Corporate Security: Securing Future Talent

'The business expects collaboration and alignment; we have to recruit for that mindset.'
Chief Security Officer (CSO) interviewee.

Key Insights Up Front

- The role of the corporate security function is evolving as a result of growing volatility and expanding security risks for multinational corporations.
- As risks converge, the C-Suite is demanding a more unified view of risk. Corporate security professionals are required to work flexibly within the function and across the organization, which makes the key skills of broad risk management, stakeholder engagement, and communication and influencing vitally important.
- Changing global operating environments impact corporate security talent needs, placing a premium on critical thinking and problem solving capabilities.
- CSOs are prioritizing business skills, and shifting away from traditional backgrounds.
- Digitalization, new technologies, and the incorporation of AI and Generative AI require strong technology skills and a broader innovation mindset.
- Organizations must adapt their talent strategies to attract a broader range of candidates from diverse backgrounds who have key business-critical skills.

The Corporate Security Function Evolves

The place and role of the corporate security function has changed. In a global operating environment characterized by volatility[1] and increased security risks, effective corporate security is now essential for commercial success. As a result, corporate security functions are growing in stature and size. Almost half (44%) of CSOs at multinational corporations expect to increase the full-time headcount over the next two to three years, and only one-in-ten (12%) think team size will decrease.

The C-Suite Expects a Unified Approach to Risk

Multinational corporations increasingly manage risks that are interconnected and span functions, and are dealing with multiple risks concurrently. Silos can result in missed opportunities, obscured risks, and blind spots.

Corporate security professionals are increasingly called upon to work collaboratively and flexibly across the function. Almost all (93%) survey respondents said they are expected to work fluidly across different areas of responsibility. As one CSO put it, 'You can't have people that only do one thing anymore; the board likes the fact that the team is agile. We need people who are able to 'lift and shift'.'

The C-Suite also expects risk professionals to collaborate cross-functionally to provide a unified risk response for the business: corporate security, cyber security, legal, compliance, brand protection, human resources, and external affairs, for example. As a CSO observed, 'The business expects collaboration and alignment; we have to recruit for that mindset.' The ability to do this is critical to success. One-third (34%) of CSOs cite 'insufficient interaction between security and other functions' as one of the top three challenges faced by their teams.

[1] *Global Risks Perceptions Survey 2022-2023*, World Economic Forum, 2023

This cross-functional approach to risk places a premium on three skills:

- **Broad risk management capabilities**: CSOs ranked this as the third most important skill that all members of the function should have, cited by 38% of CSOs (fig. 1). Risk professionals must share a common operating language and framework to be able to manage risks together.
- **Stakeholder management**: One-quarter of CSOs cited stakeholder management as a core skill for corporate security professionals.
- **Communication and influencing**: Three-quarters of CSOs rated this as a top-three skill. A CSO commented, 'It's not hard to find people who can do tasks. It's harder to find people who can integrate into the company and communicate effectively.'

