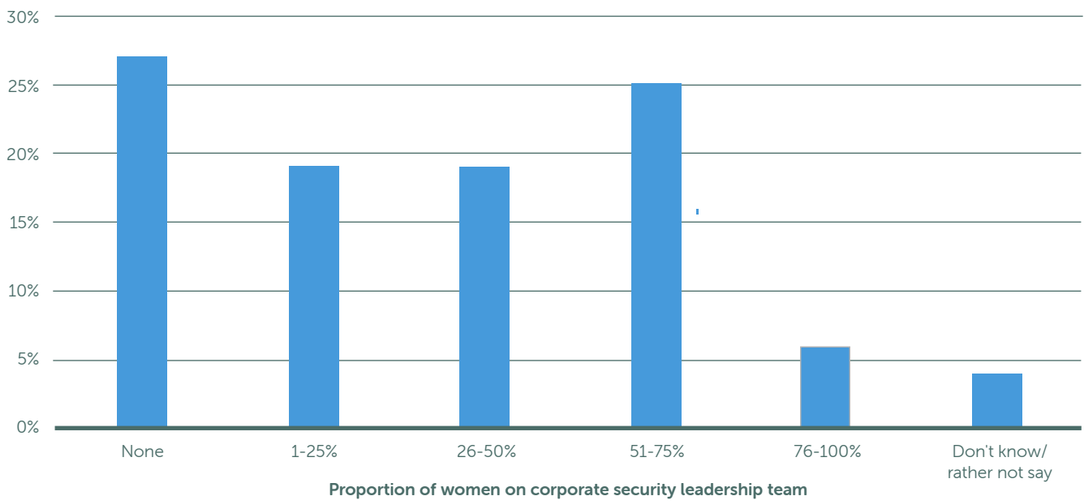
Low female representation on corporate security leadership teams

Female representation is lower at leadership level than it is across the team. More than **one-quarter (27%) of CSOs have no women on their leadership team, and only 6% have achieved gender parity** (Figure 18). There was no meaningful correlation between leadership gender and company size/headcount.

Figure 18

Proportion of women on corporate security leadership team

CSOs from MNCs



Prior government service dominates the career backgrounds of CSOs

> *It's not fair to say you shouldn't hire people from law enforcement. You should hire people that are comfortable with change and understand their purpose, wherever they come from. They must have the full range of soft skills relevant to the role.*
>
> — CSO

A majority (84%) of CSOs from multinational corporations have served in the military, law enforcement, or government intelligence. Data from a 2024 SI Placement/Clarity Factory survey suggests that younger recruits are coming from a wider range of backgrounds. A slim majority (59%) under 45-years have former public service experience.[25]

Most of the CSOs we interviewed are keen to diversify the backgrounds, experience, and expertise on their team because they believe that multifaceted teams are better placed in a complex and volatile business operating environment.

This is not a vote *against* a public service background, more a desire to select based on competencies rather than previous employment.

Outsourcing is a significant trend within corporate security

Almost half of CSOs outsource up to a quarter of the roles within their team, excluding guarding (Figure 19).

Larger companies outsource a smaller proportion of roles, although 11% of those with 100,000+ staff have corporate security teams that are more than three-quarters outsourced (Figure 20).

