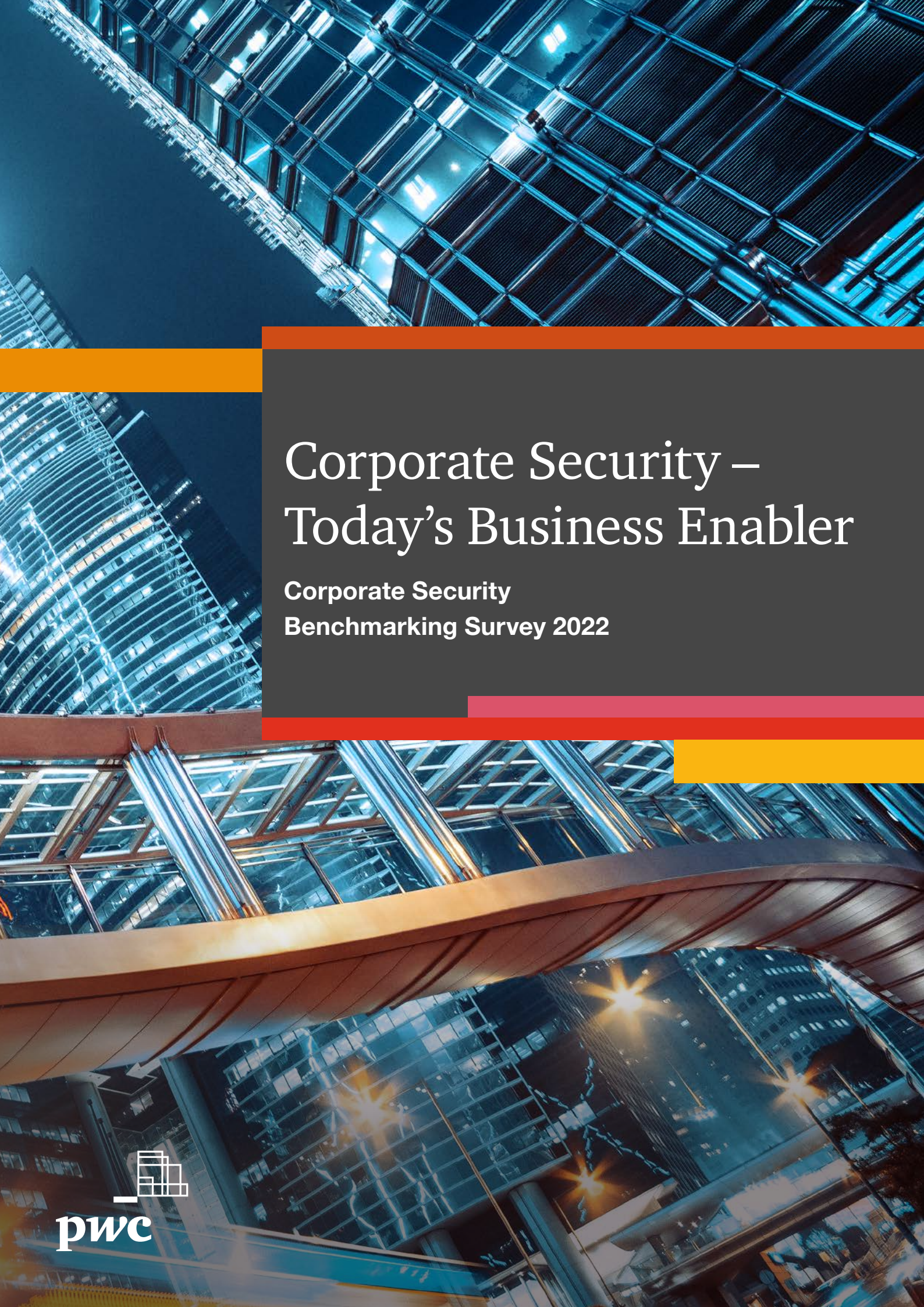


Corporate Security – Today's Business Enabler

Corporate Security Benchmarking Survey 2022

pwc

Context

Organisations have always relied on a security function of some description to protect their vital assets. Over time, however, the Corporate Security function, or equivalent (henceforth referred to as Corporate Security) has undergone a profound shift, moving from the more traditional 'guards, guns and gates' model to encompass security threats which go beyond the purely physical, overlapping with other disciplines such as 'Cyber Security'.

Since Corporate Security's work involves proactively mitigating security risks and averting threats, a lack of visibility has generally been an indicator of success, contrasting with most other functions, where good performance leads to overt recognition.

While Corporate Security may operate less conspicuously, its contribution to the organisation should not be underestimated. It has been on an upward trajectory in recent times, playing an active role in helping businesses to negotiate a number of major crises, including the pandemic, escalating global conflicts or supply chain disruption, all of which have served as a timely reminder to the C-suite[1] about the value Corporate Security can add.

Amid a backdrop of heightening uncertainty and instability, the focus has shifted once again onto the future role of Corporate Security. As businesses grapple with a growing array of potential future threats, this is prompting a fresh re-think about how Corporate Security needs to adapt to a new context.

This paper aims to generate a wider discussion about the importance of Corporate Security and how it can enable and sustain businesses to rise to the challenges they face. Based on these findings, readers can assess the extent to which the common perception gaps between C-suite and Corporate Security identified in the report may be applicable to them and respond accordingly.

As part of our analysis, we will explore:

- The degree of perception gap related to Corporate Security between the C-suite and Chief Security Officers (CSOs).
- The main identified perception gaps that organisations must address.
- Whether the C-suite sufficiently recognises the importance of Corporate Security.
- The current and future security challenges for Corporate Security from the perspective of two groups: the C-suite and CSOs.
- The degree of visibility of Corporate Security activities among the C-Suite.

1 The 'C-suite' designated target group is a collective category that includes different areas of responsibility. The participation criteria for the target group included persons from the areas of 'member of management, board of directors, C-suite'.

Survey approach

To better understand how perceptions of Corporate Security vary between CSOs and the C-suite, we conducted a survey with 150 individuals in May 2022. Respondents were evenly split between CSOs and the C-suite to ensure comparability between the two groups, who were asked the same questions. This survey brought together the views of businesses across 14 different industries, including manufacturing, consumer goods, healthcare, life sciences, and energy. Our findings consider the perspectives and experiences of a broad cross-section of organisations in terms of size, with respondents classified into three size categories: small (total revenue below €500 million [m] – 41% of respondents), mid-sized (total revenue between €500m and €1 billion [bn] – 34%) and large (total revenue above €1bn – 25%). The findings of the survey provide a further insight how the attitudes can vary depending on factors such as company size and industry.

Overview of the survey respondents

150 survey respondents

14 different industries

19% FMCG* companies

50/50 CSOs/C-suite

11% life sciences and healthcare companies

23% manufacturing companies

41% companies with a total revenue < 500m €

34% companies with a total revenue < 1bn €

25% companies with a total revenue > 1bn €

Disclaimer: the results reflect the beliefs and views of respondents at a particular moment in time, therefore, it is important to caveat any conclusions with an understanding that circumstances may have since changed.