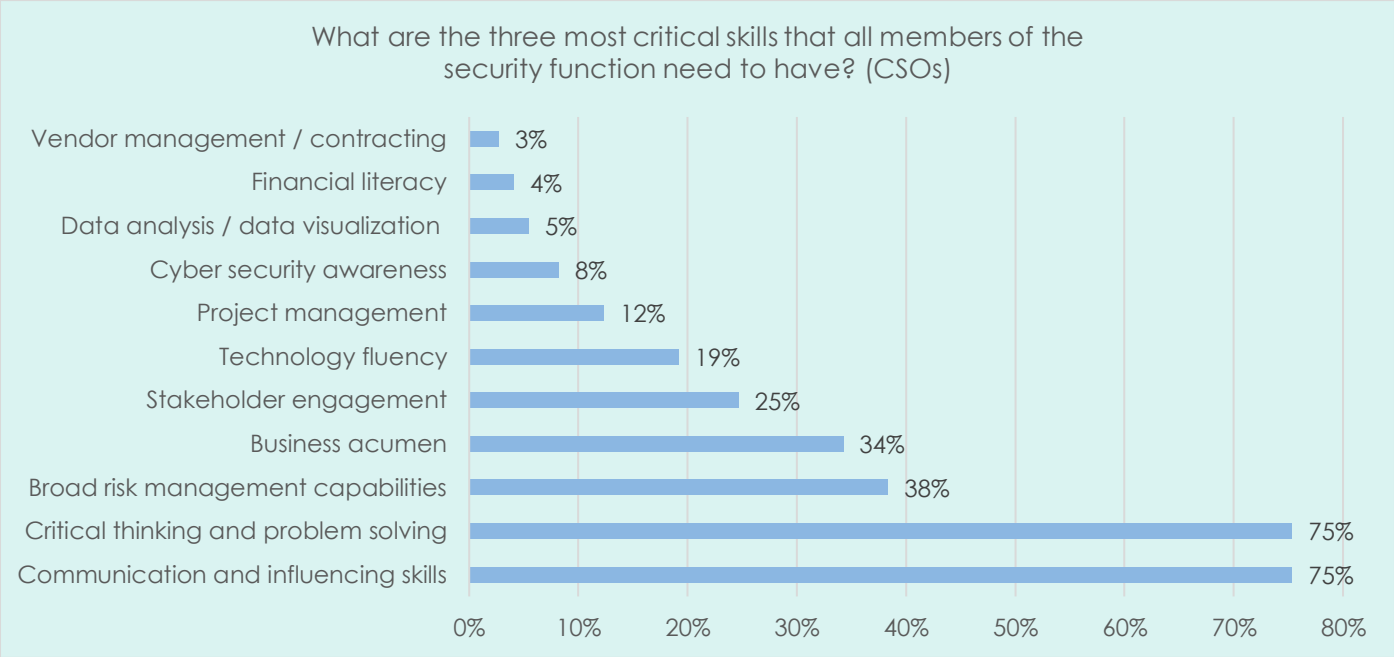

Figure 1: What are the three most critical skills that all members of the security function need to have? (CSOs at MNCs)

There is an emerging trend for corporate security professionals to have prior experience in another part of the company, which could enhance the function's ability to collaborate across the business and break down functional silos. Just below half (44%) of respondents 44 years and under have worked in another function, compared to 36% of the 55+ cohort and current CSOs. As one CSO put it, 'It brings different ways of thinking, better capability of dealing with gray areas, and understanding of the business.'

The 'Geopolitics' Effect on Corporate Security Talent

CSOs rank geopolitics as the most important factor influencing the function's talent needs. In a volatile world, critical thinking and problem solving skills are at a premium, and were ranked by CSOs as the most important skills for team members. CSOs were more than twice as likely to choose these skills (75%) than the next most popular option, broad risk management capabilities (38%) (fig. 1).

Corporate Security Functions are Diversifying – But Can Go Further

The 'diversity dividend' is critical in complex and fast-moving environments, where diverse perspectives enhance insights and improve decision making.[2] It is not surprising that CSOs are prioritizing diversity in their hiring practices. The majority of CSOs interviewed said it was one of their most urgent priorities, and two-thirds of CSOs surveyed (65%) ranked it as their top recruitment challenge. This was echoed by findings of an OSAC Women in Security (WiS) poll that found 92% of hiring managers are seeking diverse candidate pools.[3]

---

[2] See *Empowering Diversity, Equity and Inclusion in Corporate Security*, Rachel Briggs OBE and Paul Sizemore, The Clarity Factory, 2023, for further references on the diversity dividend.

[3] OSAC Women in Security survey, *Attracting, Retaining, and Empowering a Thirving Security Talent Pool*, which surveyed 158 people representative of WiS membership.

Our data shows diversity is increasing. The proportion of women 44 years and under (35%) was more than twice that in the 55+ cohort (15%) (fig. 2), and members of the younger age group are twice as likely as those 55 years and over to self-identify as having a physical disability (12% and 7% respectively) or being neurodiverse (12% and 6%).