Figure 19

Proportion of corporate security roles that are outsourced, excluding guarding

CSOs from MNCs

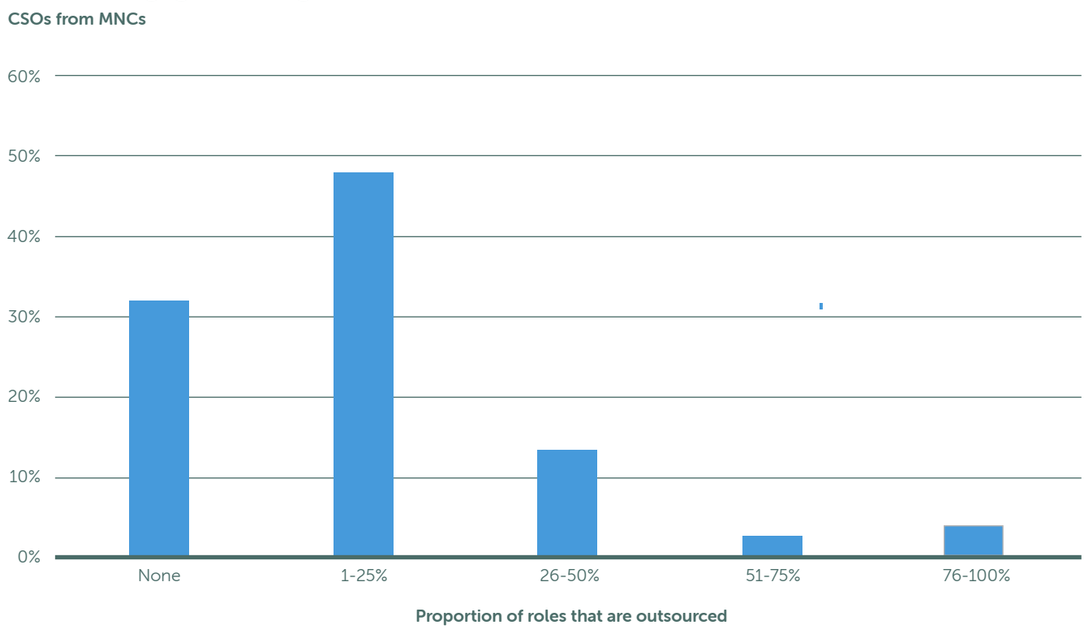
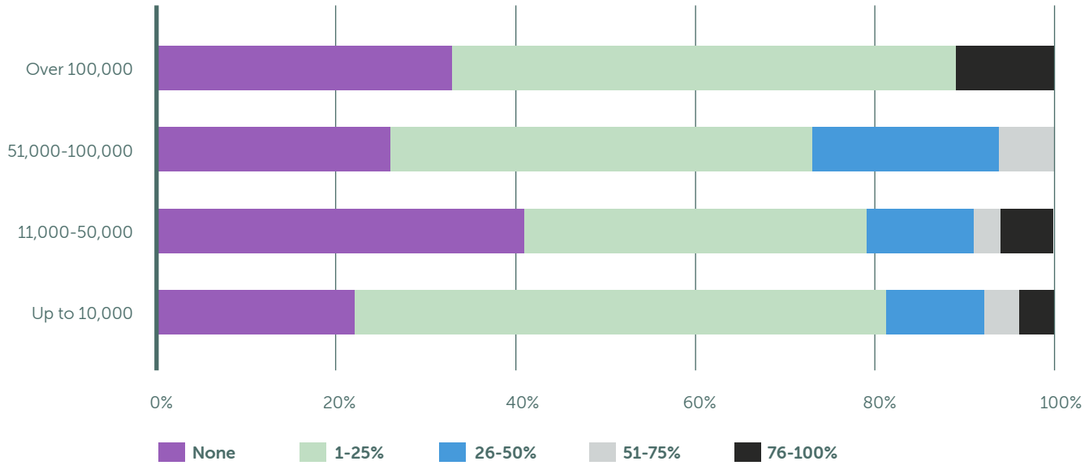


Figure 20

Level of outsourcing by company size/headcount

CSOs from MNCs



CSOs outsource a wide range of roles

Among CSOs that outsource roles within their team (Figure 21):

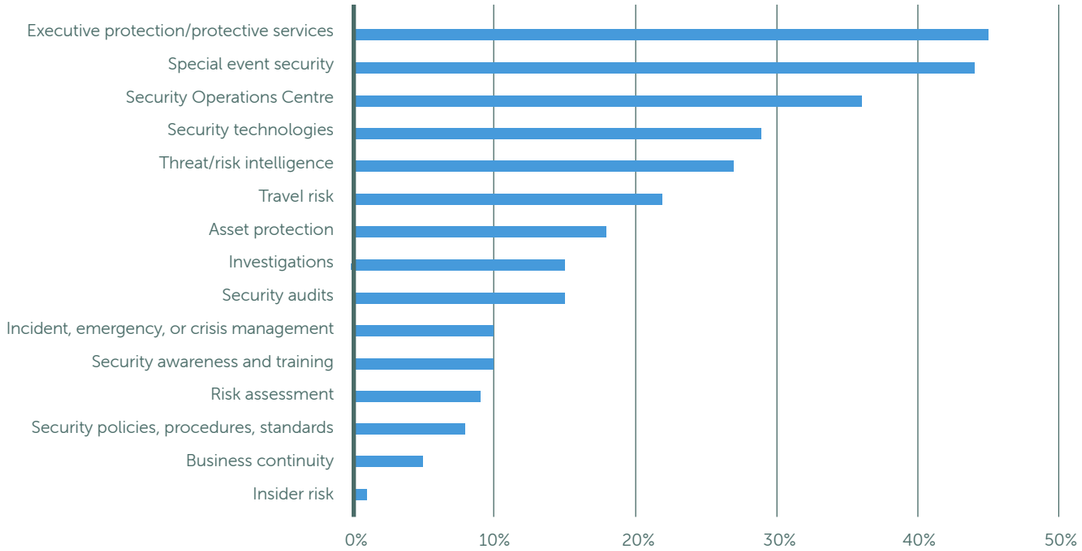
- Almost **half (45%) outsource executive protection/protective services and special event security roles.**
- **One-third have security operations centres staffed by outsourced roles.**
- **More than one-quarter outsource intelligence roles,** where those roles either sit within vendors or are embedded team members.
- Outsourcing is concentrated in key essential areas of the function's work: **executive protection, special event security, security operations**