*Fast-moving consumer goods

Key findings

Five major insights

1. The vast majority[2] (80%) of the C-suite and CSOs believe that Corporate Security is perceived as a business enabler through the entire organisation (35% of C-suite and 39% of CSOs responded with 'fully agree'; 41% of C-suite and 44% of CSOs responded with 'rather agree').

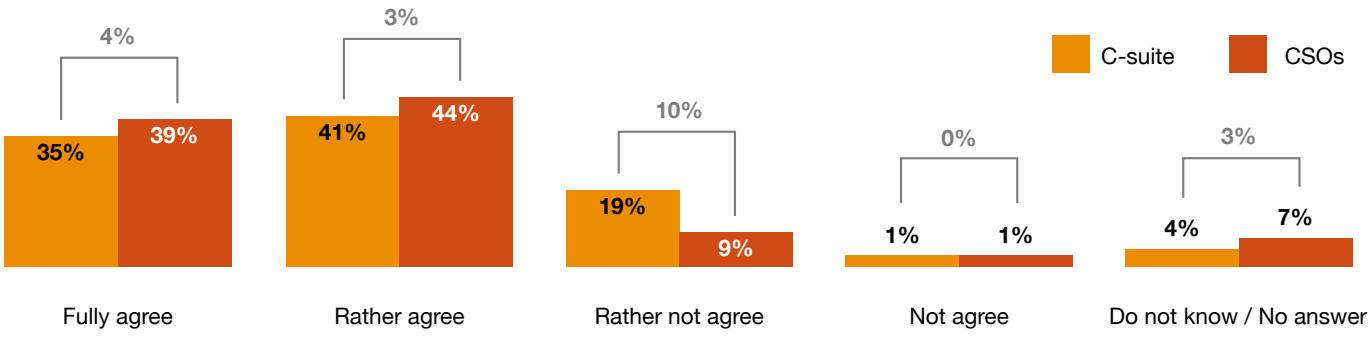
2. Almost half of the C-suite respondents (44%) and 53% of CSOs perceive the maturity of their Corporate Security function as 'established'[3].

3. Information Security is recognised as one of the main areas of Corporate Security that according to more than a half of the C-suite (60%) and 37% of CSOs needs to be improved. Cyber Security is considered to need additional skills and qualifications by 49% of C-suite and 40% of CSOs.

4. Survey participants identified the following top security challenges for the next five years as follows: Cyber-crime (78%), lack of resources (67%), and Supply Chain Security (67%). Almost half perceive geopolitics and political unrest as a challenge in the next five years.

5. The majority (69%) of C-suite and CSOs indicated that their Corporate Security Target Operating Model (TOM) setup is adequate for the challenges of modern times.

Do you believe Corporate Security is perceived as a business enabler through your organisation?



Corporate Security as a business enabler

37% of participants fully agreed with the statement "our Corporate Security function acts as a business enabler and makes a clear value contribution", while a further 43% selected the 'rather agree' option. CSOs were marginally more likely to believe their function is perceived as a business enabler throughout the organisation than their C-suite counterparts, recording a 4% and 3% higher figure on the 'fully agree' and 'rather agree' responses, respectively. Conversely, 19% of C-suite respondents selected the 'rather not agree' option.

One of the most significant outcomes of the survey is what it says about the perception of the value that Corporate Security adds to an organisation. CSOs tend to have higher estimation of the importance of the Corporate Security function compared to the C-suite, with 39% fully agreeing that the C-suite appreciates Corporate Security as a business enabler, compared to 35% of C-suite respondents. From this, we can infer a gap between CSOs' self-perception and the actual perception of the C-suite, highlighting a clear opportunity for CSOs to be more proactive in demonstrating their value and achievements.

2 Hereafter, when no separate data for CSOs and C-suite is introduced, the percentage presented is an average of the responses by both groups.

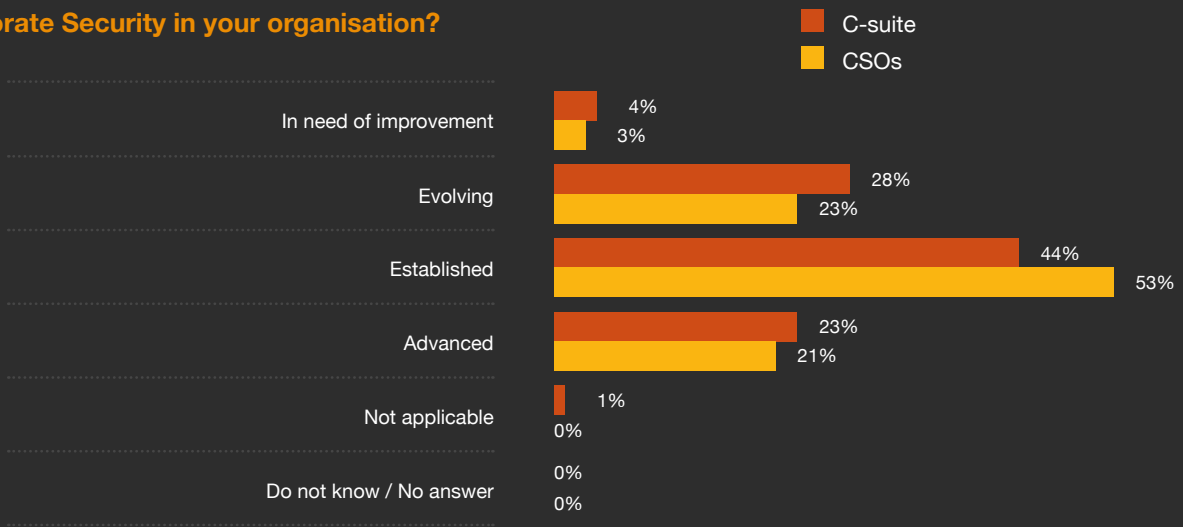
3 Maturity levels from the survey: in need of improvement, evolving, established, advanced, not applicable, do not know / no answer

A question of maturity

We asked survey participants to rate the maturity of Corporate Security within their organisation according to one of these categories: 'in need of improvement', 'evolving', 'established', 'advanced', 'not applicable', and 'do not know' or 'no answer'. 71% of respondents described their Corporate Security function as 'established' (49%) or 'advanced' (22%), while the remaining 29% of respondents selected 'in need of improvement' (3%), 'evolving' (25%), and 'does not apply' (1%).

The fact that 53% of CSOs rated their Corporate Security as 'established' demonstrate a higher degree of confidence in Corporate Security maturity than C-suite respondents, who, at 44%, were 9% less likely to select this rating. It is worth noting that, on average, confidence in the level of maturity of the Corporate Security function is highest within mid-sized companies, small companies registering a higher figure than large companies. However, it should be noted that there is not an universal framework for assessing maturity does not yet exist, therefore creation of the industry standard and the assessment framework would be an issue of the future.