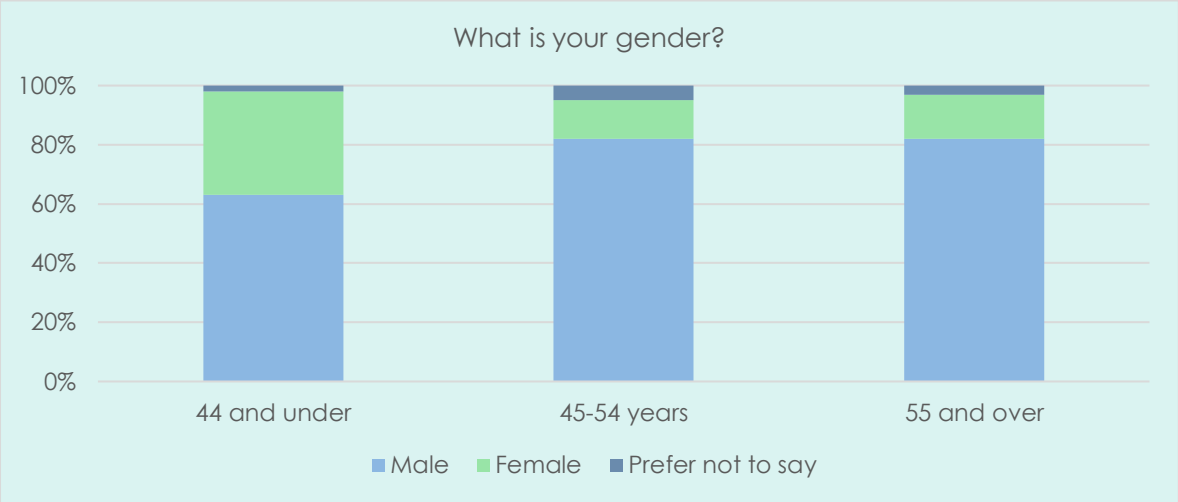

Figure 2: What is your gender? (all respondents by age)

There is considerable work to do on gender diversity:

- Almost half (49%) of CSOs have fewer than 25% women on their security team.
- Two-thirds (65%) of CSOs have fewer than 25% women on their leadership team.
- Only 10% of CSOs have achieved gender parity on their leadership team.

Data on racial diversity suggests a backwards trend. Two-fifths (19%) of all survey respondents described themselves as 'being a member of a racial or ethnic minority community' within their country of residence, but this fell to 10% for those 44 years and under.

Changing Preferences for Experience and Background

CSOs are reassessing the balance between business experience and security subject matter expertise in light of the imperative to work cross-functionally and align with the business. A majority of CSOs (62%) agree that 'business/organizational skills are more important than security subject matter expertise'. As one CSO commented, 'We take a threat-led, risk-based approach; it means we look for the right individual rather than someone who has long subject matter expertise experience.'

There is a significant generational divide in attitudes about whether public sector experience is essential to being an effective corporate security professional. Survey respondents 55+ were four times more likely (61%) than those 44 years and under (16%) to agree that this background is essential, and the younger cohort differed significantly from all age groups and CSOs on this issue (fig. 3).