centres, security technologies, threat and risk intelligence, and travel risk.

- Advances in **technology and AI** are likely to impact these trends in future years.
- Key processes of **operational resilience – business continuity and incident, emergency, or crisis management – remain firmly in-house.**

Figure 21
Corporate security roles that are outsourced

CSOs from MNCs



12. Talent

> *"The struggle for corporate security is getting people to think of us more intentionally rather than as an afterthought. We must work hard on our internal brand equity."* – CSO

Executive competencies

We asked CSOs to choose the most important executive competencies they are looking for in their team (Figure 22).

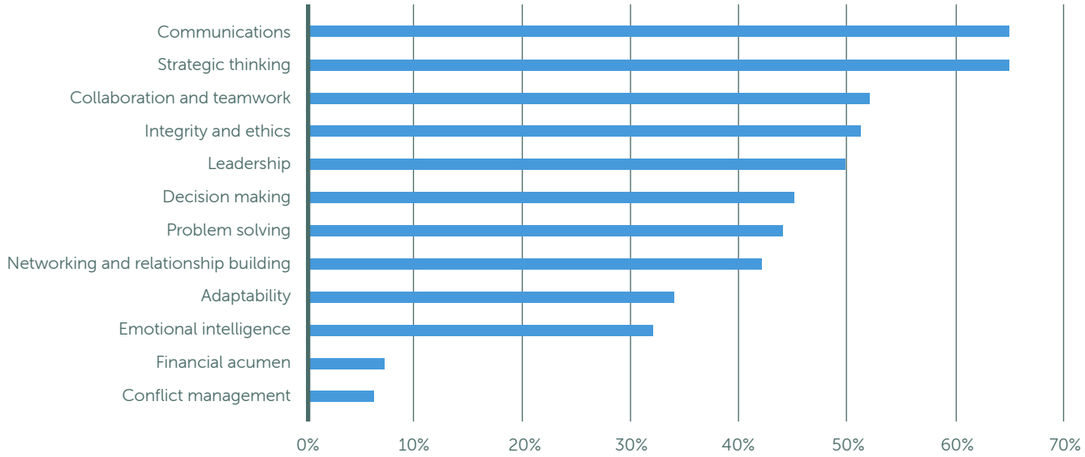
Top 5 executive competencies for corporate security teams:

1. Communications
2. Strategic thinking
3. Collaboration and teamwork
4. Integrity and ethics
5. Leadership

Figure 22

Executive competencies for corporate security

CSOs from MNCs



Communication is critical to success

Corporate security teams that lack effective communication skills run the following risks:

- **Inadequate resources:** If business leaders don't understand the value of corporate security, CSOs won't get the resource to deliver a robust service.
- **Gaps in provision:** If business colleagues don't understand the need to partner, CSOs will fail to plug gaps or deliver a holistic security service.
- **Inefficiency:** If corporate security teams can't communicate with one another, they will duplicate efforts, fail to share information, and waste time.