In your opinion, what is the maturity level of the Corporate Security in your organisation?

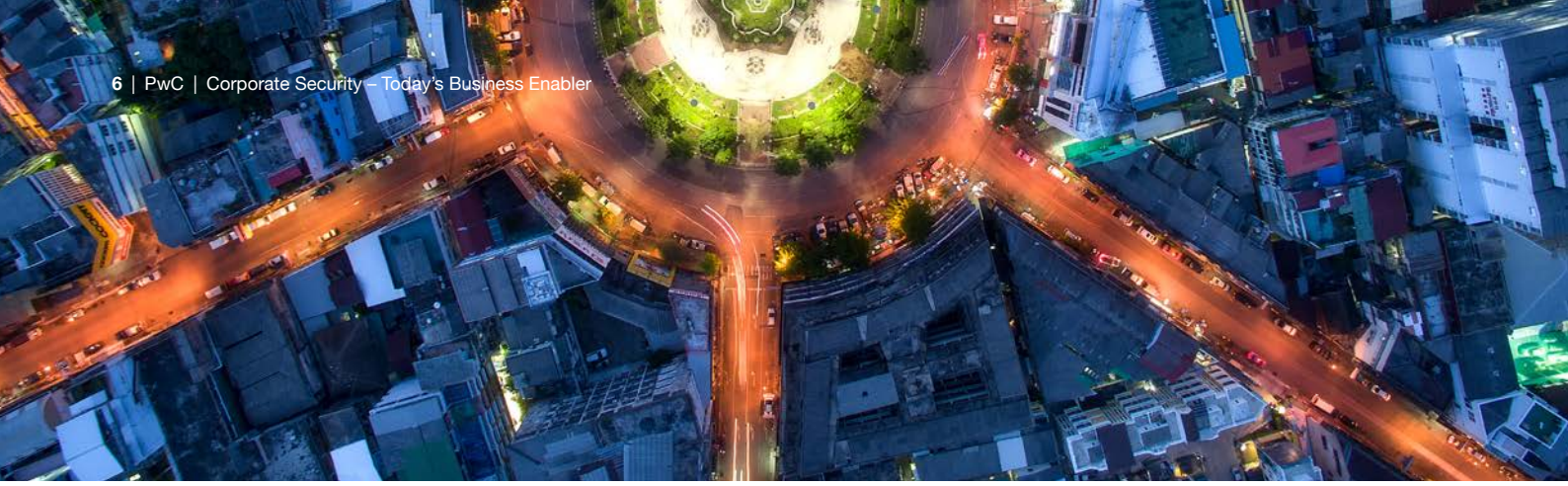


Maturity level of the Corporate Security rated as 'established' by the survey respondents by company size

57% of mid-sized companies

42% of large companies

46% of small companies



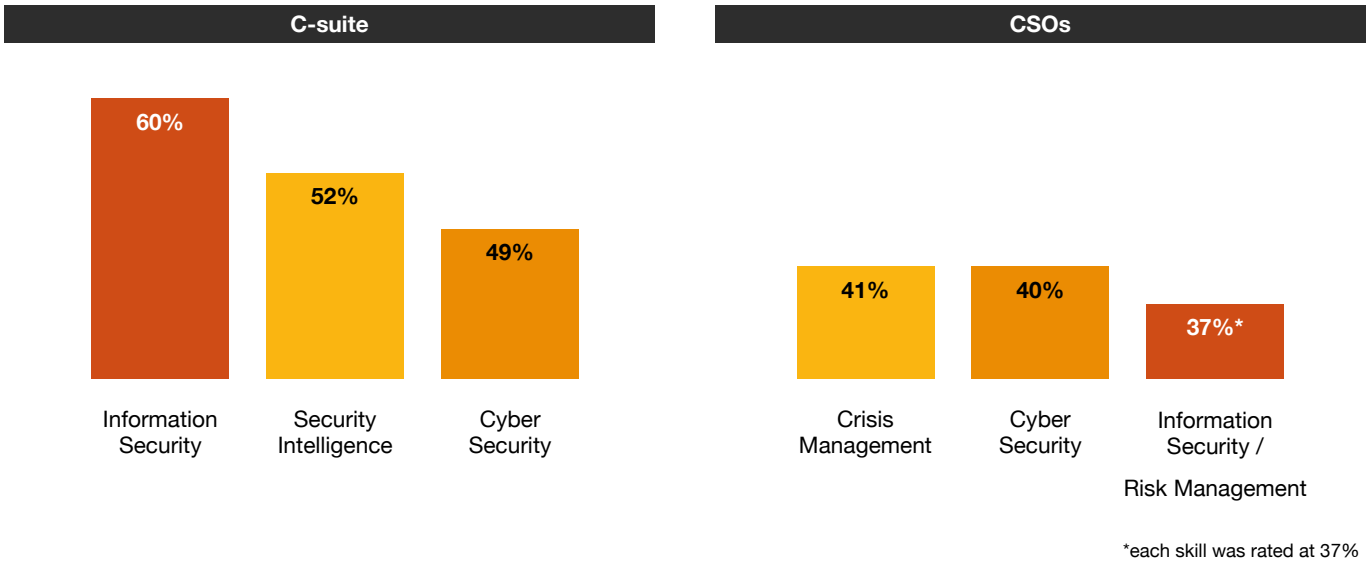
What additional skills do you wish your Corporate Security had to better address challenges it faces?

Upskilling for a new security paradigm

Businesses face an ever-growing range of security threats and look to upskill and expand their expertise to respond effectively. How Corporate Security functions equip themselves to better address the challenges they face appears to be a subject of debate between CSOs and the C-suite.

Both groups of survey participants were presented with a set of competencies and asked to highlight the areas in which they felt additional capability was most needed. Information Security (49%), Cyber Security (45%), and Crisis Management (44%) occupied the top three spots. The perception gap in the demand for additional skills and qualifications has been identified between the two groups of respondents, where the C-suite typically sees a greater need for additional skills and qualifications than CSOs. The fact that the respondents identified Information Security as the most sought-after skill set is made more noteworthy by the sizeable discrepancy between C-suite and CSO estimations. With 60% (C-suite) and 37% (CSO), a 23% gap of this kind could reflect a certain asymmetry in knowledge about where such responsibility would sit since Information Security and Cyber Security traditionally fall within the remit of IT departments. Other most significant examples are Security Intelligence, Risk Management, and Security Investigations with a gap of 28%, 10% and 16% respectively.