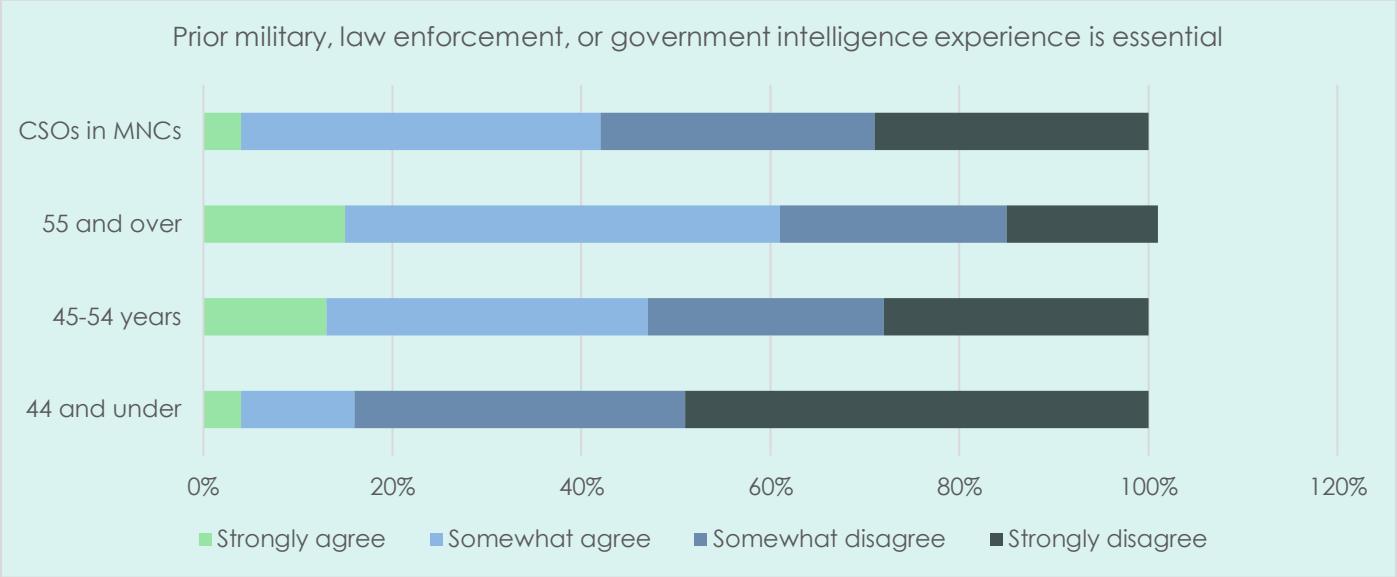

Figure 3: Prior military, law enforcement or government intelligence experience is essential to being an effective member of a security team (all respondents by age, and CSOs at MNCs)

Our survey shows a marked trend away from government career backgrounds among younger corporate security professionals. While 80% of those 55+ come from this background, this drops to 59% for those 44 years and under (fig. 4).

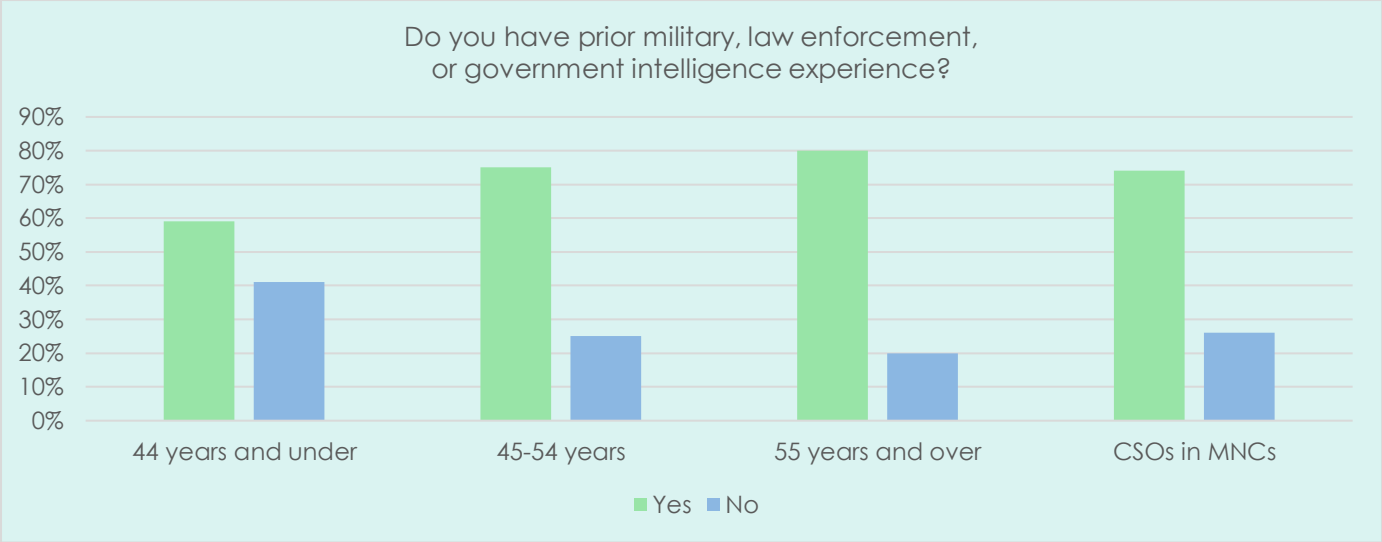

Figure 4: Do you have prior military, law enforcement, or government intelligence experience? (all respondents by age, and CSOs at MNCs)

Technology is Influencing Corporate Security Talent Needs

CSOs are increasingly reliant on technology. A large majority of CSOs said they expect technology spending to represent a growing proportion of the overall security budget over the next two to three years, and two-thirds (68%) have started to work with AI and Gen AI.