Low business leader understanding of security

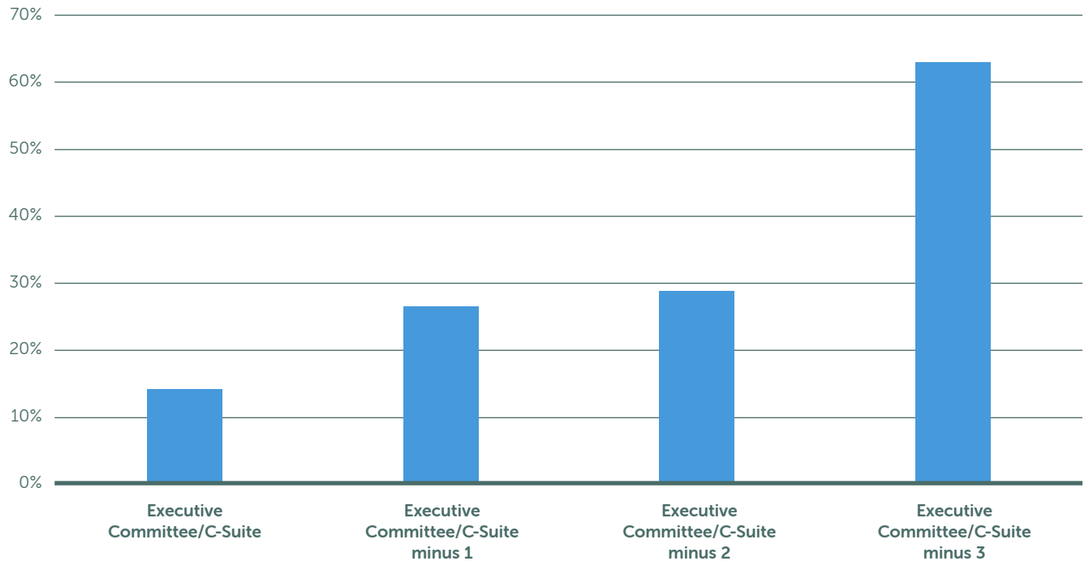
Almost one-third of CSOs scored 'low understanding of security among business leaders' as the top obstacle to the effectiveness of the function (excluding budget and headcount).

The longer a CSO's reporting line to the Executive Committee or C-Suite, the more likely they are to see low understanding among business leaders as a challenge (Figure 23).

Figure 23

Low understanding of security among business leaders is the most important obstacle to the effectiveness of corporate security

CSOs from MNCs, by proximity to Executive Committee or C-Suite



The power of storytelling

A CSO's most important role in today's complex and volatile business environment is that of storyteller. Their communication objective is not to help business leaders understand what the function does, its processes, responsibilities, and activities. Instead, they must communicate to build trust and influence, conveying meaning, impact, and value-add in terms that senior leaders will understand.

As Manish Mehta of Ontic told us: '*The C-Suite executives I've met understand enough about what physical security does. What's critical is that CSOs tie the work of their function to the business, what it cares about, and its unique vernacular. Rather than educating senior leaders on the nuts and bolts of security, they need to link physical security to business objectives and strategy.*'

> *The human mind is a story processor, not a logic processor.*
>
> — Jonathan Haidt[28]

Storytelling is a form of communication that organises human experiences in a specific structure to illicit an emotional response. This makes it highly effective at building trust and influence and eliciting behaviour change.

Storytelling is now considered a non-negotiable skill for senior business leaders. As one leading expert put it: '*Telling a compelling story is how you build credibility for yourself and your ideas. It's how you inspire an audience and lead an organisation. Whether you need to win over a colleague, a team, an executive, a recruiter, or an entire conference audience, effective storytelling is key.*'[26]

> *Soft skills are arguably more important than subject matter skills because they define the way you interact with the business and how you are seen and perceived.*
>
> — CSO

Soft skills versus technical skills

The choice between soft skills and subject matter skills is, of course, a false one. In today's complex threat environment where security is delivered through partnership, soft skills – communications, empathy, teamwork, and problem-solving – are non-negotiable.

Corporate security functions cannot get the job done with technical skills alone. **CSOs ranked 'data and organisational silos' as the third most important obstacle to success;** they know they must collaborate within the team and across the organisation.

Soft skills are critical right from the top of the business. From 2007 onwards, boards prioritised social skills over competence in managing financial and material resources when hiring CEOs. They recognised that being able to read the balance sheet is of little use if you can't read the room in today's complex business environment.[27]

When hiring CSOs, Executive Committees and the C-Suite must emphasise soft skills and leadership, and impress upon CSOs the need to do the same in their hiring strategy.