What additional skills do you wish your Corporate Security had to better address challenges it faces? (Top three)



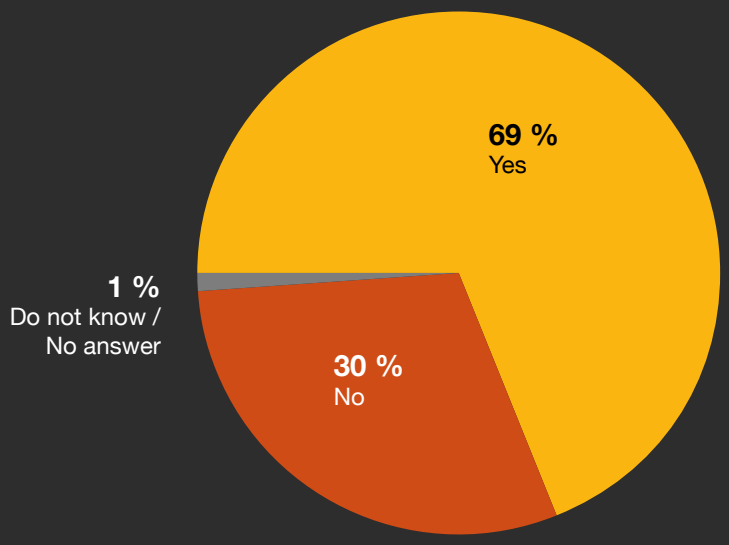
*each skill was rated at 37%

Opportunities for digitalisation within Corporate Security

Given that Information Security and Cyber Security were identified as the skills in greatest demand, we had expected to see a stronger wish for digitalisation among the respondents. In fact, only one third (30%) rated their Corporate Security as not digitalised enough.

CSOs (69%) and the C-suite (68%) were strongly aligned on the view that their Corporate Security function is sufficiently digitalised to meet their current challenges. The rate of respondents who judged their Corporate Security function to be sufficiently digitalised was 8% higher among companies in the large category compared with small and mid-sized ones.

Do you think your Corporate Security is digitalised enough to address the current challenges?



Top security challenges

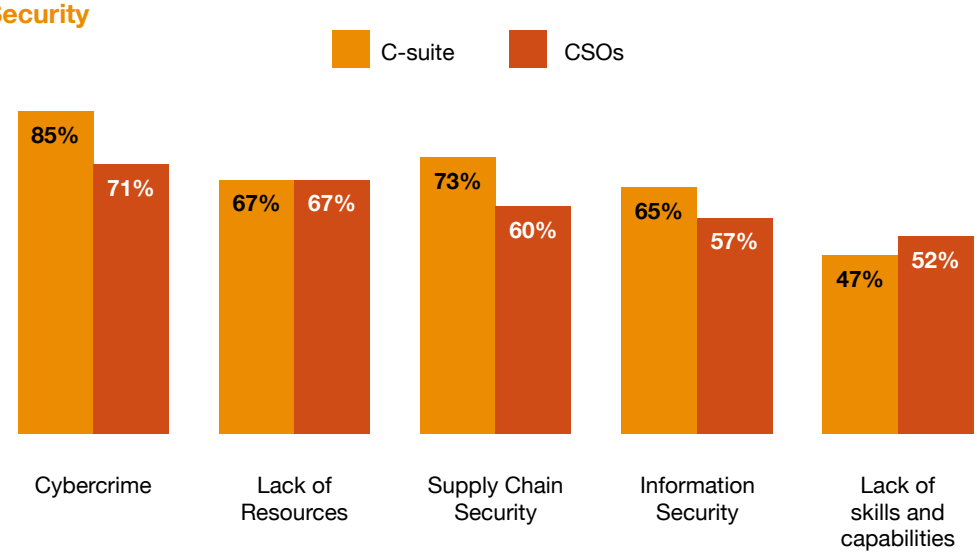
The world has become increasingly challenging due to rapid technological change, geopolitical tensions, and climate-related uncertainty. These are just some of the elements shaping a new era for Corporate Security. Learning how to cope with a growing array of threats will require Corporate Security to undergo an important evolution, one that will involve continually embracing digital tools and seeking the latest solutions to support better monitoring capabilities, updating their understanding of security threats, and fostering ever closer links to the C-suite. The looming threats of cybercrime, supply chain disruption, and mounting political tensions all add to the complexity of task ahead, highlighting the importance of a stronger awareness of the security landscape.

Our survey highlighted cybercrime as the main challenge for Corporate Security in the next 5 years by some margin (listed by 85% of the C-suite and 71% of CSOs), followed by a lack of resources indicated by 67% of the C-suite and CSOs (e.g., financial resources or FTEs, not applicable to skills and qualifications), Supply Chain Security (73% of the C-suite; 60% of CSOs), Information Security (65% of the C-suite; 57% of CSOs), and lack of skills and capabilities (47% of the C-suite; 52% of CSOs). Geopolitics and political instability ranked equally in sixth place, with 47% of the votes.

C-suite respondents demonstrated a deeper concern regarding future challenges, ranking more highly than CSOs on 12 of the 17 issues. The two groups ranked equally on lack of resources and natural disasters. For instance, 48% of C-suite indicated industrial espionage / theft of trade secrets as the main challenge for Corporate Security in the next five years, while only 32% CSOs did.

The challenges appear to correlate with company size. Larger companies view cybercrime, Supply Chain Security, lack of skills and qualifications, geopolitics, political stability, and natural disasters as problematic. Larger companies also highlighted a significantly higher number of challenges than small and mid-sized companies.

In your opinion, what are the main challenges for the Corporate Security in the next 5 years? (Top five)



Other findings

Corporate Security and its sphere of influence

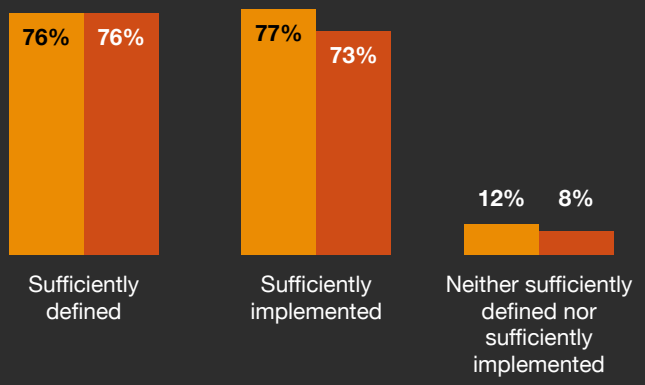
Security governance refers to how an organisation controls and directs its approach to security. When done effectively, security governance provides a pathway to guide an organisation within its security-related activities, informing decision-making and establishing clear lines of communication and accountability. 76% of respondents assessed Security Governance within their company as 'sufficiently defined', with no variance between C-suite and CSOs, while 75% felt it was 'sufficiently implemented', with C-suite only slightly (4%) more likely to agree with this view than CSOs.

In response to the question "Are you satisfied with Corporate Security's oversight function?", the survey identified a higher rate of satisfaction among C-suite (32%) choosing 'very satisfied' than CSOs (23%).