Technology is influencing corporate security talent needs. CSOs ranked it as the second most important factor, selected by 51% of CSOs. One-third (33%) said that 'insufficient technology and digital skills' is one of the top three challenges facing the function, and the same proportion (29%) said 'finding candidates with relevant technology, data, or cyber security experience' was one of their top recruitment challenges.

CSOs are accelerating recruitment of personnel with technology skills. Almost half of those surveyed said they have team members with specialized technology expertise, such as software engineers, data scientists, developers, or machine learning engineers.

Corporate Security Recruitment Best Practices

Finding candidates with the full range of skills, competencies, and experience is challenging. Just under half (42%) of CSOs have unfilled vacancies on their team, and one in ten (11%) have postings that have been open for six months or longer.

CSOs must change their approaches to recruitment if they are to find a broader and more diverse range of applicants that meet the function's shifting needs. If you want to be different, you have to do different.

We recommend eight changes CSOs should make to the recruitment process.

1. Prioritize the skills that matter most

Recruitment must align specialized subject matter expertise with the core skills that CSOs rank as most important. The following are now 'essential' rather than 'desirable' skills: critical thinking and problem solving, broad risk management capabilities, stakeholder engagement, communications and influencing, and technology competencies.

2. Seek a diverse range of perspectives and backgrounds

One dimensional teams are not appropriate in a complex and volatile operating environment. The most effective corporate security functions are those that achieve diversity across a range of vectors, such as gender, race, professional background, age, and outlook. Recruitment isn't just about finding the right 'person' for the job, it's about achieving benchstrength across the whole team. CSOs should consider whether a university degree is critical for all roles. If it is not, leaving it in as a requirement limits the talent pool and hinders efforts to diversify.

3. Rethink job descriptions

Many CSOs we interviewed recognized they need assistance crafting job descriptions that properly reflect what's needed now and in the future, as opposed to what was important in the past.

Our own review of job descriptions across sectors, geographies, and roles shows that many documents are poorly written and hinder efforts to drive the kind of forward-looking talent strategy we articulate in this paper.

CSOs and hiring managers need to focus on six imperatives for effective job descriptions:

- **Create realistic and coherent roles**: Job descriptions too often combine numerous roles and responsibilities, creating the challenge of finding purple unicorns.
- **Focus on skills and competencies rather than specific work experience**: Many job descriptions still specify that candidates should have specific work experience or length of tenure. Instead, spell out the skills, competencies, and qualities needed to be effective in the role.
- **Distinguish between 'essential' and 'desirable' skills and experience**: Most CSOs say that many roles can be learned on the job, but most job descriptions do not reflect this, thereby limiting the candidate pool.
- **Use gender neutral language**: 90% of respondents to the OSAC WiS survey said the language in job postings influences whether or not they apply. Using gender neutral language can broaden the candidate pool.
- **Keep job descriptions updated**: Roles, functional missions, and expectations change over time. It is vital that job descriptions reflect this. Some CSOs go as far as deleting all prior versions from company servers.
- **Tailor descriptions to the role and organization**: Job descriptions must be tailored and avoid generic, broad or vague descriptions.
- **Avoid jargon**: Write clearly and succinctly what is needed in terms of experience and qualifications as well as responsibilities, and avoid language that will exclude candidates without government experience.

4. Diversify recruitment channels

CSOs mainly use three channels for recruitment, which tend to reinforce existing recruitment patterns: the internal talent acquisition team (78%), their own professional networks (68%), and LinkedIn (59%) (fig. 5).