Recruitment challenges

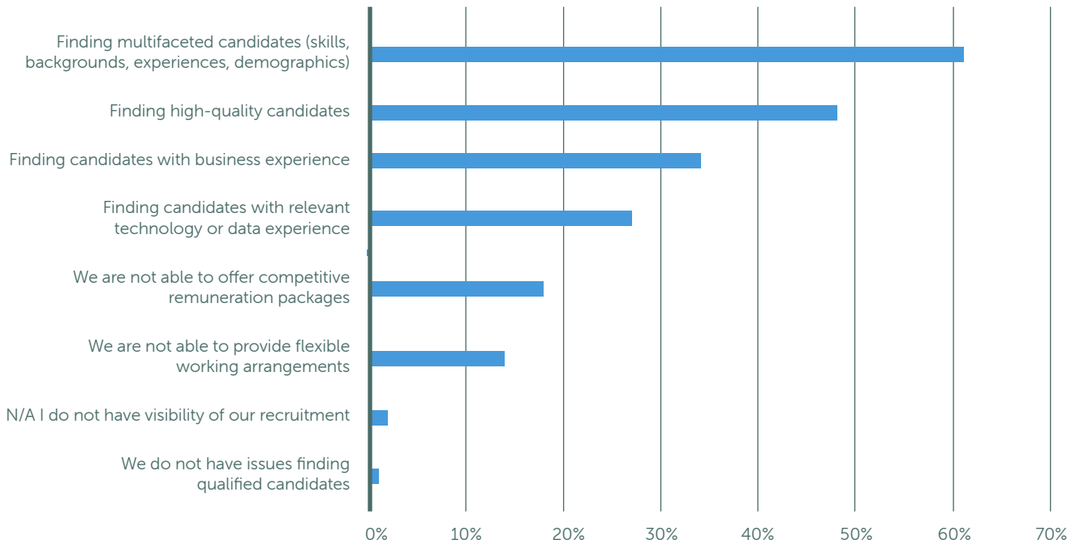
Finding multifaceted candidates, in terms of skills, backgrounds, experiences, and demographics, is the biggest recruitment challenge, cited by 61% of CSOs at multinational corporations. A large minority also struggle to find high-quality candidates and those with business experience (Figure 24).

There were few noticeable differences between US and UK CSOs, although US CSOs were six times more likely to struggle to find candidates with business experience than their UK counterparts.

Figure 24

Recruitment challenges

CSOs from MNCs



Development opportunities

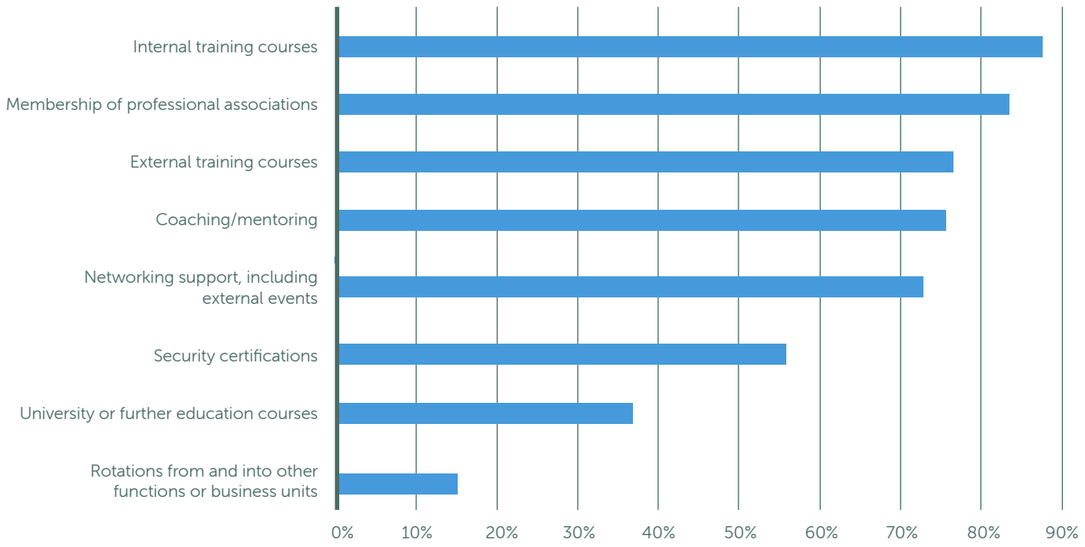
Almost all (93%) CSOs have a dedicated professional development budget, and offer a range of opportunities (Figure 25).

Given the importance of partnerships across the business, it is notable that only a small minority (15%) offer internal rotations. This would offer vital opportunities for corporate security professionals to learn first hand about how the business works, what it needs from corporate security, and how to partner effectively.

Figure 25

Development opportunities offered by corporate security

CSOs from MNCs



Professional or industry associations

Almost all CSOs (97%) belong to a professional or industry association and a large majority (84%) offer membership as a professional development opportunity for their team (Figure 25).

CSOs see many valuable benefits to membership (Figure 26):

- **Networking, conferences/meetings, and education and training** are the most important membership benefits.
- Only one-in-five CSOs consider **certification** a top membership benefit.