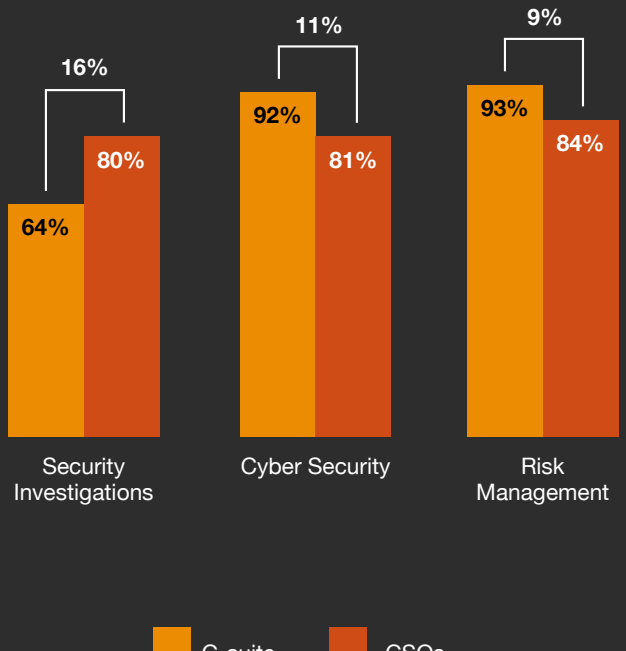
The ideal scope of the Corporate Security function is highly debatable and often varies between organisations. While there was clear agreement between both groups that certain topics fell within the remit of their Corporate Security, the data also revealed some important perception gaps on topics covered by Corporate Security, with notable examples in the areas of Security Investigations (16%), Cyber Security (11%), and Risk Management (9%). On the other hand, safety in the workplace (97%), Physical Security (93%) and Risk Management (89%) emerged as the top topics covered by Corporate Security, with identical scores between C-suite and CSOs on the first two areas. Supply Chain Security was identified as a Corporate Security focus area by a mere 66% of participants, closely followed by Security Intelligence (71%) and Security Investigations (72%). The lower percentages for these topics could indicate they are covered by other functions within the organisation.

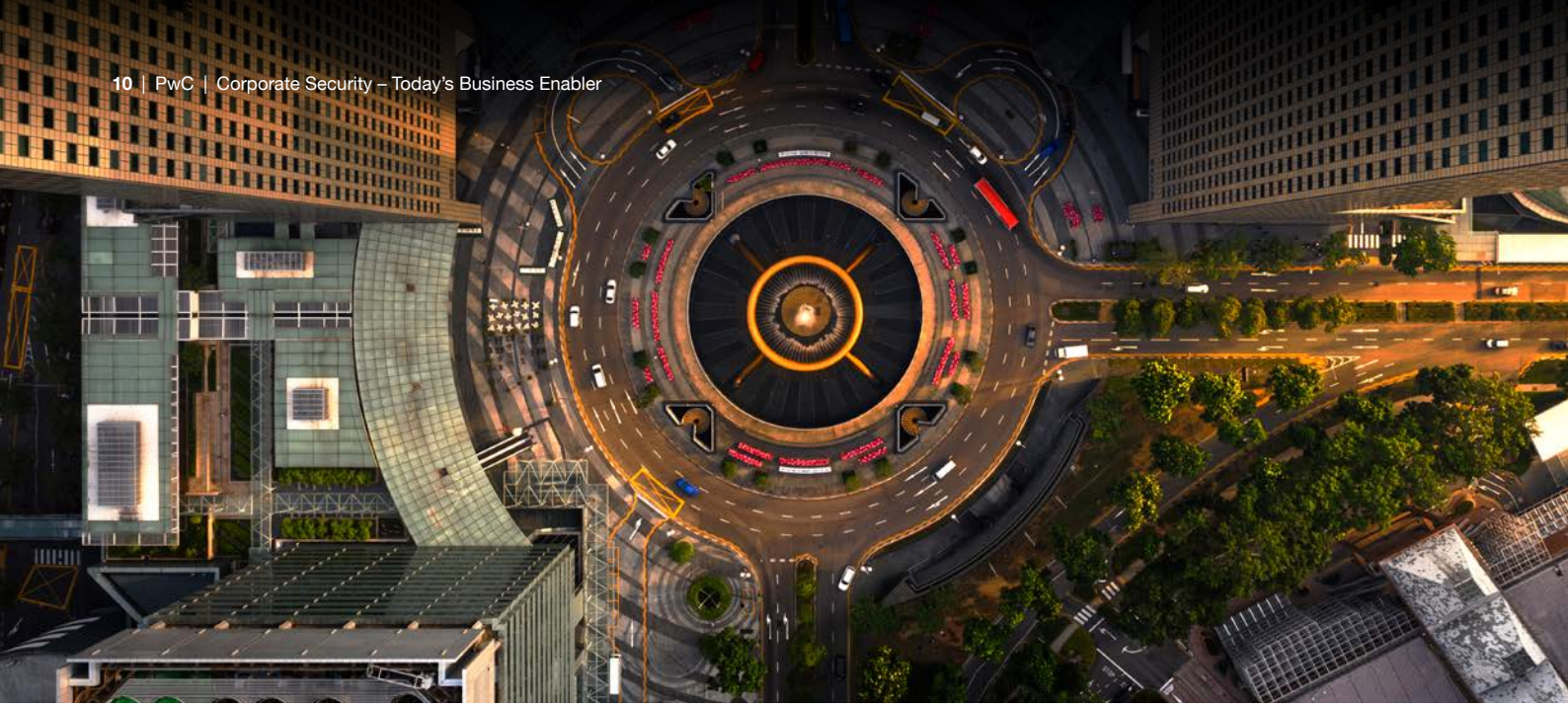
23% CSOs have requests for additional subject areas compared to 11% of C-suite. The open question "Which security topics do you wish your Corporate Security covered?" generated multiple responses for the topics Supply Chain Management, Risk Management and Physical Security. 46% of the respondents answered with 'do not know'.

Do you think that your Security Governance is sufficiently defined and implemented?



Top three perception gaps between the C-suite and CSOs of topics covered by the Corporate Security





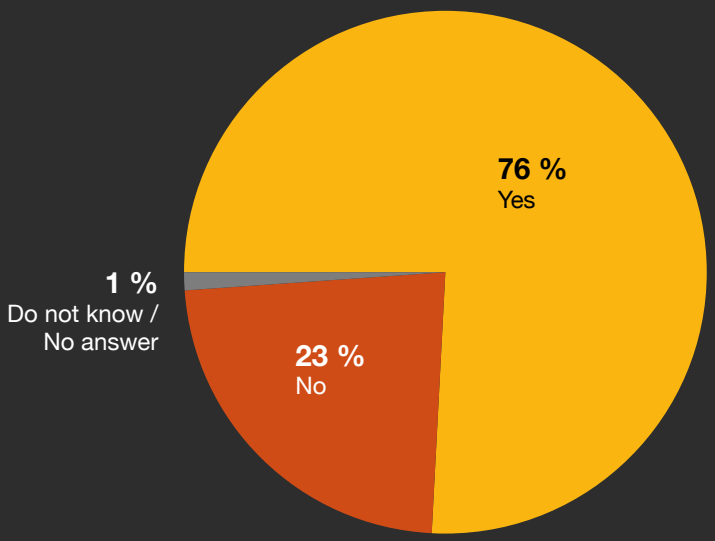
The visibility of Corporate Security

Becoming more closely aligned with the C-suite is critical to the success of the Corporate Security function and its ability to demonstrate value in managing potential security risks. Both groups presented fully aligned on whether Corporate Security is sufficiently recognized by the C-suite, with 76% agreeing and 23% disagreeing with the statement. Respondents within smaller companies are more likely to respond negatively, with 30% believing that Corporate Security is insufficiently recognised compared with 16% of respondents from mid-sized companies and 21% from large companies. However, 84% of mid-sized companies responded positively, with this number falling to 67% and 79% for companies within the small and large categories, respectively.