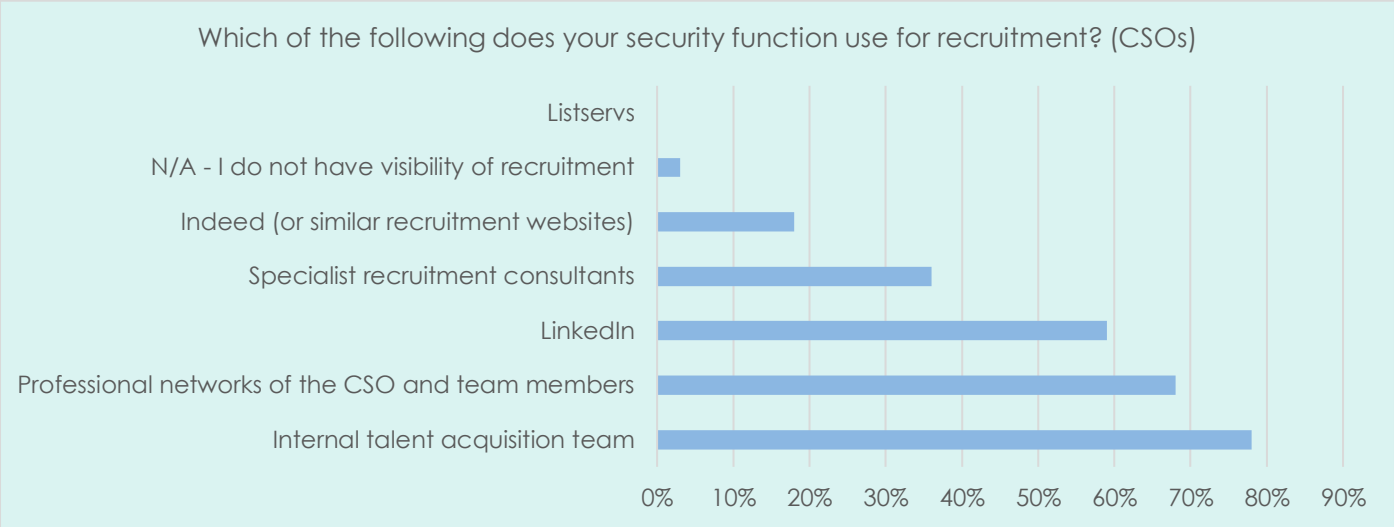

Figure 5: Which of the following methods does your security function use for recruitment? (CSOs at MNCs)

Each of these channels brings its own issues:

- **The internal talent acquisition team**: As the most utilized recruitment channel, some 42% of CSOs reported that internal acquisition teams do not understand their needs (fig. 6). A CSO told us, 'We have had to put a strong emphasis on training HR about what corporate security needs.' Often junior level talent acquisition specialists do not have a deep understanding of the corporate security function, which means they are unable to evaluate resumes with any degree of sophistication. These individuals often work across all functions and change jobs frequently.
- **Professional networks**: This taps into the "known network", usually those who have experience in the same circles as the hiring managers.
- **LinkedIn**: This platform only taps into active candidates. It misses out on many passive candidates who are not monitoring LinkedIn for jobs, do not use the platform regularly, or are not on LinkedIn at all.

CSOs should use a diverse range of recruitment channels, utilizing all of the above, along with specialized recruiters and broader professional networks to ensure roles are accessible to the widest talent pools.