Figure 26

Useful benefits of membership of professional or industry associations

CSOs from MNCs

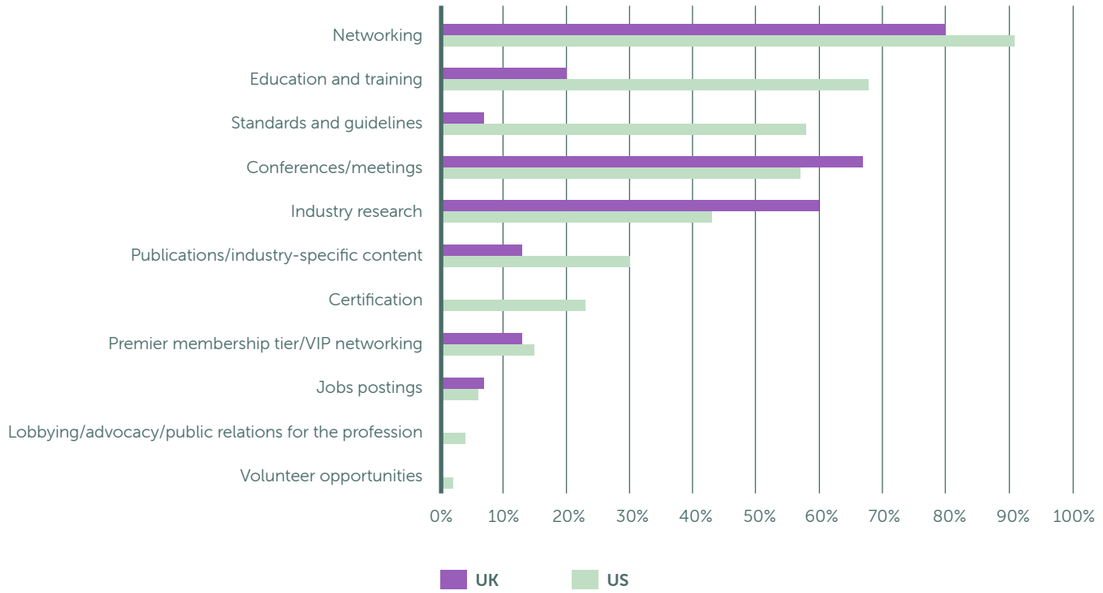
There are interesting differences between US and UK CSOs (Figure 27):

- **Education and training:** US CSOs are three times more likely to value it.
- **Standards and guidelines:** US CSOs are eight times more likely to value it.
- **Certification:** Selected by one-quarter of US CSOs but no UK CSOs.
- **Conferences:** US CSOs are more interested in conferences and industry research.

Figure 27

Useful benefits of membership of professional or industry associations

US and UK CSOs from MNCs



Appendix

Methodology

The 2025 CSO Survey was conducted between April and June 2025. It received 200 responses, 96 of which were from CSOs at international companies with more than 3,000 staff globally. The data referenced in this report refers to the dataset of 96 CSOs. The survey was open to all and anonymous. We also interviewed CSOs, representatives from sponsors, and industy experts.

The following individuals acted as members of the 2025 CSO Survey Advisory Council, informing and shaping the survey questions and analysis: Steve Brown, Alex Hawley, Wayne Hendricks, Charles Lacy, Joshua Levin-Soler, Duncan Manning, Kirsten Meskill, Jules Parke-Robinson and Derek Porter.

Partners

The 2025 CSO Survey is kindly sponsored by Ontic, ASIS International and Emergent Risk International. 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 offers a fascinating snapshot in time, but in the years that follow, CSOs will be able to track trends and understand important changes within our community. I hope the data will enable CSOs to finetune their programmes, benchmark their efforts, and make the business case for their work.

I would like to extend my sincere thanks to the companies who sponsored the 2025 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, and Emergent Risk International 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 the survey data, offered feedback, and 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 Steve Brown, Alex Hawley, Wayne Hendricks, Charles Lacy, Joshua Levin-Soler, Duncan Manning, Kirsten Meskill, Jules Parke-Robinson and Derek Porter.

I would like to thank the following people who helped in various ways, contributing their time, resource, ideas, and practical help: Scott Briscoe, Kat Brooks, Ryan Destefano, Kirsten Fields, Kelsey Gunderson, Jonesy (Scott Jones), Tim Kirkham, Carla Lochiato, Taylor Mansfield, Manish Mehta, Robin Welch Stearns, Bill Tenney, Meredith Wilson, Zander Wharton, and Erol Yalciner.