What is the value of having a strong security culture within a company?

A strong security culture is most likely the foundation for the security strategy and thus the effectiveness of Corporate Security. In this regard, the survey highlighted a perception that there is room for improvement (24% of all survey respondents). However, 26% of respondents judged their company's security culture as 'very strong', while 50% rated this as 'rather strong'. There were no significant gaps in perception between C-suite and CSO participants on this point.

Do you think Corporate Security is recognised enough by the C-Suite?



26%
rated their security culture as 'very strong'

50%
rated their security culture as 'rather strong'

24%
see a 'rather' and 'strong' need of their security culture

Security strategy

Having a clear, structured security strategy in place allows businesses to become more resilient in the face of threats, helping to minimise any adverse impact on physical and digital assets and operations. These can take a myriad of forms, all of which can result in additional uncertainty and impact on performance if left unchecked.

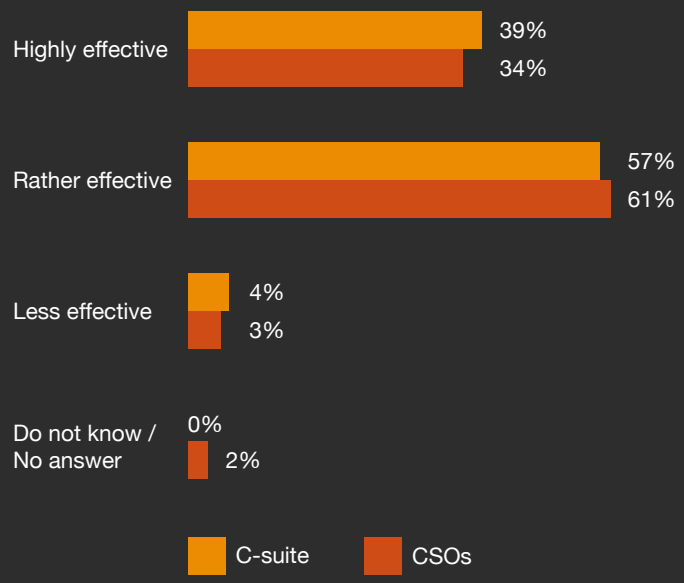
From a broader perspective, a clear security strategy is an important pillar in Corporate Security decision-making, since it can be used to justify various recommendations by aligning them with the wider company goals. 85% of organisations confirmed they have a formalised security strategy, while this figure was higher at 95% for large organisations compared to 86% of mid-sized companies, and 79% of small companies.

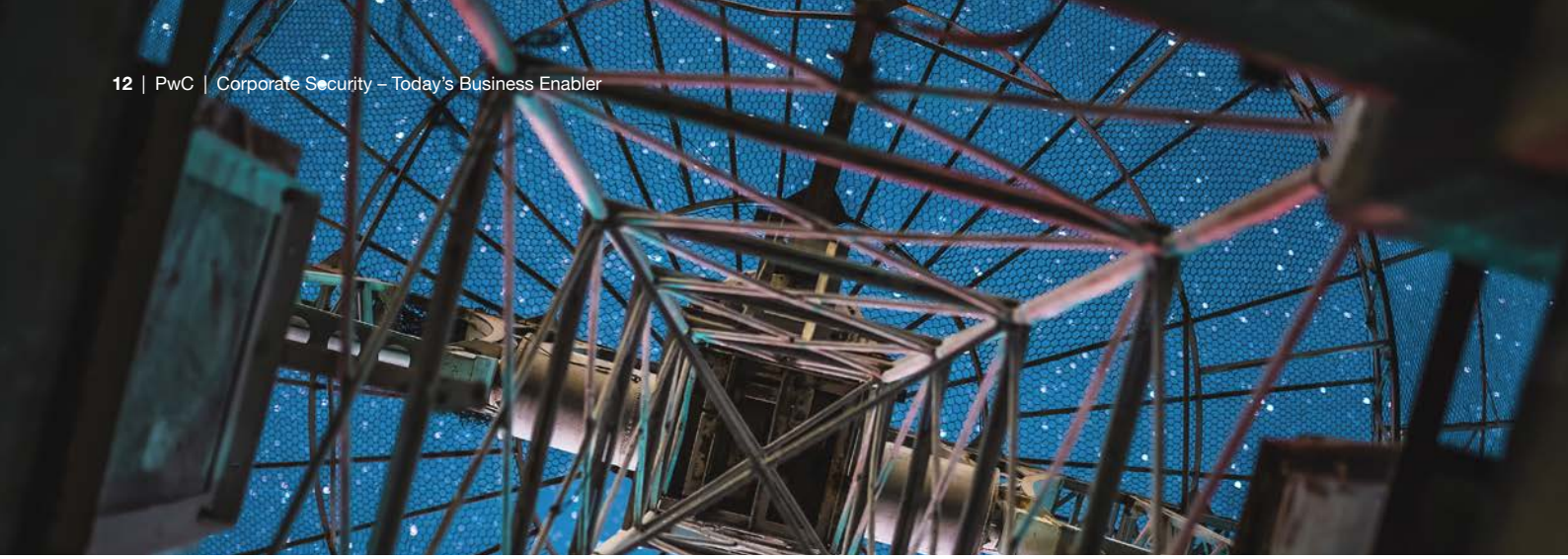
In addition, 37% of respondents rated their security strategy in mitigating business risks as 'highly effective', while 59% viewed it as 'rather effective'. Excluding the small segment of respondents (4%) who indicated their company security strategy falls short of expectations, CSOs and C-suite share a similar positive opinion on the efficacy of security strategies in mitigating business risks.

85% **of organisations have a formalised security strategy**

In terms of overall effectiveness, 72% of respondents judged their Corporate Security function as 'rather effective' in mitigating business risks (75% C-suite vs 69% CSO), with a further 17% responding with 'highly effective', split equally between both groups.