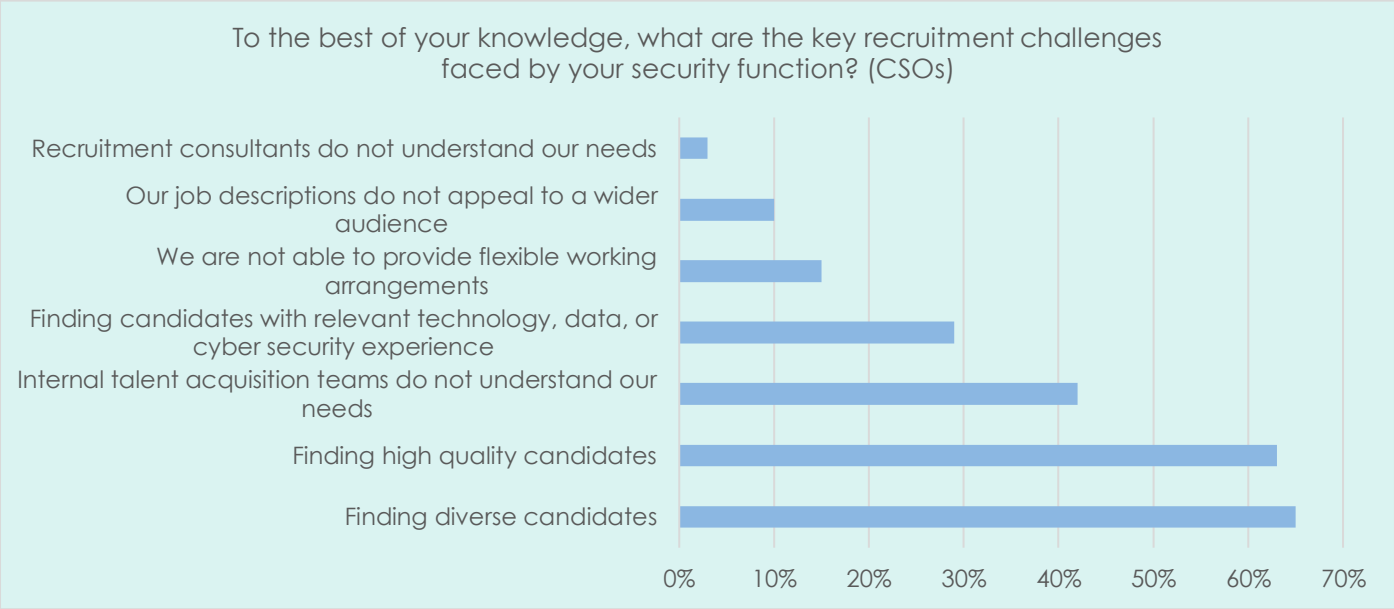

Figure 6: To the best of your knowledge, what are the key recruitment challenges faced by your security function? (CSOs at MNCs)

5. *Adopt a proactive strategy to achieve diversity*

CSOs report the most important recruitment challenge they face is finding diverse candidates, with 65% pointing to this (fig. 6). As the data on gender and professional background demonstrates, diverse candidates are in demand, and to be successful in attracting this limited talent pool, CSOs must have a concerted strategy. The most successful CSOs clearly articulate the diversity imperative and hold hiring managers accountable for this objective. Luck is not an effective strategy.

6. *Rethink job titles*

CSOs should be intentional with job titles, to avoid turning off diverse candidates or those who may not meet every requirement. They should also ensure titles reflect the responsibilities of the role. Even subtle shifts can dramatically broaden the talent pool.

7. *Revise resume review and interview processes*

CSOs must incorporate best practices, such as:

- Remove names from resumes to ensure a neutral review process.
- Train team members on how to conduct interviews professionally and consistently.
- Teach those involved in interviews about implicit bias.
- Use interview panels, including colleagues from outside the security function, to prioritize core business skills alongside security knowledge.
- Focus on qualities, competencies, and skills rather than prior work history. As a CSO told us, 'Character and competencies are critical – the rest is teachable.'

8. *Be mindful of generational change*

Today, leaders can find themselves managing across four generations. One in five (22%) CSOs said 'generational change within the workplace' is one of the key factors influencing their talent needs over the next two to three years. As organizations seek to attract diverse and qualified candidates, including those with technology skills, it is important that roles appeal to the next generation.

Only a slim majority (54%) of CSOs think security is an attractive career option for young people (fig. 7). Security professionals under the age of 45 years are seven times more likely to strongly disagree that it is an attractive option (20%) than CSOs (3%). CSOs must ensure their talent strategies, job descriptions, and working styles keep pace with the expectations of the next generation.