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

Tom Hampson (Hampson Studio) for his brilliant work bringing the data to life; Sophie Gillespie (Inkwell Communications & Design) for ensuring the report communicates clearly and succinctly; and Jo Sayer (Virtual Alchemists) for making everything work so effortlessly.

Finally, I would like to thank Paul and Dot for bringing joy.

All errors are, of course, my own.

Rachel Briggs OBE, 23 August 2025

Endnotes

1 'CrowdStrike outage explained: What caused it and what's next', *TechTarget*, 29 October 2024. www.techtarget.com/whatis/feature/Explaining-the-largest-IT-outage-in-history-and-whats-next

2 'Man charged with health insurance CEO murder to accept $300,000 in donations', *The Guardian*, 11 February 2025. www.theguardian.com/us-news/2025/feb/11/brian-thompson-shooting-accused-donations

3 'British Museum forced to partly close after alleged IT attack by former employee', *The Guardian*, 25 January 2025. www.theguardian.com/culture/2025/jan/24/british-museum-forced-to-partly-close-after-alleged-it-attack-by-former-employee

4 'Marks & Spencer Breach: How a ransomware attack crippled a UK retail giant', *BlackFog*, 7 August 2025. www.blackfog.com/marks-and-spencer-ransomware-attack/#:~:text=In%20April%202025%20Marks%20&%20Spencer,bare%20and%20fueling%20customer%20frustration

5 'Data Breach at Coinbase Exposes Information of Nearly 70,000 Customers', *Bitdefender*, 22 May 2025. www.bitdefender.com/en-gb/blog/hotforsecurity/data-breach-at-coinbase-exposes-information-of-nearly-70-000-customers

6 'A mistaken elevator, frantic emails and a run for help – how New York shooting unfolder', BBC News, 29 July 2025. www.bbc.co.uk/news/articles/cy85737235go

7 Global Risks Report 2025, World Economic Forum, 2025. www.weforum.org/publications/global-risks-report-2025

8 *The Business Value of Corporate Security*, Rachel Briggs, The Clarity Factory, 2023. www.clarityfactory.com/cso-value

9 *Global Risks Report, 2025*, World Economic Forum, 2025. www.weforum.org/publications/global-risks-report-2025

10 *Winning Today's Race While Running Tomorrow's*, PwC, 2023. www.pwc.com/mu/en/publications/ceo-survey-2023.html

11 *Corporate Security*, PwC, 2022

12 *Corporate Security*, PwC, 2022

13 'As the world shifts, so should leaders', Nitin Nohria, *Harvard Business Review*, July-August 2022. https://hbr.org/2022/07/as-the-world-shifts-so-should-leaders

14 *2022 Edelman Trust Barometer*, Edelman, 2022. www.edelman.com/trust/2022-trust-barometer

15 'Insider Threat: The shift from report to support', Megan Gates, *Security Management*, 1 September 2021

16 Global Risks Report 2025, World Economic Forum, 2025. www.weforum.org/publications/global-risks-report-2025

17 *The Business Value of Corporate Security*, Rachel Briggs, The Clarity Factory, 2023. www.clarityfactory.com/cso-value

18 Revolutionary Violence in the New Gilded Age, Insight Forward, 2025. www.insightforward.co.uk/wp-content/uploads/go-x/u/9623e58b-f566-43e4-93c1-814ae14316c5/Revolutionary-Violence-in-the-New-Gilded-Age.pdf

19 'The dark fandom behind CEO murder suspect', BBC News, 13 December 2024. www.bbc.co.uk/news/articles/cp8nk75vg81o

20 'Insider Threat: The shift from report to support', Megan Gates, *Security Management*, 1 September 2021

21 'Insider Threat: The shift from report to support', Megan Gates, *Security Management*, 1 September 2021

22 *Holistic Security: How physical and cyber security can join forces to strengthen operational resilience*, Rachel Briggs, The Clarity Factory, 2025. www.clarityfactory.com/holistic-security

23 *Corporate Security: Securing Future Talent*, Kathy Lavinder and Rachel Briggs, SI Placement and The Clarity Factory, 2024. www.clarityfactory.com/reports

24 *Corporate Security: Securing Future Talent*, Kathy Lavinder and Rachel Briggs, SI Placement and The Clarity Factory, 2024. www.clarityfactory.com/reports