Effectiveness of the security strategy in addressing business risks





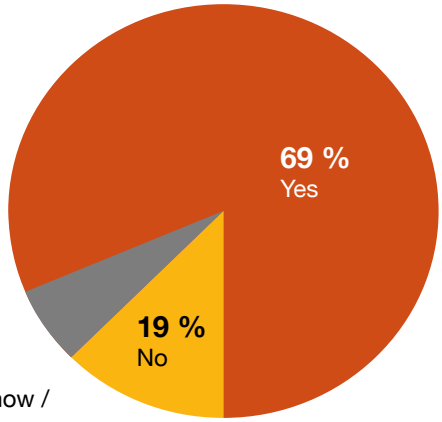
The resources for success

Given the growing number of security challenges currently facing companies, developing a robust Corporate Security TOM is more important than ever in enabling businesses to deliver on their vision and security strategy. When asked, "do you believe that your current TOM setup is adequate for the challenges of modern times", 69% of respondents indicated 'yes'.

C-suite appears more critical towards Corporate Security TOM, with 23% of them compared to 15% of CSOs assessing the TOM as non-adequate. This same trend also applies to larger companies, who are more likely to rate their TOM setup as inadequate (26%) compared with small (20%) and mid-sized (12%) companies. 12% of all respondents selected the 'do not know / no answer' response regarding the adequance of their TOM setup for the challenges of modern times.

There is a notable split in opinion on the question of whether Corporate Security receives adequate financial support. 75% of all participants responded that their Corporate Security function was adequately resourced, while 23% of CSOs disagreed with this stance compared with only 11% of C-suite. 12% of C-suite and 4% of CSOs selected the 'do not know / no answer' option, which might indicate insufficient information about the financial resources allocated to Corporate Security on the part of the management. Respondents belonging to the category of large companies are more likely (24%) to report a lack of financial resources compared to companies with a total revenue of less than €1bn (an average of 14%).

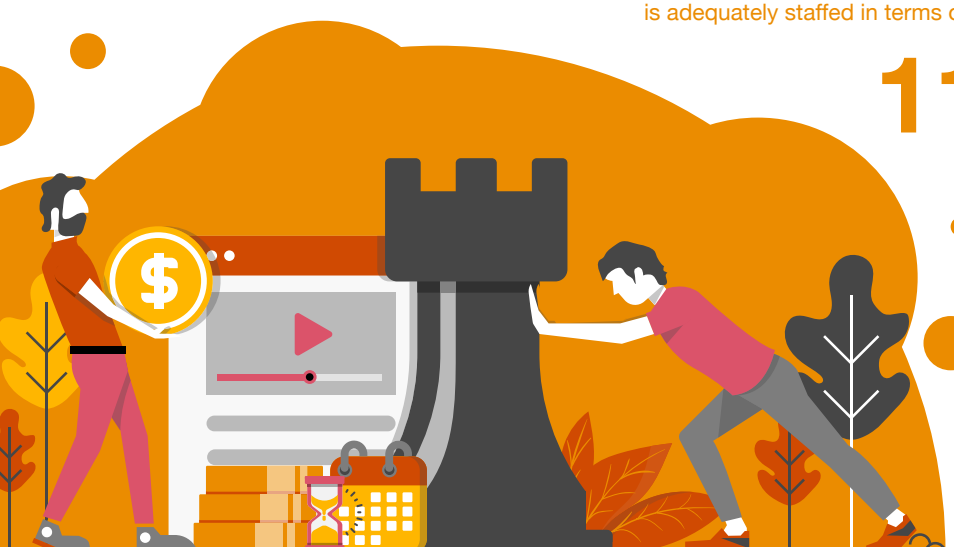
From your viewpoint, is your current TOM setup adequate for the challenges of modern times?



75% of the respondents indicated that Corporate Security is adequately staffed in terms of financial resources

11% of the C-suite said that Corporate Security is not adequately staffed in terms of financial resources

23% of CSOs said that Corporate Security is not adequately staffed in terms of financial resources



CSOs are less likely (60%) to judge Corporate Security staffing levels as 'adequate' than C-suite respondents (68%). Furthermore, CSOs are more critical than their C-suite colleagues and are 5% more likely to assess staffing levels as 'not adequate'. Larger companies are also more likely (58%) to describe themselves as 'adequately' staffed in terms of full-time employees than smaller businesses, emphasising the need for more security personnel within larger organisations.

There was a perception gap identified between groups in answering the question of whether Corporate Security was sufficiently staffed in terms of skills and qualifications. According to the data, 5% more C-suite representatives (21%) compared to CSOs (16%) saw such a need.

Responses to this question were also correlated with company size; the smaller the company, the more satisfied they were with level of skills and qualifications within their Corporate Security. 82% of the small companies assessed their Corporate Security function as 'adequate' in terms of skills set, falling to 78% and 76% for the mid-sized and large categories, respectively.

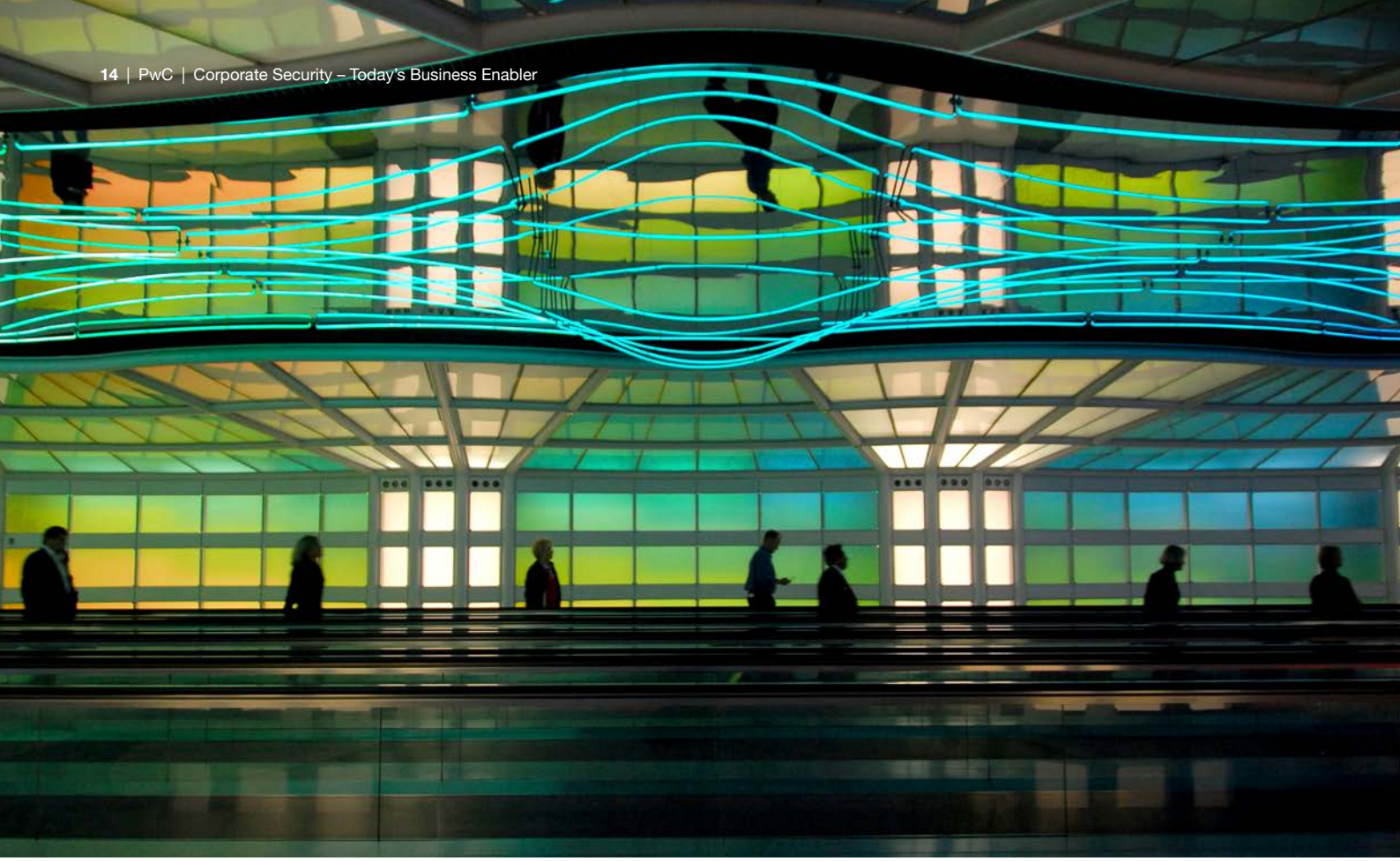
79% of CSOs and C-suite declared that their Corporate Security is adequately staffed in terms of skills and qualifications