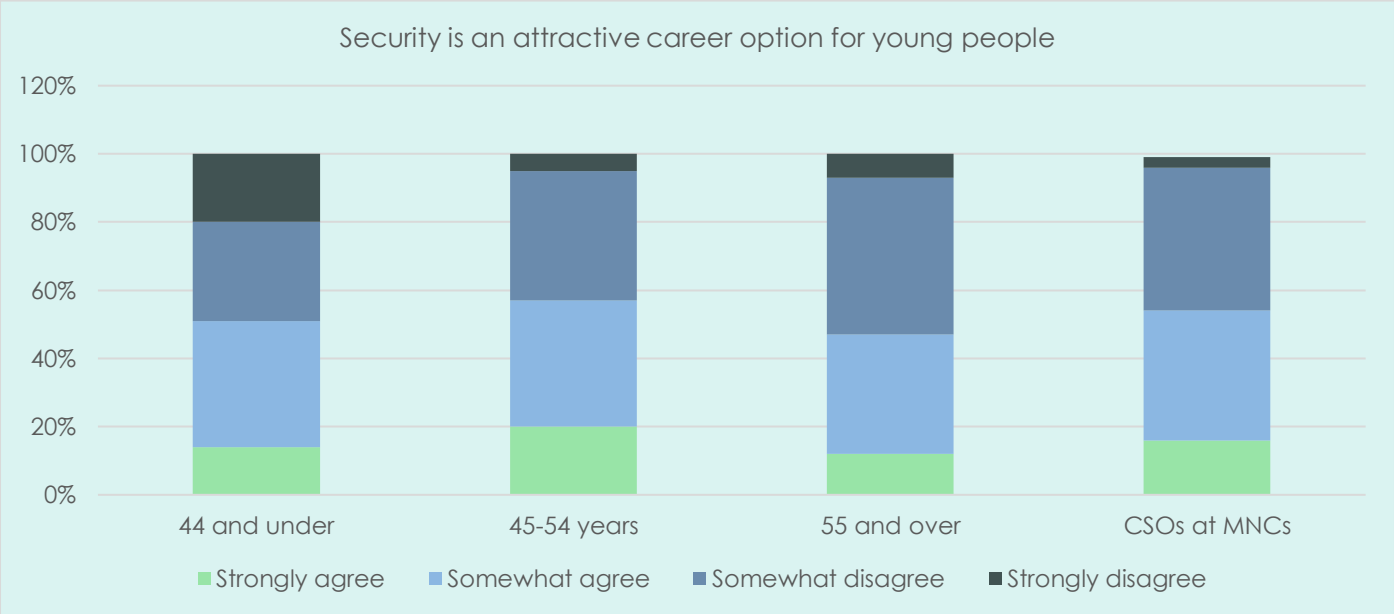

Figure 7: Security is an attractive career option for young people (all respondents by age and CSOs at MNCs)

Recommendations for CSOs

- Refresh your talent strategy to ensure it meets your needs for the future.
- Prioritize the skills that matter most: critical thinking and problem solving, communication and influencing, stakeholder engagement, broad risk management capabilities, and technology competencies.
- Be proactive in your approach to attracting a diverse talent pool.
- Reevalute job descriptions.
- Diversify your recruitment channels to maximize exposure to a broader range of candidates.
- Revise resume review and interview processes to eliminate implicit bias and ensure screening prioritizes competencies rather than backgrounds.
- Stay focused on generational change to future-proof your talent strategy.

About the Authors and Partners

Kathy Lavinder is Founder and Executive Director of SI Placement
Rachel Briggs OBE is Founder and CEO of The Clarity Factory

SI Placement is the premier retained recruiting firm operating in the security arena. With more than 20 years' experience and a proven track record for assisting multinationals and the family offices of the high-net-worth community with critical talent needs, SI Placement has a unique window into the needs and concerns of complex organizations.

The Clarity Factory consults with major multinationals, producing knowledge, actionable insights, and practical solutions to drive innovation in corporate security and cyber security.

SI Placement and The Clarity Factory offer a range of joint services to assist CSOs with their talent strategies. This includes: talent audits, future talent strategy facilitation, staff development and training, compensation reviews, job description reviews, and advice on recruitment needs.

To discuss how SI Placement and The Clarity Factory can assist you, please contact Kathy Lavinder or Rachel Briggs.

About the Study

This insight draws on research conducted by SI Placement and The Clarity Factory in 2024, including interviews with CSOs from a range of sectors and geographies, and a global survey of corporate security professionals. The survey data for CSOs quoted in this insight relates to CSOs from multinational corporations. Where survey data is broken down by age, it draws on all survey respondents. More information on this study can be found here.