25 *Corporate Security: Securing Future Talent*, Kathy Lavinder and Rachel Briggs, SI Placement and The Clarity Factory, 2024. www.clarityfactory.com/reports

26 'Storytelling can make or break your leadership', Jeff Gothelf, *Harvard Business Review*, 19 October 2020. https://hbr.org/2020/10/storytelling-can-make-or-break-your-leadership

27 'The C-Suite Skills that Matter Most', Raffaella Sadun, Joseph Fuller, Stephen Hansen and PJ Neal, *Harvard Business Review*, July-August 2022. https://hbr.org/2022/07/the-c-suite-skills-that-matter-most

28 *The Righteous Mind: Why good people are divided by politics and religion*, Jonathan Haidt, 2012. www.goodreads.com/book/show/11324722-the-righteous-mind

About The Clarity Factory

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

The Clarity Factory can help you in the following ways:

- **Holistic Security Maturity Assessment Scorecard:** Our digital assessment tool measures the maturity of the relationship between your physical and cyber security teams, delivers individual and team maturity scorecards, and offers a roadmap for improvement. www.clarityfactory.com/holistic-security
- **Storytelling for Security Leaders:** Security leaders must influence to get the resource they need to be effective. Our storytelling workshops and coaching, delivered with HumanStory, empower CSOs, CISOs, and their teams to communicate with clarity and influence at the executive level. www.clarityfactory.com/storytelling
- **Strategic Assessments:** We deliver tailored assessments of your function or an area of your work, drawing on industry data and benchmarking to help you prioritise investments. www.clarityfactory.com/strategic-assessments
- **Executive briefings:** Our CEO, Rachel Briggs, offers high-impact briefings, providing latest data and actionable insights. www.clarityfactory.com/briefings
- **Research studies:** Our original research offers deep insight into the challenges and opportunities facing security leaders. Our project Advisory Councils provide a space for peer learning among CSOs. www.clarityfactory.com/research

Sign up to our monthly newsletter
www.clarityfactory.com/subscribe

Get in touch
info@clarityfactory.com

Thinking ahead

The Clarity Factory Annual CSO Survey, 2026

Sponsorship opportunities

The Clarity Factory looks forward to working with thought-leading innovators within the security industry to deliver our **Annual CSO Survey, 2026**.

We are pleased to offer a range of sponsorship opportunities, starting from $6,500/£5,000. More information about the survey and sponsorship packages can be found at:

www.clarityfactory.com/annual-survey

The survey report will be published by The Clarity Factory in September 2026. This coincides with CSO budgeting and review cycles, so that our data can be used to inform decision making. It will be widely circulated through our networks, partners, events, and LinkedIn, and sponsors will be acknowledged in Clarity Factory presentations at industry events. We will host a virtual launch event, and will identify additional opportunities to share the survey with CSOs.

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

rachel.briggs@clarityfactory.com

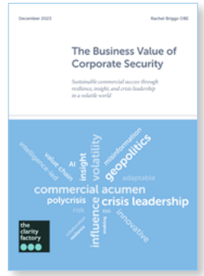
Other reports by Rachel Briggs OBE

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

The Clarity Factory, 2025

Connected Corporate Security: How to manage threats and risks with a unified model

The Clarity Factory and Ontic, 2024



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

The Clarity Factory, 2023

Corporate Security: Securing Future Talent

With Kathy Lavinder,
SI Placement and
The Clarity Factory, 2024

Cyber Security Leadership is Broken: Here's how to fix it

With Richard Brinson,
Savanti, 2022

the clarity factory

Annual CSO Survey, 2025

The past year has been challenging for corporate security: geopolitical volatility, threats to senior executives, growing insider risk, and sophisticated cyberattacks. The Clarity Factory Annual CSO Survey helps CSOs track trends and prioritise resources.

It offers three recommendations for 2026:

Prioritise partnership: Three-quarters of CSOs say silos and fragmented data hinder effectiveness. Build a partnership culture and champion discussions on geopolitical risk.

Invest in storytelling: Metrics are a management tool, not a communication technique. Executives' poor grasp of security is the function's biggest obstacle – but effective stories can generate compound interest for corporate security brand equity.

Tighten your talent strategy: Finding multifaceted candidates is CSOs' top recruitment challenge. Reprioritise social skills, foster 'technological curiosity', and stay connected to industry innovation.

Platinum partner

ONTIC

Gold partners

ASIS INTERNATIONAL
Advancing Security Worldwide®

EMERGENT RISK INTERNATIONAL

ISBN 978-0-99-702549-1

www.clarityfactory.com