21% of the C-suite responded that they are not adequately staffed in terms of skills and qualifications

16% of CSOs declared that they are not adequately staffed in terms of skills and qualifications

64% of the respondents declared to be adequately staffed in terms of full-time security personnel

28% of the C-Suite indicated that the Corporate Security is not adequately staffed in terms of full-time security personnel

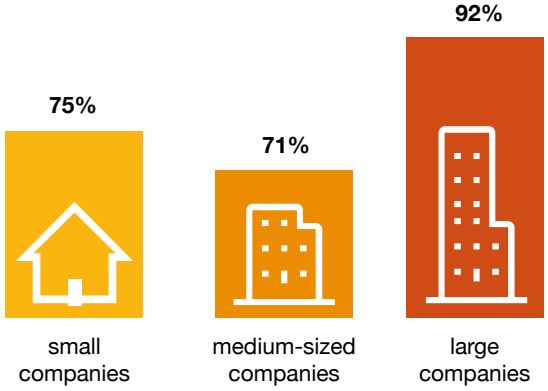


Geopolitical concerns in a globalised world

Geopolitical issues are becoming increasingly prominent on the radar of Corporate Security professionals. As the tensions keep on raising across the globe, it is incumbent on businesses to understand how Geopolitics will impact them and their objectives.

78% of respondents believe the importance of geopolitics for Corporate Security will increase in light of the war in Ukraine, with larger companies (92%) significantly more likely to subscribe to this view compared to small (75%) and mid-sized (71%), suggesting an important link between company size and the propensity to view geopolitics as a major security risk. Almost half (48%) of the respondents felt that the war in Ukraine increases security risks for their company.

Increase of the importance of Geopolitics in the light of the war in Ukraine



48%

of respondents said that the war in Ukraine increases the security risk for their company

78%

of respondents declared that the importance of Geopolitics will increase in the light of the war in Ukraine

Summary of findings

The survey indicates that while specific perception gaps exist between the C-suite and Corporate Security representatives in relation to security management within organisations, they remain aligned on key topics. As the survey is the first of its kind, we do not have a basis for comparison to help identify any longer-term trends to show the evolution of Corporate Security overtime. That said, our first-hand experience of working with companies across multiple sectors has given us a unique perspective on the changing role of Corporate Security. Playing a major role in managing crises and coordinating Crisis Management teams, for instance against the backdrop of the coronavirus pandemic or the impacts and geopolitical developments due to the war in Ukraine, gave Corporate Security increased exposure to the C-suite and enhanced the general perception of Corporate Security.

At the same time, our survey identified perception gaps that highlight a persistent need for closer alignment between the C-suite and Corporate Security. While the vast majority of respondents regard Corporate Security as a business enabler, the outcomes of the survey showcase a divergence between the perceptions of groups on several topics. The existence of such gaps emphases the need for enhancement of cooperation and communication between the parties while addressing current or future challenges.

Furthermore, our survey provides a snapshot of how both groups perceive modern enterprises' biggest security challenges. We see important differences in how CSOs and the C-suite perceive the evolution of security challenges such as industrial espionage and the threat of trade secrets over the next five years.

A further trend we observed is that while the C-suite and CSOs are generally well aligned in terms of their views on the scope of the topics covered by Corporate Security, there is some discrepancy between what the C-suite thinks Corporate Security covers and what it actually does. A gap in perception between the C-suite and CSOs on whether Corporate Security is responsible for activities like Security Investigations provides a clear case in point, emphasising the need for a realignment of expectations.

Overall, the findings reflect that both C-suite and CSOs perceive that Corporate Security has achieved a good level of maturity in their companies. However, the absence of a global Corporate Security framework or a common assessment methodology means that parties should pay additional attention to trends in the industry and find ways of benchmarking themselves against best practices. The introduction of clear criteria to evaluate Corporate Security as part of wider processes for continuous improvement will prove an essential step in ensuring organisations are fully prepared to meet the security challenges that lie ahead. Becoming more visible and engaging in a proactive dialogue with the C-suite on key topics will reinforce the importance of Corporate Security, while allowing it to spot new opportunities to grow its influence and add greater value.

Main identified gaps

28% gap

A different perception of the need for additional skills and qualifications in the field of Security Intelligence: 52% of C-Suite declared a need for them vs. only 24% of CSOs.

23% gap

A different perception of the need for additional skills and qualifications in the field of Information Security: 60% of C-Suite declared a need in this regard vs. only 37% of CSOs.

16% gap

A different understanding of scope of the security program: 80% of CSOs included Security Investigations as one of the topics covered by them, while only 64% of the C-Suite believe their Corporate Security covers them.

16% gap

Different expectations of the main challenges in the next five years: 48% of C-Suite indicated industrial espionage / theft of trade secrets as a main challenge for Corporate Security, while only 32% CSOs believed this.

Contact us to learn more

Arndt Engelmann
Partner
Advisory Risk & Regulatory

Bernhard-Wicki-Straße 8
80636 Munich

Phone: +49 89 57 90-5850
Mobil: +49 151 148 06264
E-Mail: arndt.engelmann@pwc.com

Jens Greiner
Director
Advisory Risk & Regulatory

Friedrich-Ebert-Anlage 35-37
60327 Frankfurt am Main

Phone: +49 69 9585-5831
Mobil: +49 175 353 2089
E-Mail: jens.greiner@pwc.com

pwc